Cybersecurity

Project 3 Review Questions

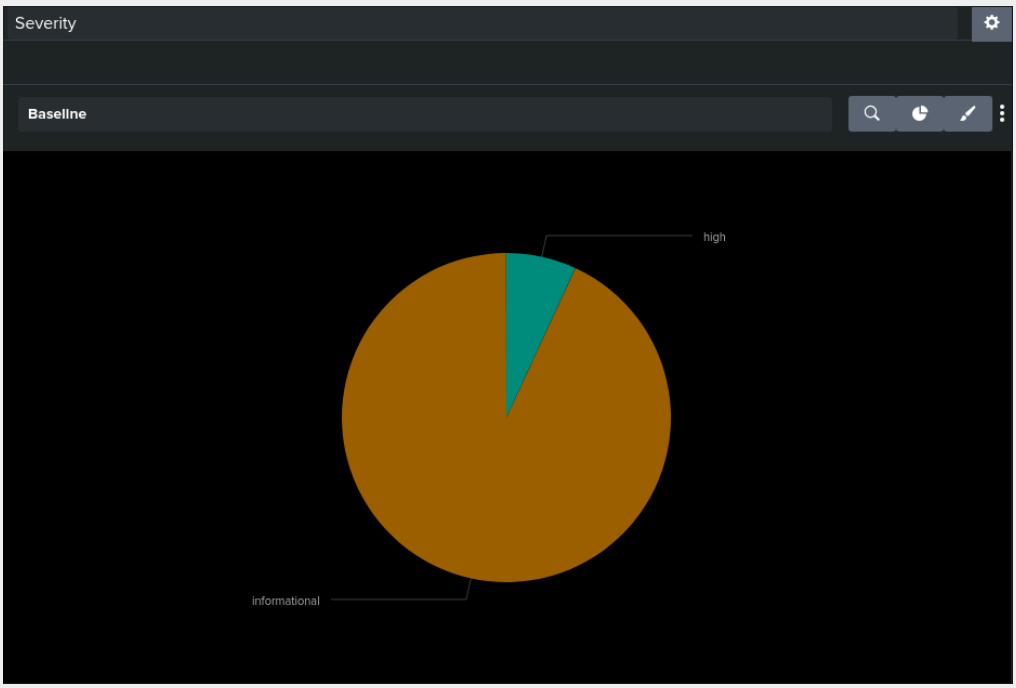
Make a copy of this document before you begin. Place your answers below each question.

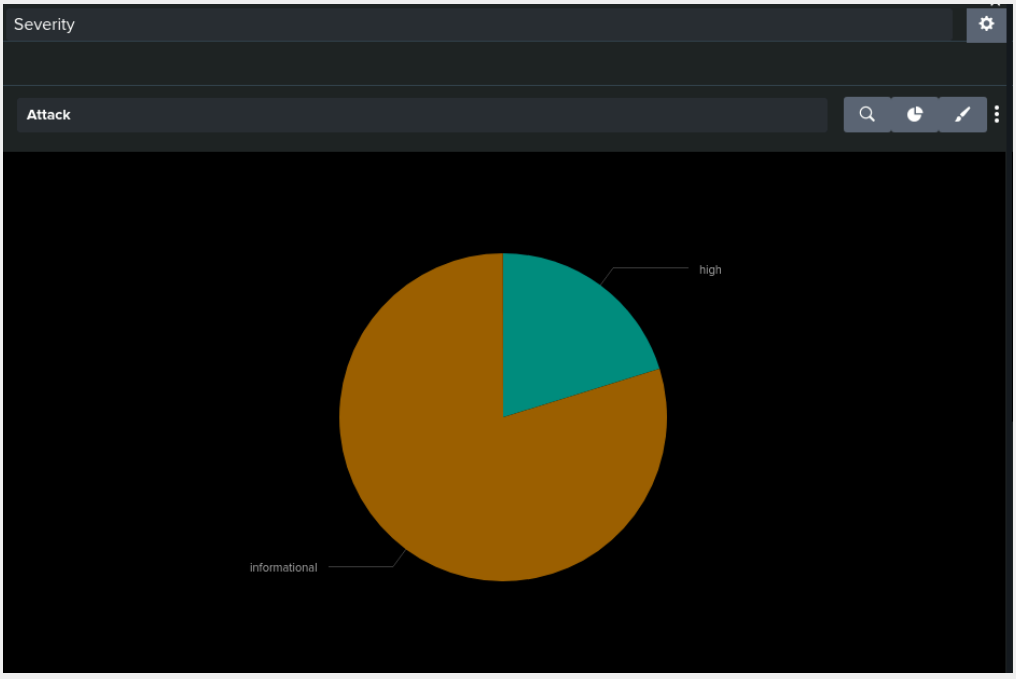
Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

```
Yes. The attack logs show "high" instances made up 20.222% of the overall,
versus 6.906% in the logs reflecting normal activity.
```

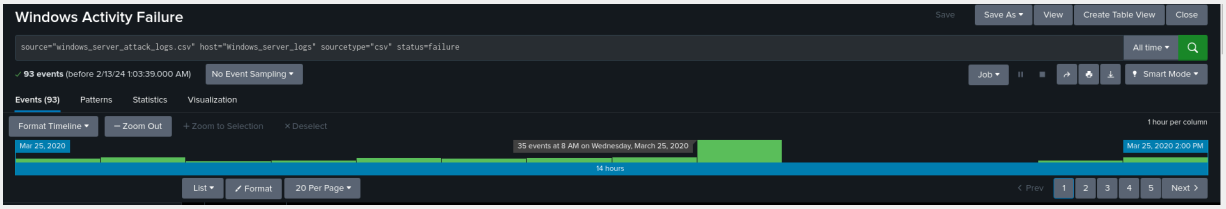




Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
Yes
```



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 events
```

- When did it occur?

```
8:28:54 AM - 8:40:38 AM Wednesday March 25, 2020
```

- Would your alert be triggered for this activity?

```
Yes
```

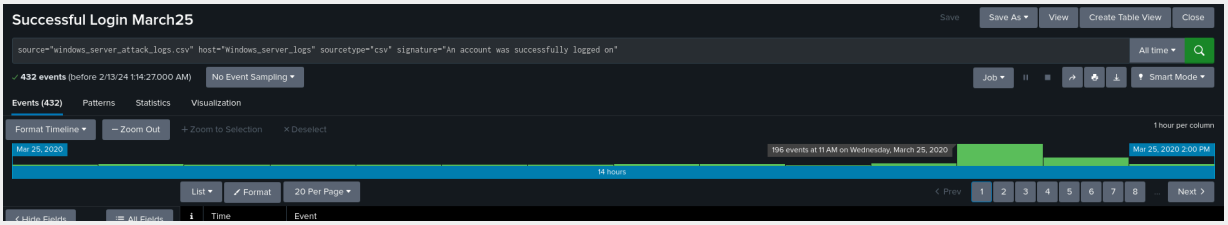
- After reviewing, would you change your threshold from what you previously selected?

```
No
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

Yes



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

196 at 11 AM and 77 at 12 PM

- Who is the primary user logging in?

user_j

- When did it occur?

10:23:55 AM - 12:26:12 PM March 25, 2020

- Would your alert be triggered for this activity?

Yes (>15)

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

Yes. While there is no other hour which would have triggered this alert, there is a large gap between the norm/threshold and what was seen in this attack, so it appears a higher threshold could be set which would still catch suspicious activity, while preventing false positives. Would recommend an adjustment to >50.

Alert Analysis for Deleted Accounts

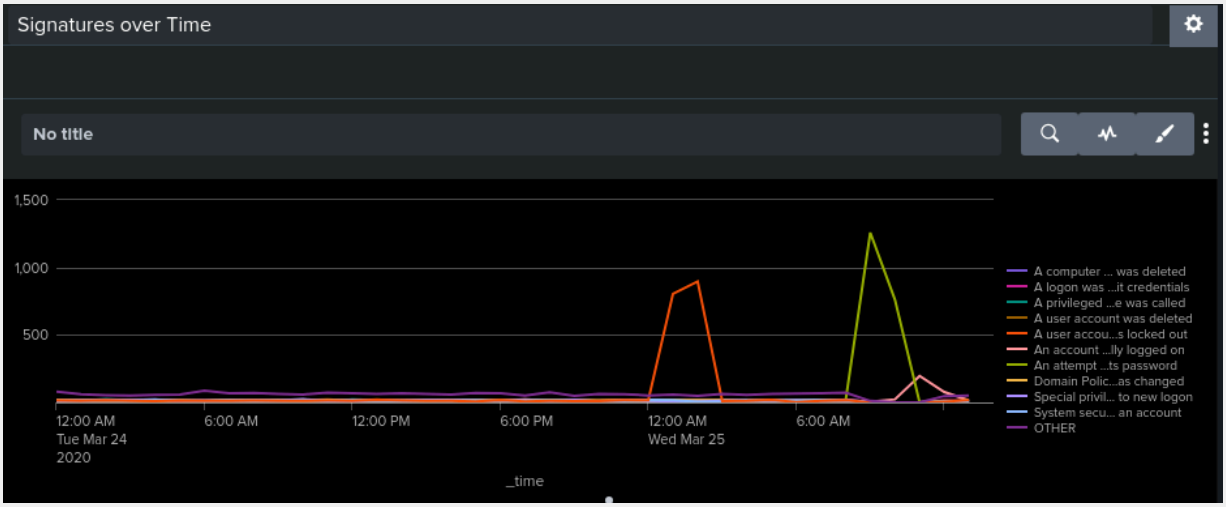
- Did you detect a suspicious volume of deleted accounts?

No

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

Yes



- What signatures stand out?

"A user account was locked out" and "An attempt was made to reset an account's password"

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

Locked out hour windows: 12:43:30 AM - 1:38:05 AM
Password reset requests: 9:32:38 AM - 10:54:24 AM
While there are other instances of each signature on either side, these appear to be the start/stop times based on the length of time between events and the overall peaks.

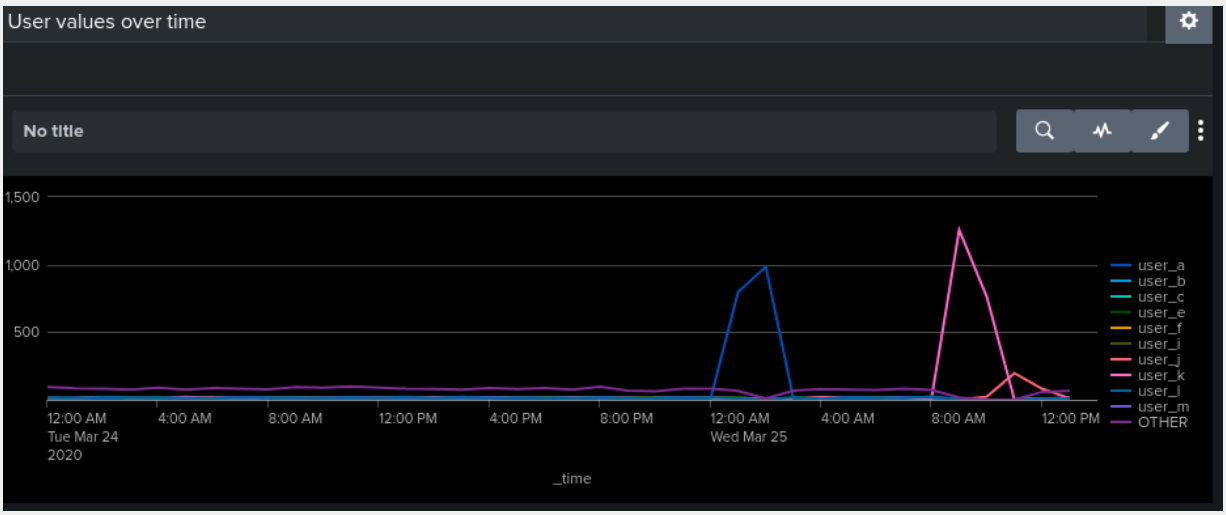
- What is the peak count of the different signatures?

Lockout: 896
Password Reset: 1258

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes. Activity is more concentrated rather than evenly spread between users.
```



- Which users stand out?

```
User a and user k
```

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

```
User_a  1:49:28 AM - 2:55:57 AM
User_k  9:32:38 AM - 10:54:24 AM
*additional logins were noted for each on the date of the attack, but these
appear to be the specific attack window events based on volume and
repetitive nature of the requests.
```

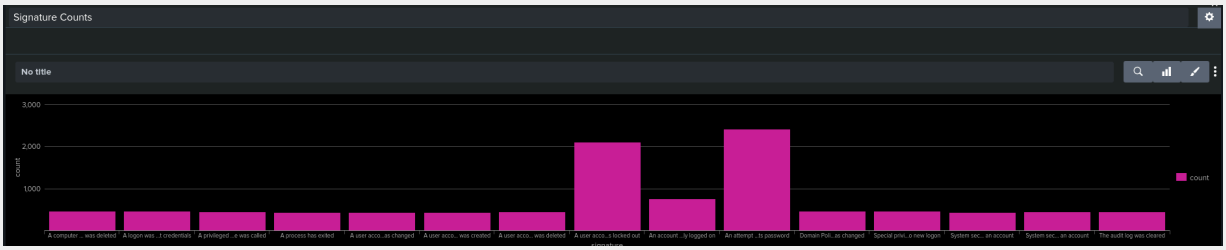
- What is the peak count of the different users?

```
A: 984
K: 1256
```

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

- Does anything stand out as suspicious?

Yes, counts for account lockout and password reset attempt are elevated compared to other signatures. While the line graph for the time chart is more obvious because it shows the peak at specific times, the overall volume still shows suspicious results on the bar graph



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

Yes

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

- Does anything stand out as suspicious?

Yes, users a and k take up much larger sections of the pie chart compared to the relatively even spread on a "normal" day. Similar to the Signatures charts/graphs, the line graph drills down by hour so the peaks are more obvious, but the overall volume still shows suspiciously large sections attributed to users a and k on the pie chart.

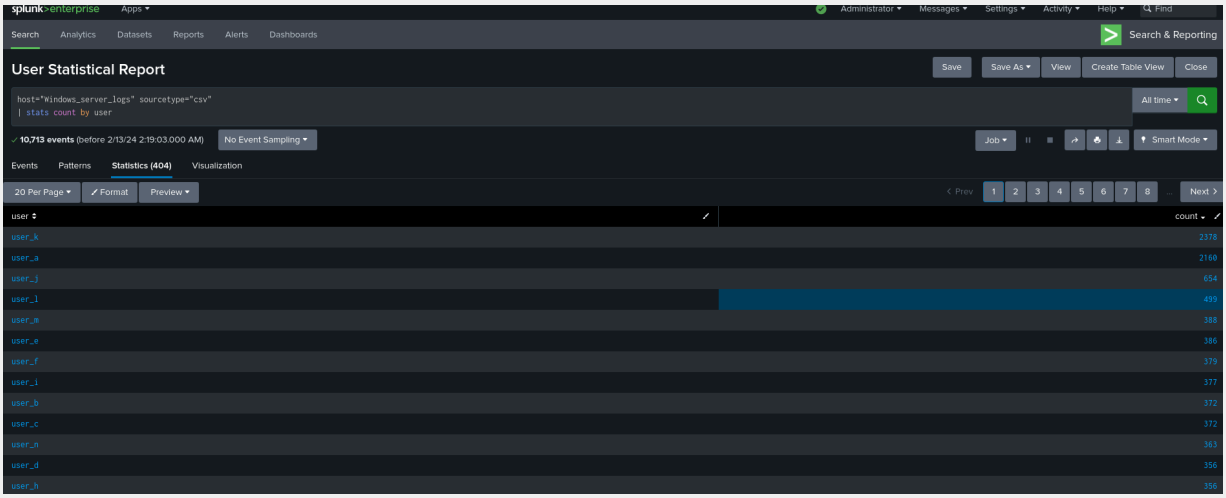
- Do the results match your findings in your time chart for users?

```
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?

```
There is a large volume of users. The statistical chart feature to sort by
user means there is no "other" section like there would be on a pie chart,
and it is not as crowded as a bar graph would be. An analyst can easily
create a list of those users with the most activity to focus on. This is
advantageous once an attack has been identified.
However, if an attack is not yet confirmed with corroborating data, a visual
representation is more likely to help with uncovering the attack before
diving into the statistical charts or details of individual logs.
```



Apache Web Server Log Questions

Report Analysis for Methods

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

```
GET requests spiked during the 6PM hour, suggesting higher than usual traffic in general. POST requests spiked during the 8PM hour. The increase in POST requests is the more drastic and concerning request type.
```

- What is that method used for?

```
The POST method sends data to a server.
```

Report Analysis for Referrer Domains

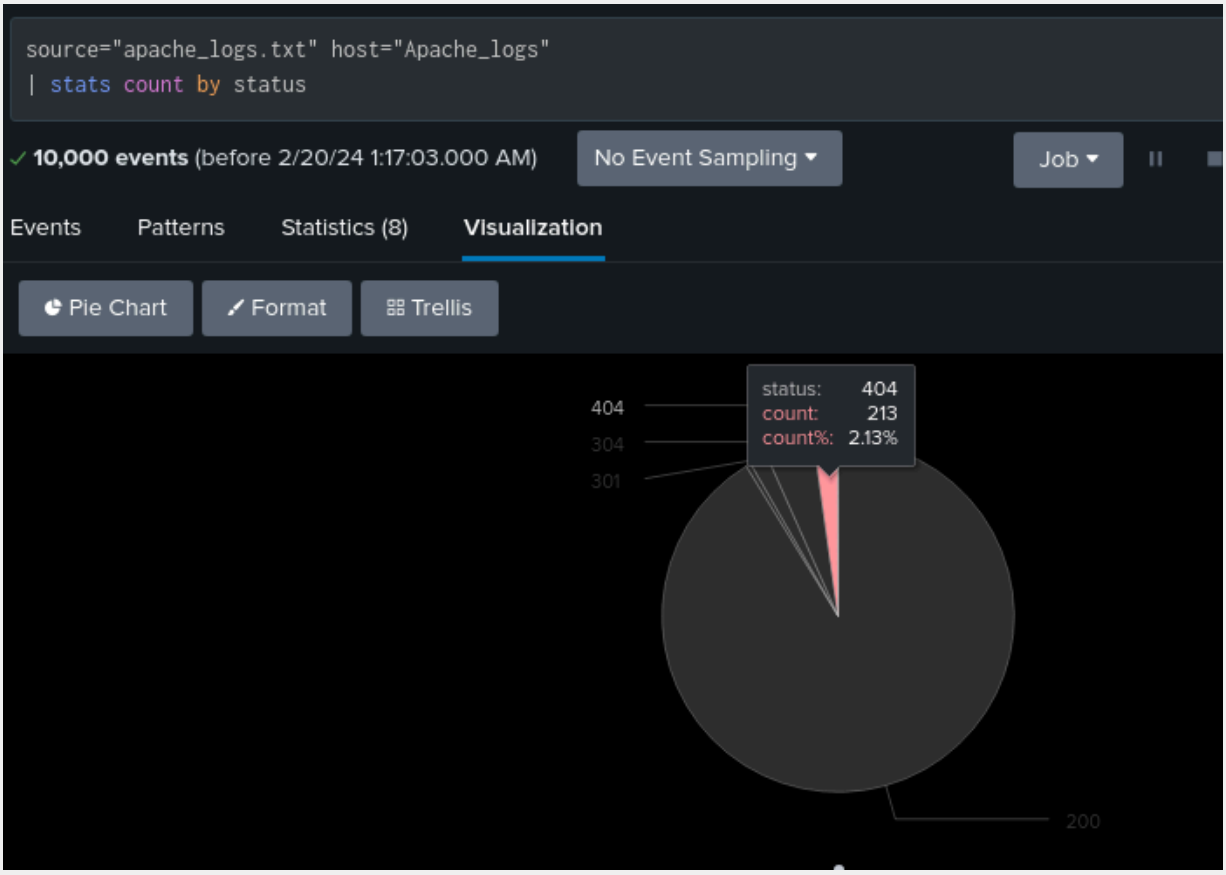
- Did you detect any suspicious changes in referrer domains?

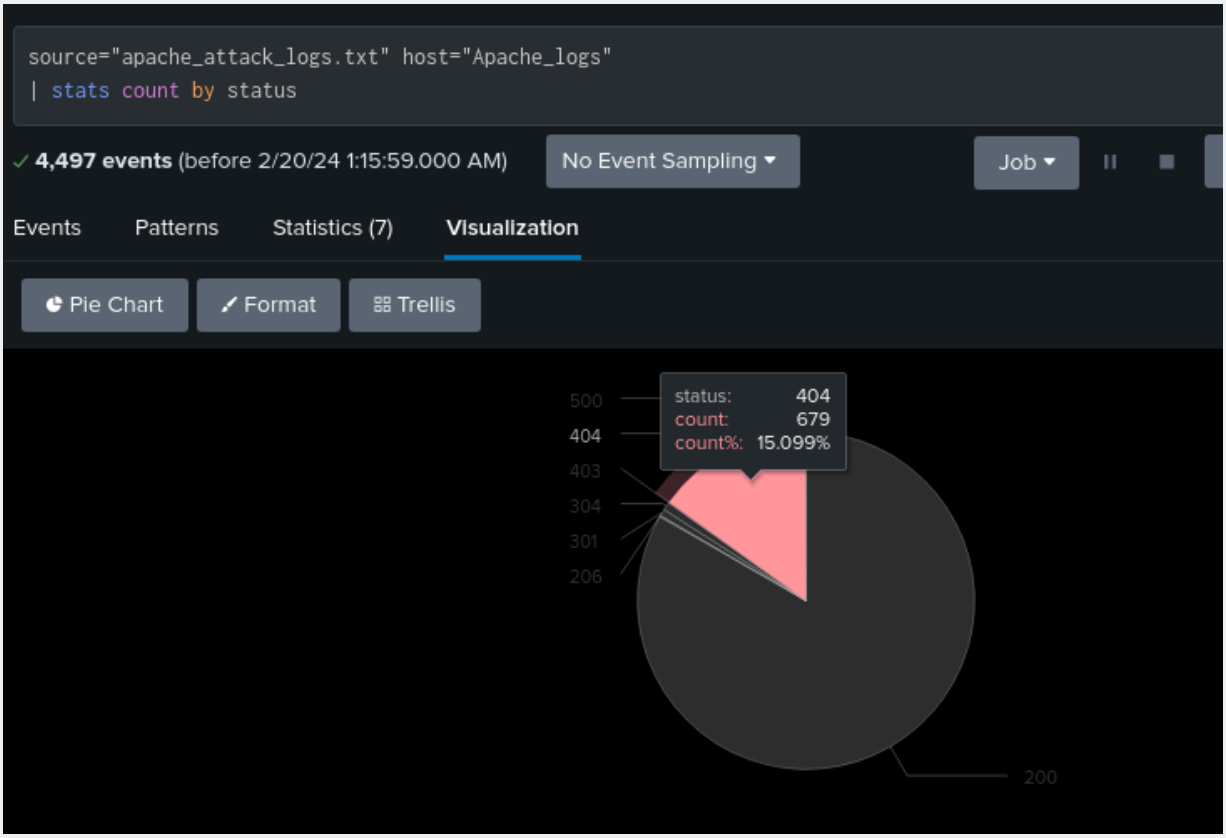
```
No.
```

Report Analysis for HTTP Response Codes

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

```
Yes. 404 response codes increased substantially. In the baseline data, 213 404 responses made up 2.13% of all responses. On the date of the attack, there were 679 404 responses which made up 15.10% of all responses.
```


source="apache_logs.txt" host="Apache_logs"
| stats count by status
10,000 events (before 2/20/24 1:17:03.000 AM)
No Event Sampling
Job
Events
Patterns
Statistics (8)
Visualization
Pie Chart
Format
Trellis
404
304
301
200
status: 404
count: 213
count%: 2.13%



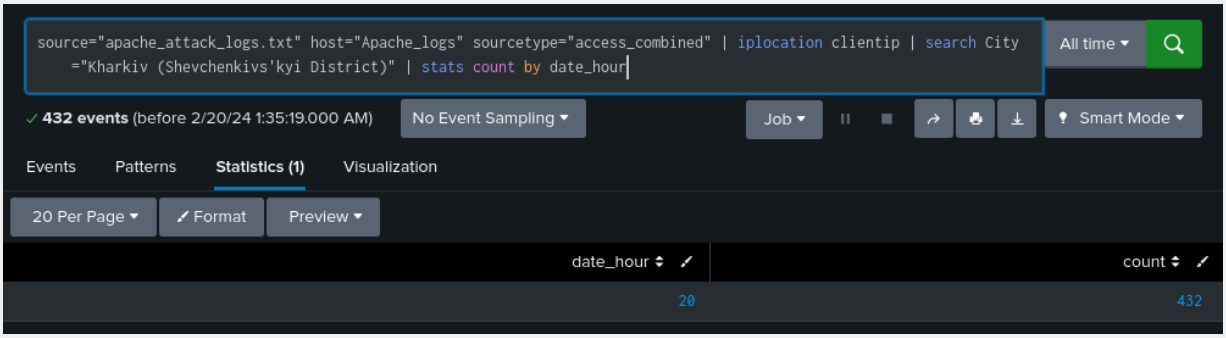
Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

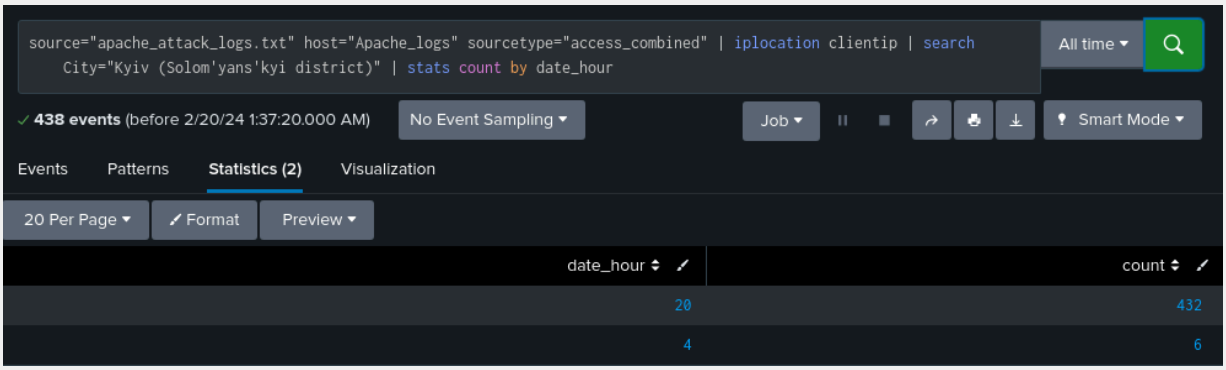
```
Yes. A larger than usual amount of traffic was coming from Ukraine.
Typically, they would not be found in the top 10 countries for traffic, but
on the date of the attack, they were second only to the United States.
```

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

```
There were 432 events originating from Kharkiv, all of which were in the 8-9
PM window.
```



There were 438 events originating from Kyiv, the bulk of which (432) were in the 8-9 PM window.



- Would your alert be triggered for this activity?

Yes.

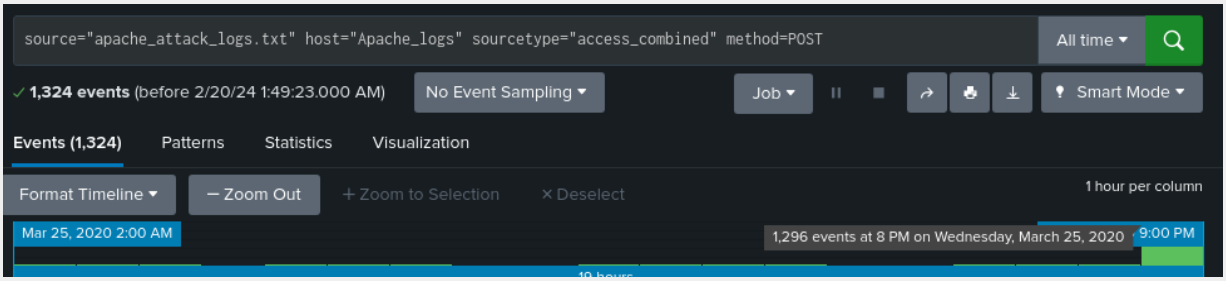
- After reviewing, would you change the threshold that you previously selected?

No. We previously set the threshold at 140, which is pretty far below the count at the time of this attack, however, there are no other hours that would come close to triggering the alert as written, so there is not currently an indicator of false positives being generated with this threshold.

Alert Analysis for HTTP POST Activity

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

Yes



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

1296

- When did it occur?

8-9 PM

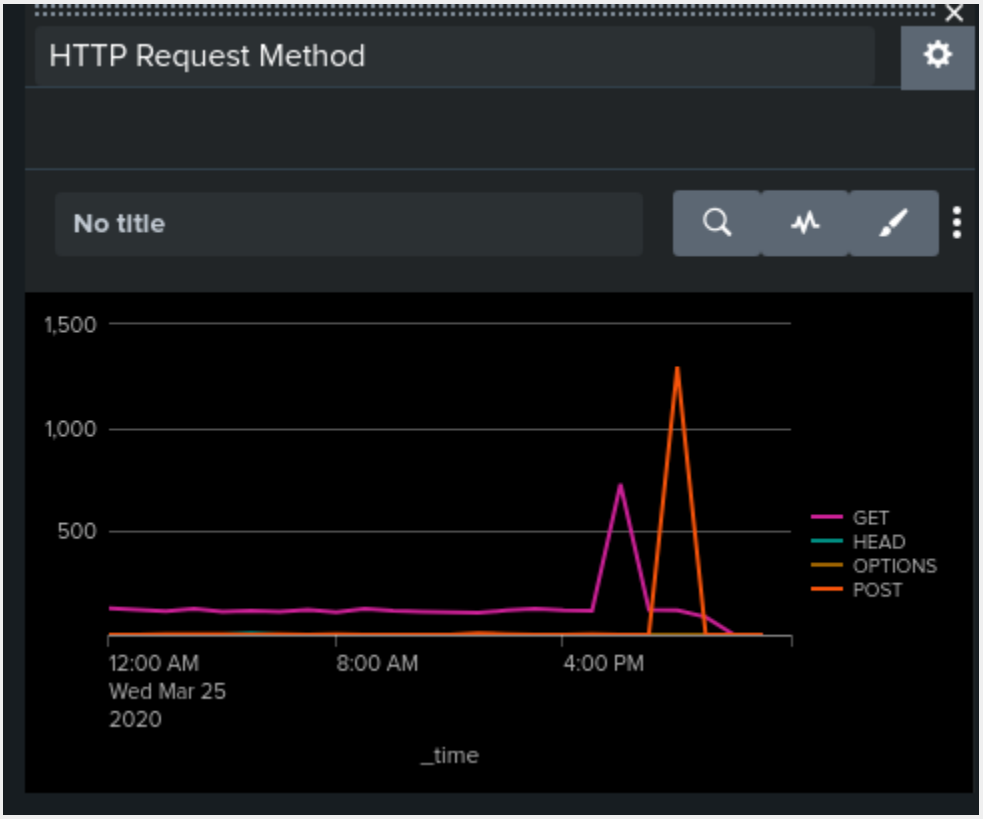
- After reviewing, would you change the threshold that you previously selected?

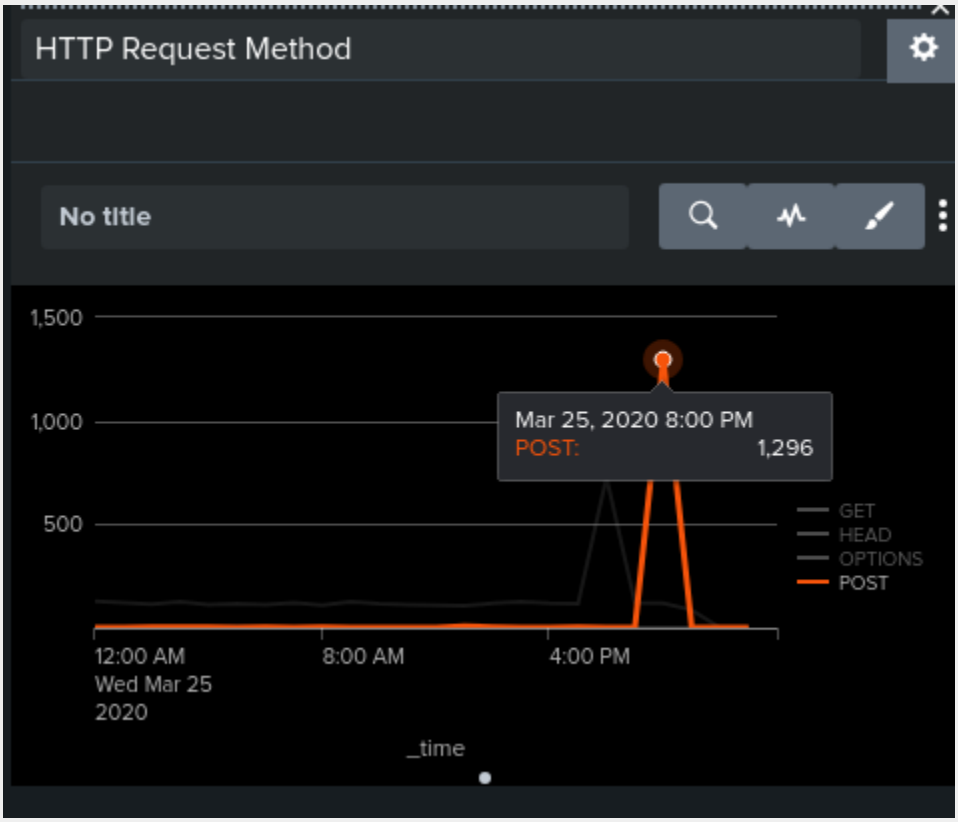
Yes. Even though no other hour would have triggered the alert in this instance, we had the threshold set at 9, which is very far below what was seen in the attack, and much closer to typical usage. Adjusting the threshold to 100 would still be certain to catch concerning activity, while lessening the likelihood of false positives.

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

Yes, large spike in POST requests is visible





- Which method seems to be used in the attack?

```
POST
```

- At what times did the attack start and stop?

```
The attack was during the 8-9PM hour. Events all appear to be at 8:05:59
```

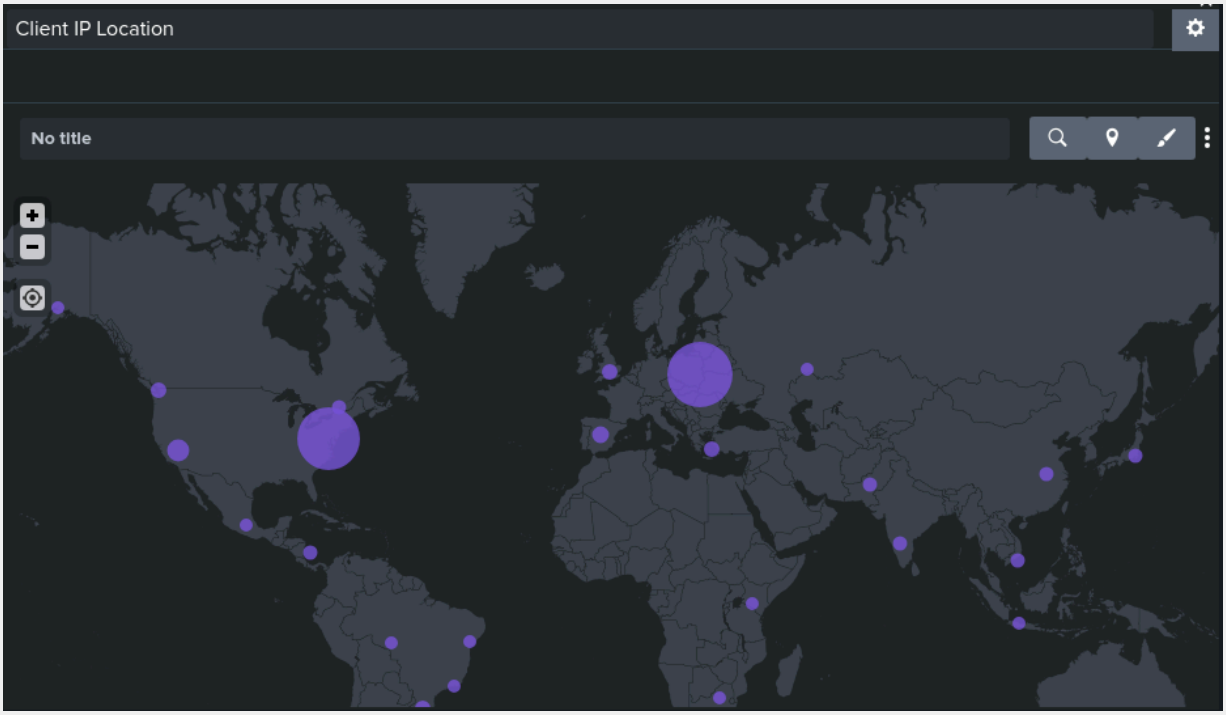
- What is the peak count of the top method during the attack?

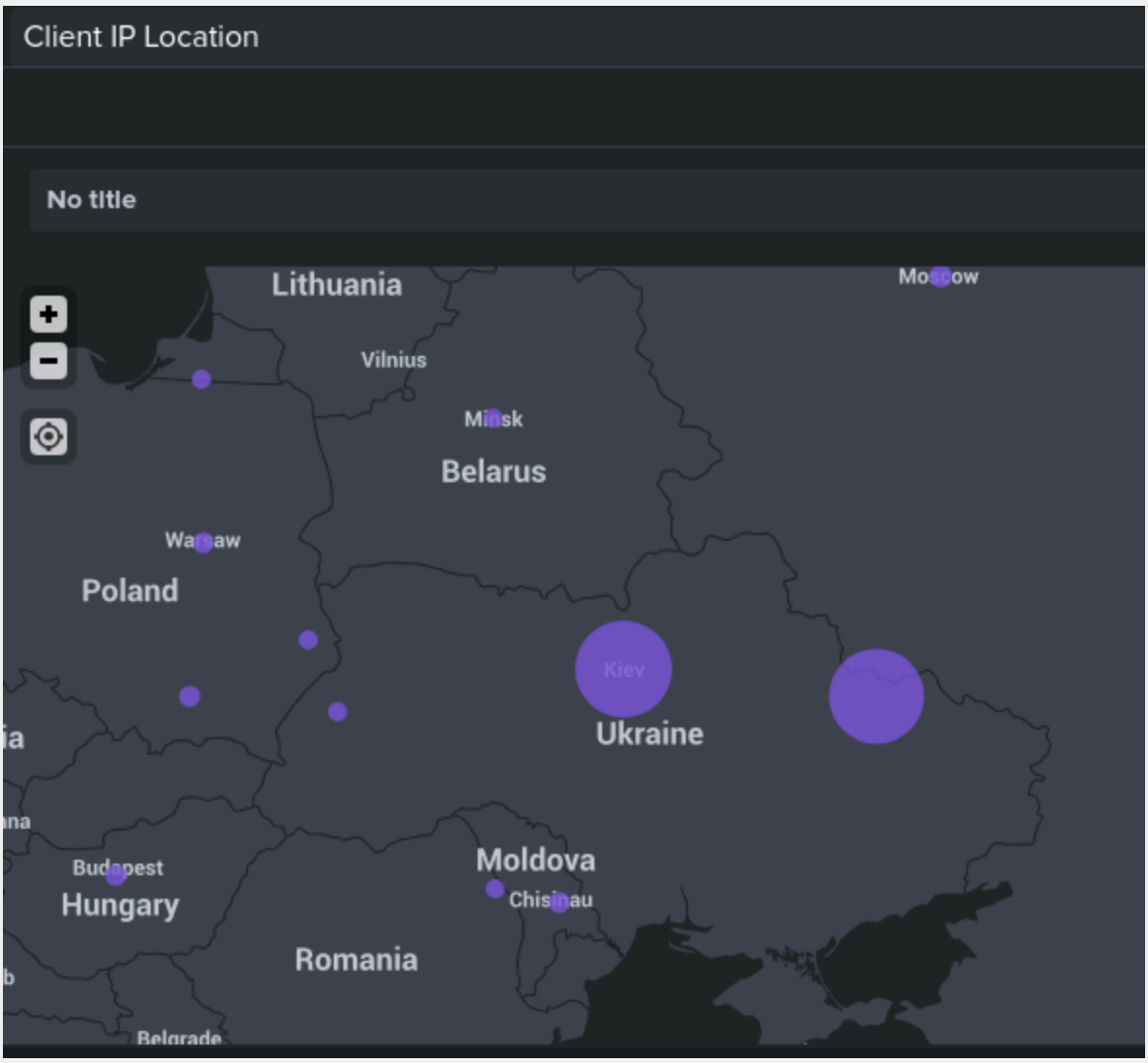
```
1296
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

Large indicator in eastern Europe, when zooming in, this is in Ukraine.





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

```
Both Kiev and Kharkiv in the Ukraine appear to have elevated activity.
```

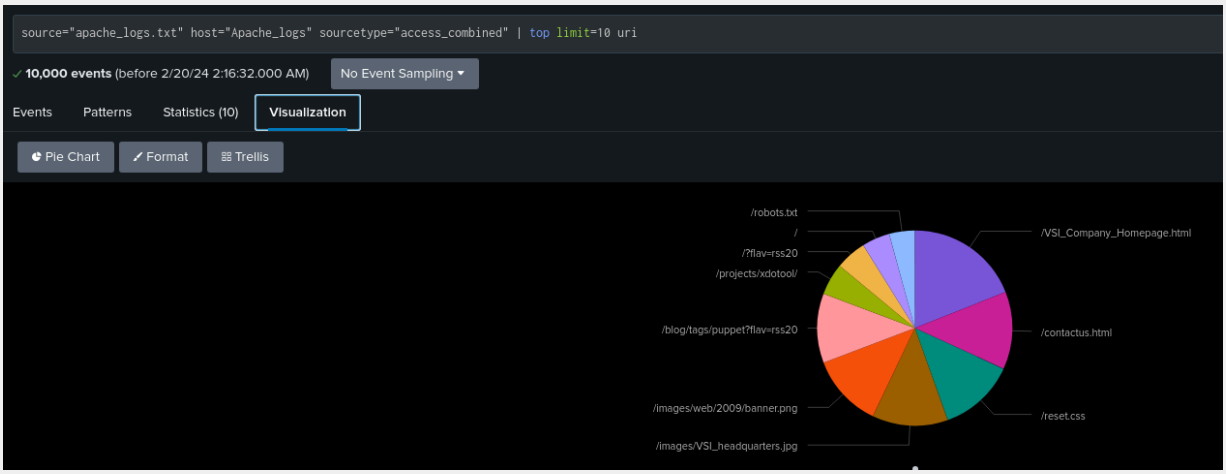
- What is the count of that city?

```
Kiev - 438
Kharkiv - 432
```

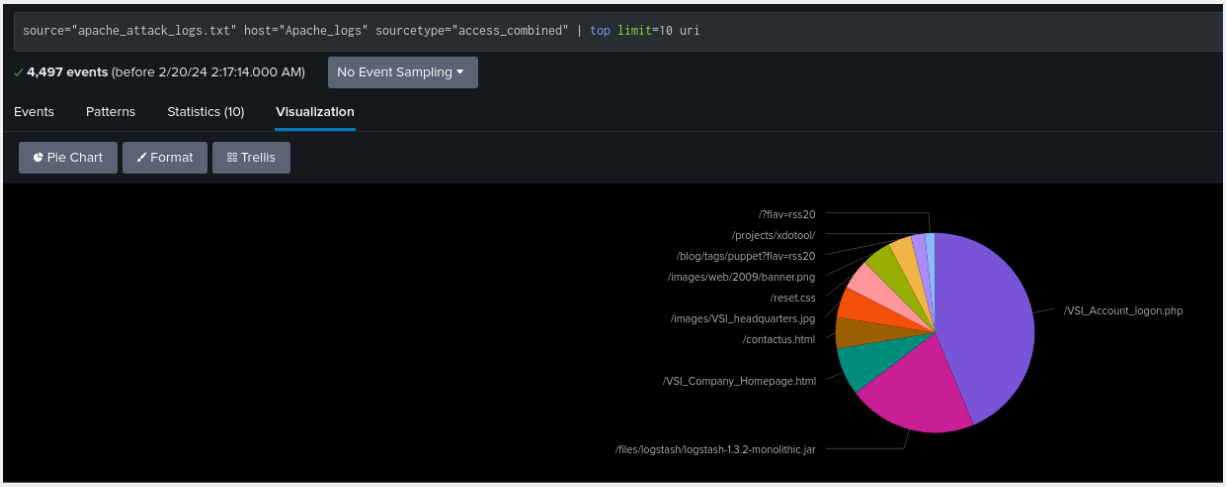
Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

Yes. Based on the baseline data, the homepage is the most common URI. On the date of the attack, this shifts drastically.
Baseline



Attack



- What URI is hit the most?

/VSI_Account_logon.php

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

This indicates a brute force attack to crack user password(s).