Cybersecurity

Project 3 Review Questions

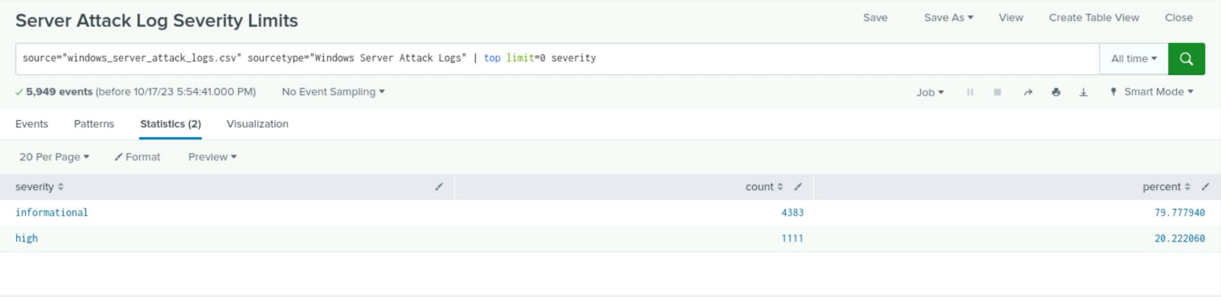
Make a copy of this document before you begin. Place your answers below each question.

Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

Between the Windows Server Logs and the Windows Server Attack Logs, we can see a major difference in the number of High severity occurrences, whereas the informal roughly stays the same. On the windows server attack logs, we can see the number of high severity occurrences is 1111, but if we look at the windows server logs we can see a much smaller number, 329.

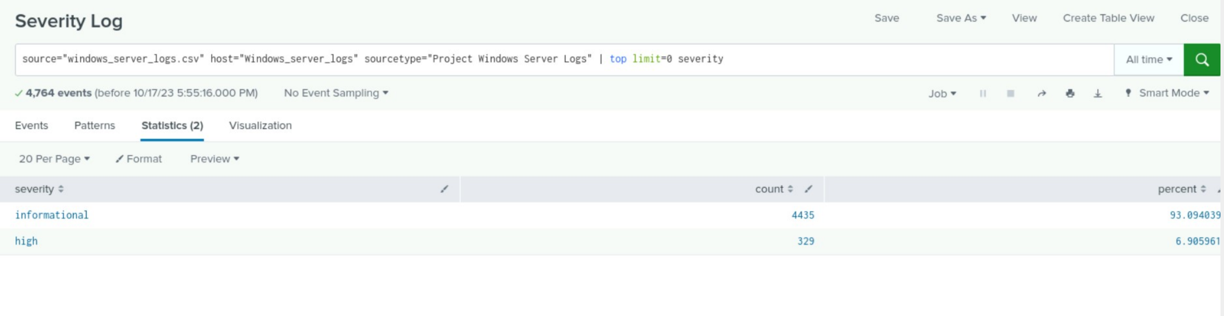


Server Attack Log Severity Limits

```
source="windows_server_attack_logs.csv" sourcetype="Windows Server Attack Logs" | top limit=0 severity
```

✓ 5,949 events (before 10/17/23 5:54:41.000 PM) No Event Sampling ▾

severity	count	percent
informational	4383	79.777940
high	1111	20.222060



Severity Log

```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="Project Windows Server Logs" | top limit=0 severity
```

✓ 4,764 events (before 10/17/23 5:55:16.000 PM) No Event Sampling ▾

severity	count	percent
informational	4435	93.094039
high	329	6.905961

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

Between the two windows server files, there is a little bit of suspicious activity regarding the success counts. In the Windows Server Attack Logs we can see an increase in successful logins by about 1200 when compared to the windows server logs.

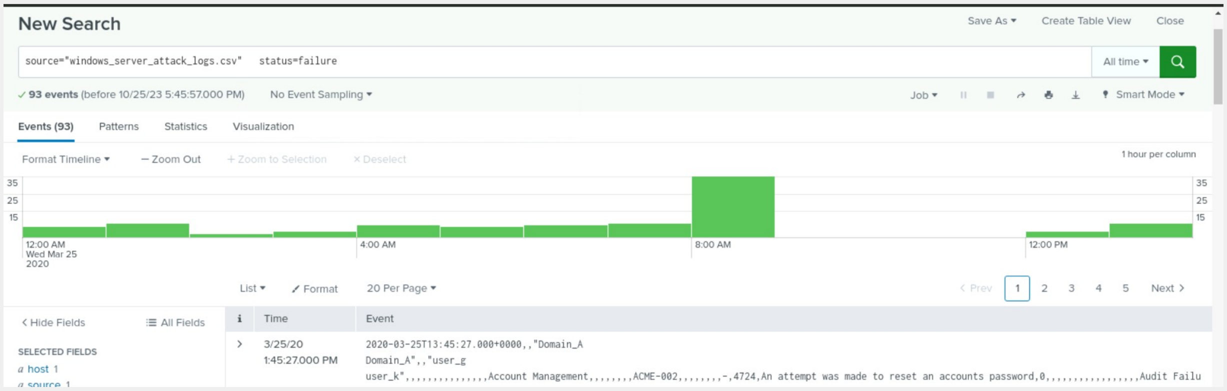
Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

There was a slight spike in suspicious activity once we analyzed the windows attack logs, I wouldn't look at the whole day and say it was an abnormal value other than the one time, which was 8:00 AM

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

There were 35 Events at the peak time at 8:00



```
source="windows_server_attack_logs.csv"   status=failure
```

✓ 93 events (before 10/25/23 5:45:57.000 PM)

3/25/20 1:45:27.000 PM

```
2020-03-25T13:45:27.000+0000,,"Domain_A
Domain_A",,"user_g
user_k",,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,,,,,Audit Failu
```

- When did it occur?

8:00AM

- Would your alert be triggered for this activity?

```
Yes, we had originally set the threshold at 15 so the alert would have been
triggered
```

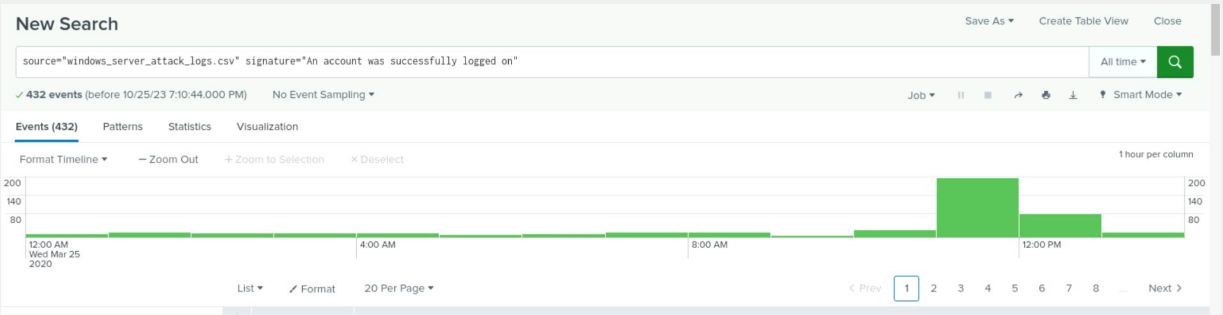
- After reviewing, would you change your threshold from what you previously selected?

```
We would maybe lower the threshold a little to maybe 20 to be safe
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
Yes we did
```



```
source="windows_server_attack_logs.csv" signature="An account was successfully logged on"
```

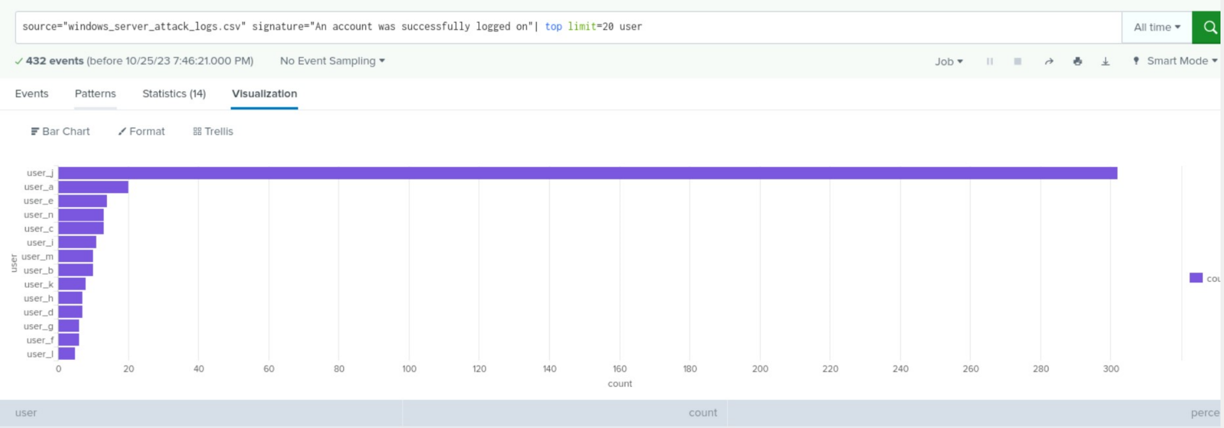
✓ 432 events (before 10/25/23 7:10:44.000 PM)

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

```
196 at 11AM Wednesday
```

- Who is the primary user logging in?

```
User J
```



```
source="windows_server_attack_logs.csv" signature="An account was successfully logged on"| top limit=20 user
```

✓ 432 events (before 10/25/23 7:46:21.000 PM) No Event Sampling ▾

- When did it occur?

```
Between 11 and 1
```

- Would your alert be triggered for this activity?

```
Yes as our Threshold was set at 25
```

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

```
We would maybe raise our threshold a bit.
```

Alert Analysis for Deleted Accounts

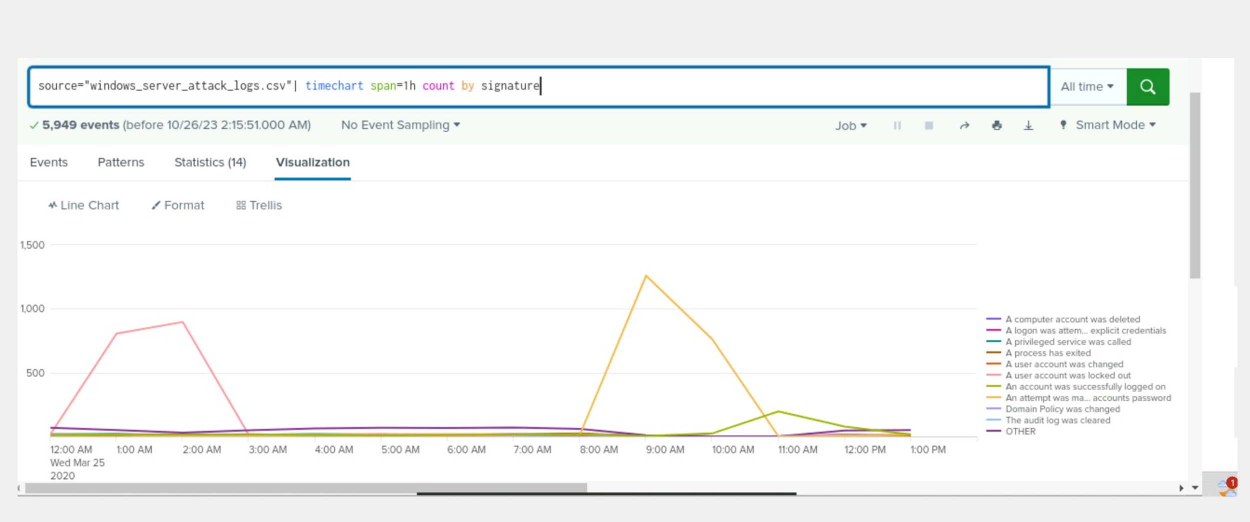
- Did you detect a suspicious volume of deleted accounts?

```
Yes we did, at around 9:00AM
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
Yes, the password reset and account lockout spikes in the day
```



```
source="windows_server_attack_logs.csv"| timechart span=1h count by signature
```

✓ 5,949 events (before 10/26/23 2:15:51.000 AM)

All time ▾
No Event Sampling ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (14)
Visualization
Line Chart
Format
Trellis
1,500
1,000
500
12:00 AM
Wed Mar 25
2020
1:00 AM
2:00 AM
3:00 AM
4:00 AM
5:00 AM
6:00 AM
7:00 AM
8:00 AM
9:00 AM
10:00 AM
11:00 AM
12:00 PM
1:00 PM
A computer account was deleted
A logon was attem... explicit credentials
A privileged service was called
A process has exited
A user account was changed
A user account was locked out
An account was successfully logged on
An attempt was ma... accounts password
Domain Policy was changed
The audit log was cleared
OTHER

- What signatures stand out?

```
An Attempt was made to reset an accounts password and A user account was locked out
```

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

```
12-3 AM for the User account lockout, and around 8-11 AM for the reset password
```

- What is the peak count of the different signatures?

```
896 for the User account lockout, and around 1,258 for the reset password
```

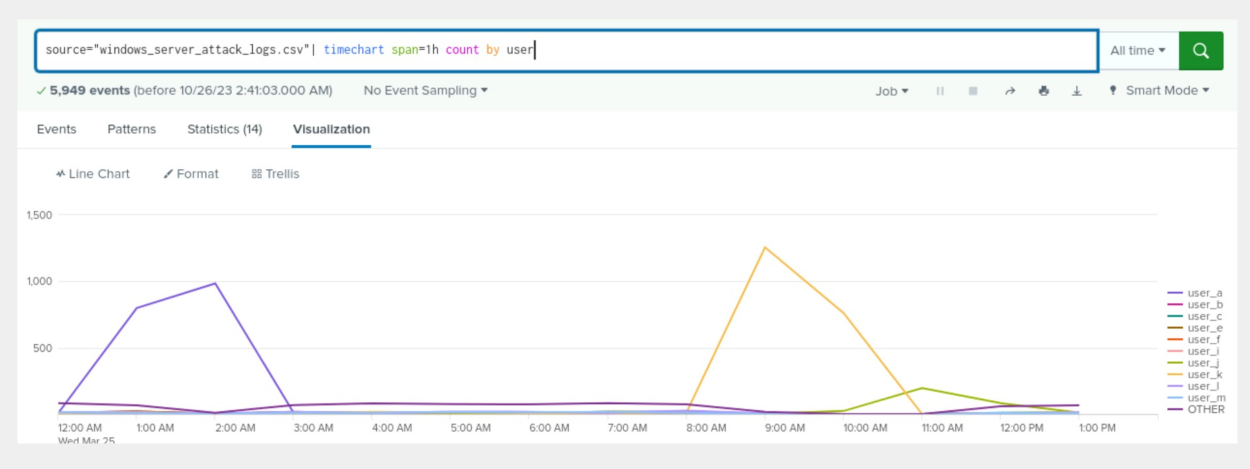
Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes, 2 spikes from 12-3 AM and 8-11AM
```

- Which users stand out?

```
User A and User K
```



```
source="windows_server_attack_logs.csv"| timechart span=1h count by user
```

✓ 5,949 events (before 10/26/23 2:41:03.000 AM)

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

```
User A went from 12am-3am and User K went from 8 to about 11
```

- What is the peak count of the different users?

```
The peak for User A was 984 and 1256 for User K
```

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

- Does anything stand out as suspicious?

```
Yes, there were a few differences between the Bar and pie chart
```

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

```
It seemed like the bar and pie charts were a little bit more precise in
breaking down the totals per hour. Because of this there were more peaks and
the numbers were a little skewed. For example with a bar chart we can see
two major spikes at 1 am and 2 am and concrete numbers for both.
```

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

- Does anything stand out as suspicious?

Yes

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

The same can be said with the users chart that was said for the signature chart, it breaks down multiple instances of activity and illustrates a more detailed timeline.

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?

Visually it definitely helps to look at this as a graph so you can quickly pinpoint the peaks, however the stats page allows you to be more granular over time and look at specific points for each user.

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 significant decrease in normal activity with the GET Method and significant increase with the POST Method

- What is that method used for?

They are used to send and request data to the 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, almost all of the POST came at 8:00PM
```

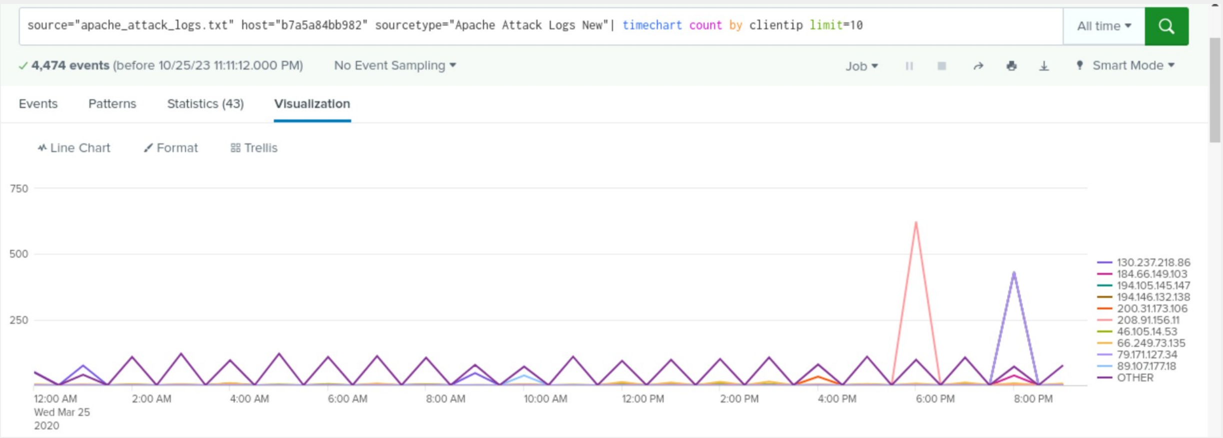
Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes, we found a couple major spikes in International Activity
```

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

```
We found a count of 624 at 6:00PM and another spike of 432 at 8:00PM
```



```
source="apache_attack_logs.txt" host="b7a5a84bb982" sourcetype="Apache Attack Logs New"| timechart count by clientip limit=10
```

All time ▾

✓ 4,474 events (before 10/25/23 11:11:12.000 PM)   No Event Sampling ▾

- Would your alert be triggered for this activity?

```
Yes it would have, as we set our alert to 125
```

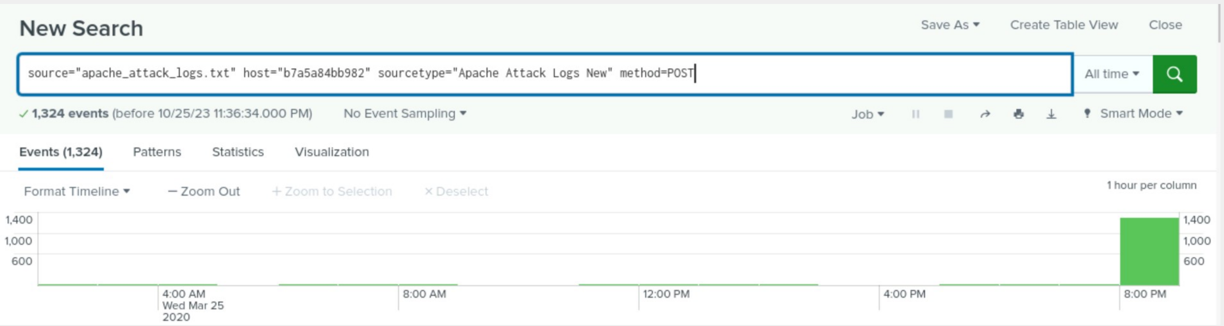
- After reviewing, would you change the threshold that you previously selected?

```
We would most likely not change the threshold
```

Alert Analysis for HTTP POST Activity

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

```
Yes we did, there was one unusual spike later in the day
```



```
source="apache_attack_logs.txt" host="b7a5a84bb982" sourcetype="Apache Attack Logs New" method=POST
```

✓ **1,324 events** (before 10/25/23 11:36:34.000 PM)

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

```
1,296
```

- When did it occur?

```
8:00PM
```

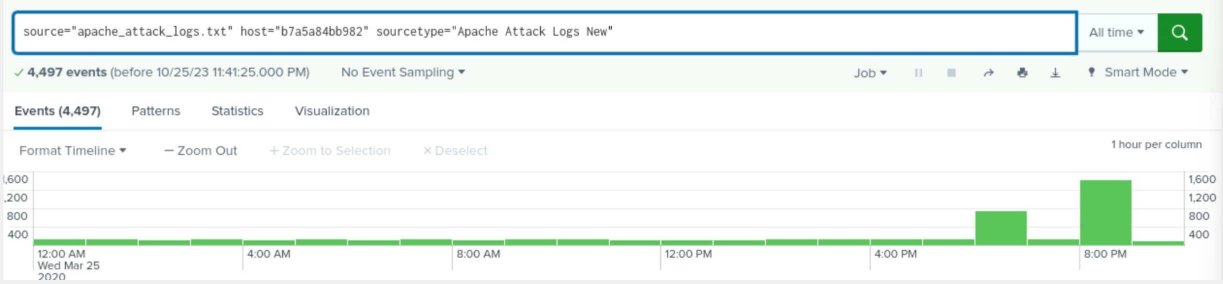
- After reviewing, would you change the threshold that you previously selected?

```
I would not change the threshold, as the spike seems to be an extreme outlier
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
Yes, there are two fairly suspicious spikes towards the end of the day
```

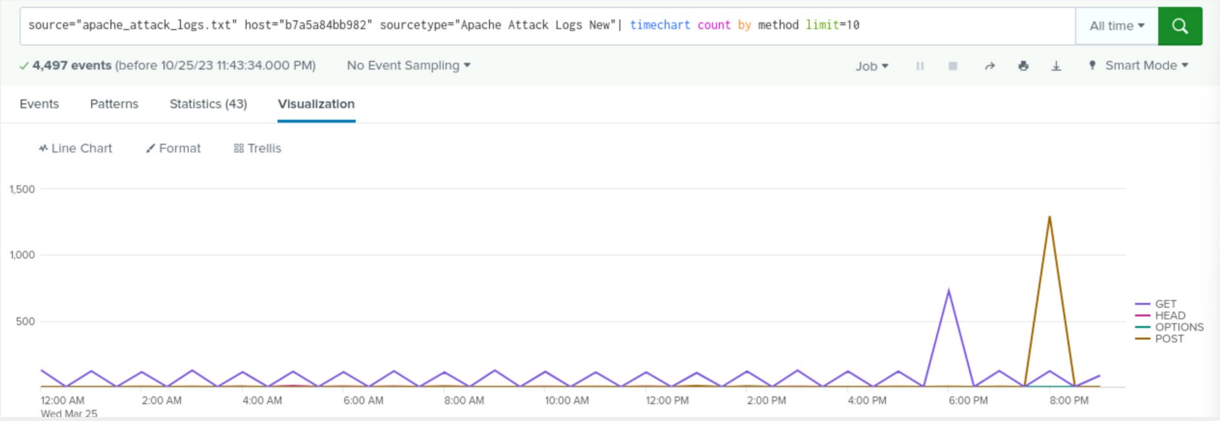


```
source="apache_attack_logs.txt" host="b7a5a84bb982" sourcetype="Apache Attack Logs New"
```

✓ **4,497 events** (before 10/25/23 11:41:25.000 PM)

- Which method seems to be used in the attack?

```
Post
```



```
source="apache_attack_logs.txt" host="b7a5a84bb982" sourcetype="Apache Attack Logs New"| timechart count by method limit=10
```

✓ **4,497 events** (before 10/25/23 11:43:34.000 PM) No Event Sampling ▾

- At what times did the attack start and stop?

```
From about 5:30 - 8:30
```

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

```
1,296 for Post
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Yes, there are major clusters in the US and Eastern Europe
```

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

```
Ashburn VA, United States
```

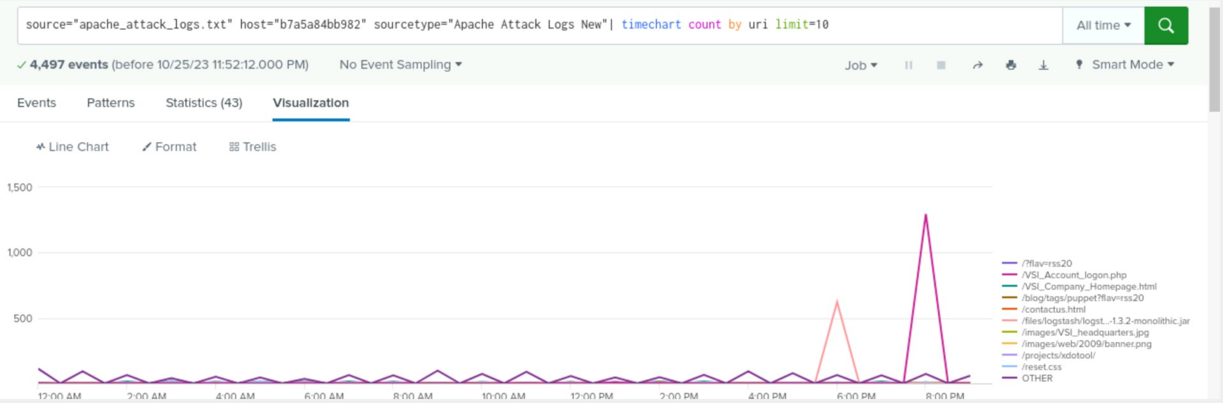
- What is the count of that city?

```
668
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes, there are corresponding spikes to when we see the HTTP requests:
```



```
source="apache_attack_logs.txt" host="b7a5a84bb982" sourcetype="Apache Attack Logs New"| timechart count by uri limit=10
```

✓ 4,497 events (before 10/25/23 11:52:12.000 PM)

- What URI is hit the most?

```
/VSI_Account_logon.php:
```

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

```
This could be a Brute Force attack with the attacker trying to access secure
data with different usernames and passwords.
```