



# Cybersecurity

## Project 3 Review Questions

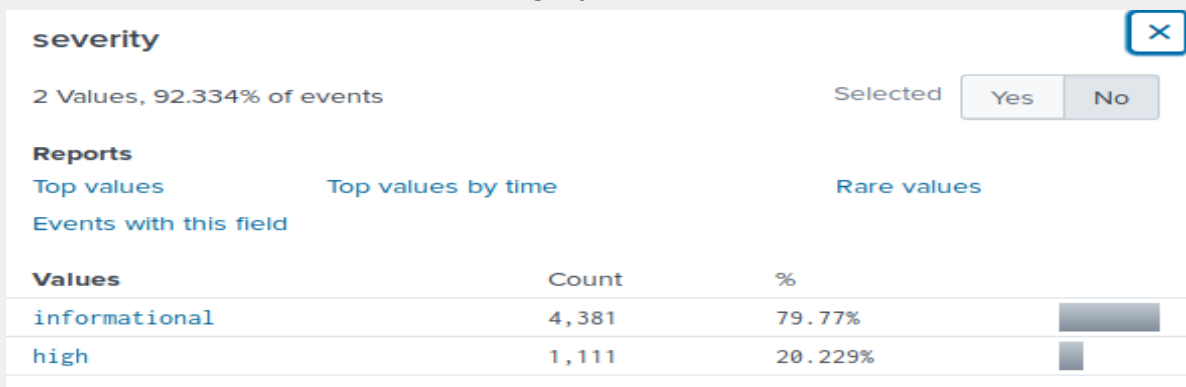
Make a copy of this document before you begin. Place your answers below each question.

### Windows Server Log Questions

#### Report Analysis for Severity

- Did you detect any suspicious changes in severity?

Yes, severity levels in the “high” category increased from 6% to 20%, and the level of “informational” category decreased from 93% to 79%



top severity

All time

✓ 4,761 events (before 12/1/22 3:59:38.000 PM)

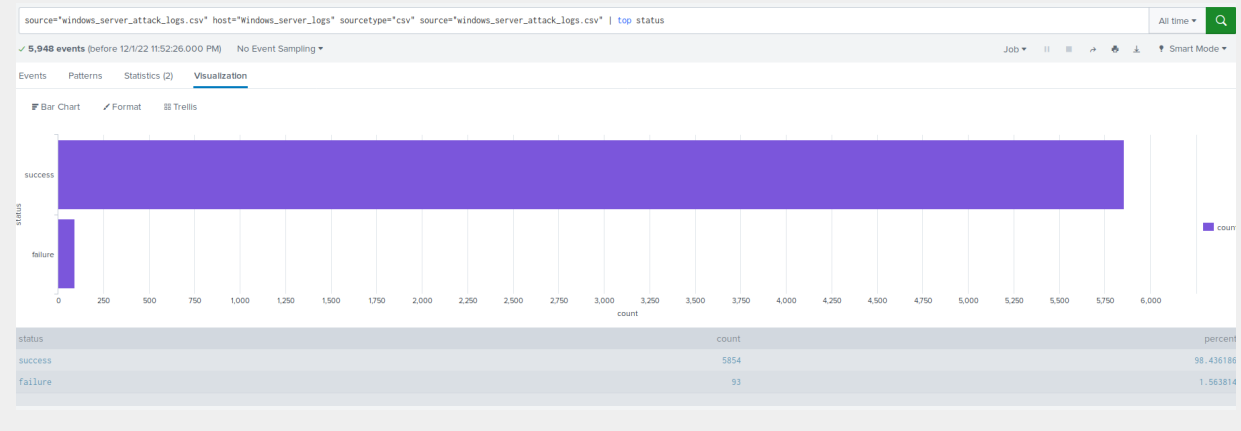
2 results      20 per page

| severity      | count | percent   |
|---------------|-------|-----------|
| informational | 4429  | 93.085330 |
| high          | 329   | 6.914670  |

#### Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

Yes, there were more successes than failures after the attack



## 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

- When did it occur?

At 8 am, March 25, 2020



- Would your alert be triggered for this activity?

Yes. It exceeded our threshold

- 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?

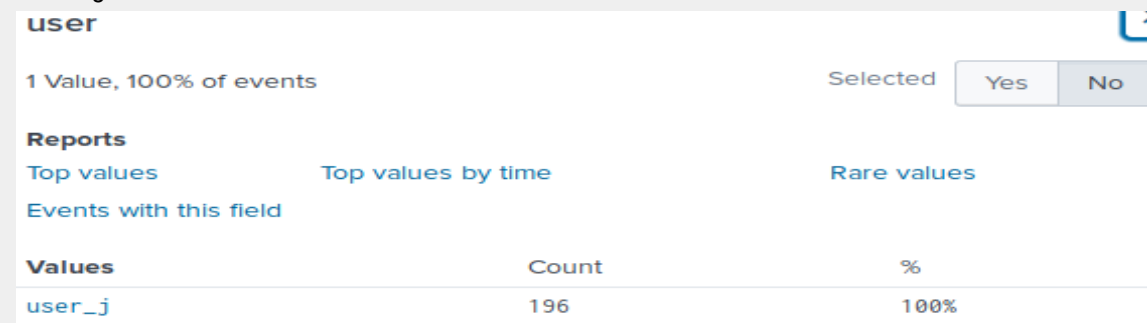
Yes

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

196 events

- Who is the primary user logging in?

User\_j

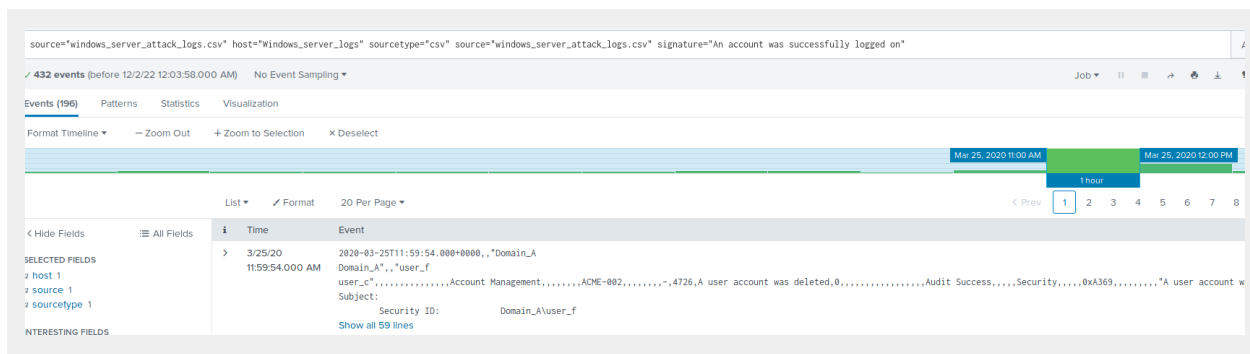


The screenshot shows a security dashboard interface. At the top, it displays 'user\_j' and 'user'. Below this, it indicates '1 Value, 100% of events' and has a 'Selected' dropdown menu with 'Yes' and 'No' options. Under the 'Reports' section, there are three links: 'Top values', 'Top values by time', and 'Rare values'. Below these links, there is a table titled 'Events with this field'.

| Values | Count | %    |
|--------|-------|------|
| user_j | 196   | 100% |

- When did it occur?

11 am, March 25, 2020



- Would your alert be triggered for this activity?

Yes, It exceeded our threshold of 10

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

Yes, we would increase our threshold from 10-25

## Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

No, we didn't, because our threshold was set to >25

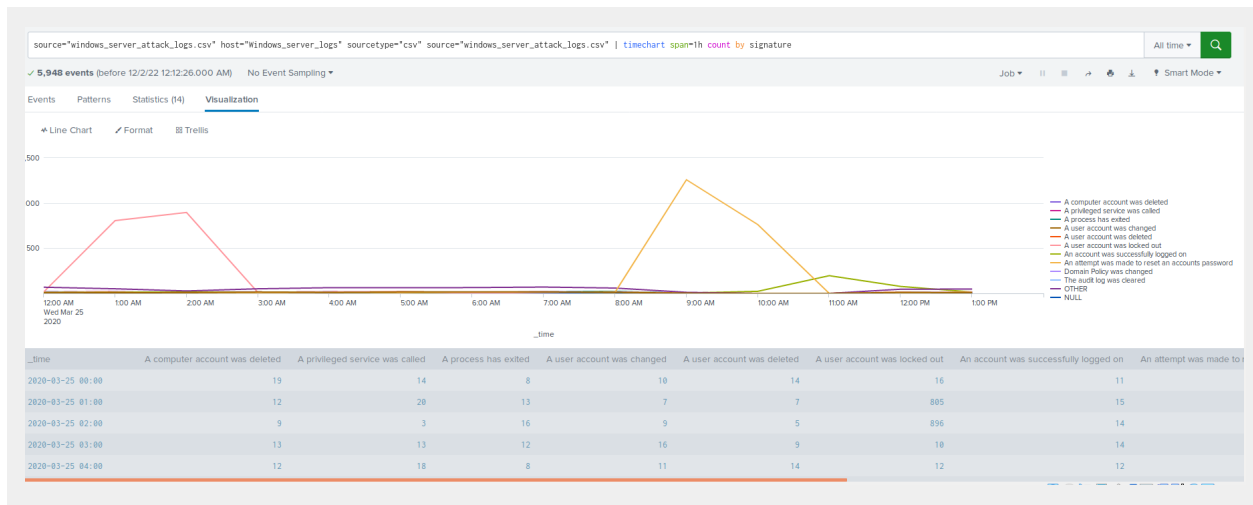
## Dashboard Analysis for Time Chart of Signatures

- 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 accounts password"



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

“A user account was locked out”- started at 1am and stopped 2 am  
 “An attempt was made to reset an accounts password” - started at 9am and stopped at 11 am

- What is the peak count of the different signatures?

The peak for “A user account was locked out”-896  
 The peak for “An attempt was made to reset an accounts password” -1,258

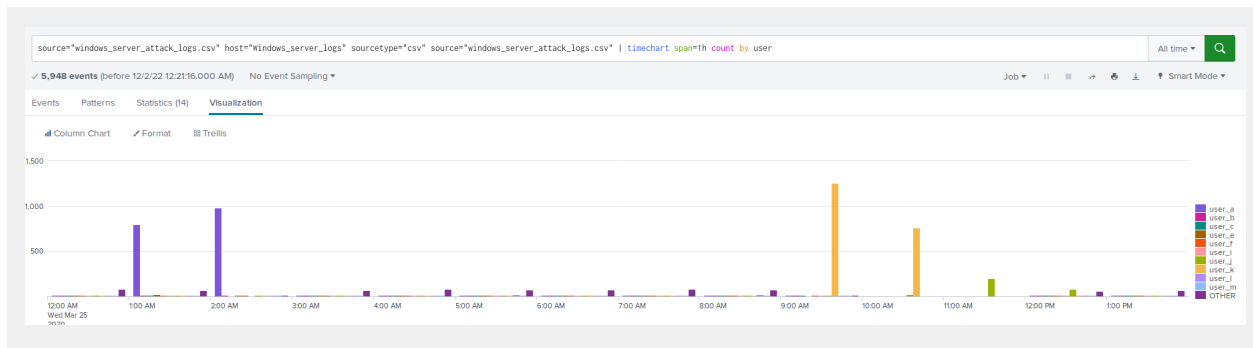
## Dashboard Analysis for Users

- Does anything stand out as suspicious?

Yes

- Which users stand out?

User\_a and User\_k



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

For the user\_a it started at 1:15am and stopped at 2:15am  
 For the user\_k it started at 9:40am and stopped at 10:40am

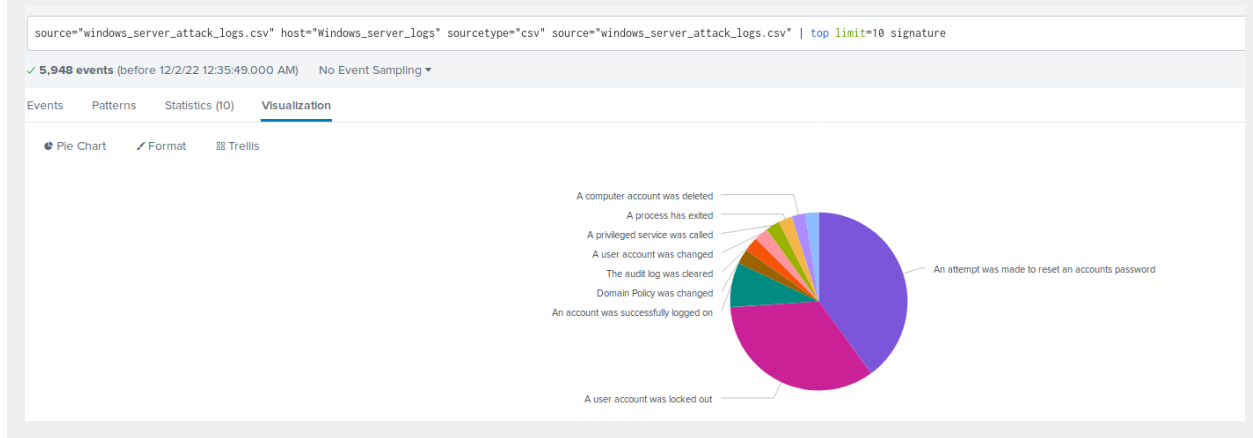
- What is the peak count of the different users?

User\_a - 984  
 User\_k - 1256

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

- Does anything stand out as suspicious?

Yes, it does



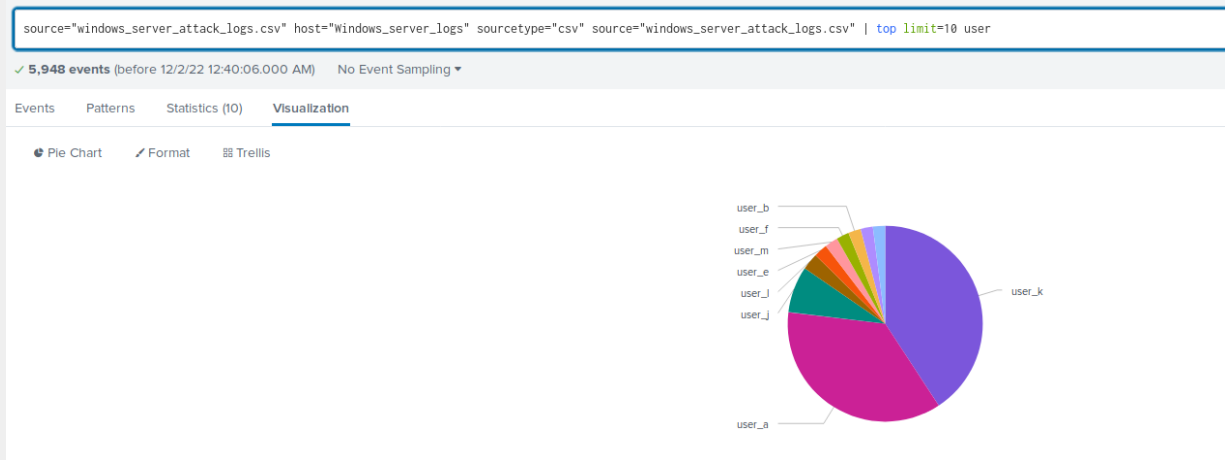
- Do the results match your findings in your time chart for signatures?

Yes

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

- Does anything stand out as suspicious?

Yes



- 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?

An advantage is that it is very easy to see outliers and which user it was right away. A disadvantage would be that we cannot see the time and how long each attack took place for on the bar graph, only the line graph shows it.

## Apache Web Server Log Questions

### Report Analysis for Methods

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

Yes, level of the POST increased from 1% to 29%; level of the GET decreased from 98% to 70%

diff HTTP methods

All time

✓ 10,000 events (before 12/1/22 4:49:00.000 PM)

Job

| method  | count | percent   |
|---------|-------|-----------|
| GET     | 9851  | 98.510000 |
| POST    | 106   | 1.060000  |
| HEAD    | 42    | 0.420000  |
| OPTIONS | 1     | 0.010000  |

source="apache\_attack\_logs.txt" host="apache\_attack\_logs" sourcetype="access\_combined" | top method

✓ 4,497 events (before 12/2/22 12:44:40.000 AM) No Event Sampling

Job

Events Patterns **Statistics (4)** Visualization

20 Per Page Format Preview

| method  | count | percent   |
|---------|-------|-----------|
| GET     | 3157  | 70.282357 |
| POST    | 1324  | 29.441850 |
| HEAD    | 15    | 0.333556  |
| OPTIONS | 1     | 0.022237  |

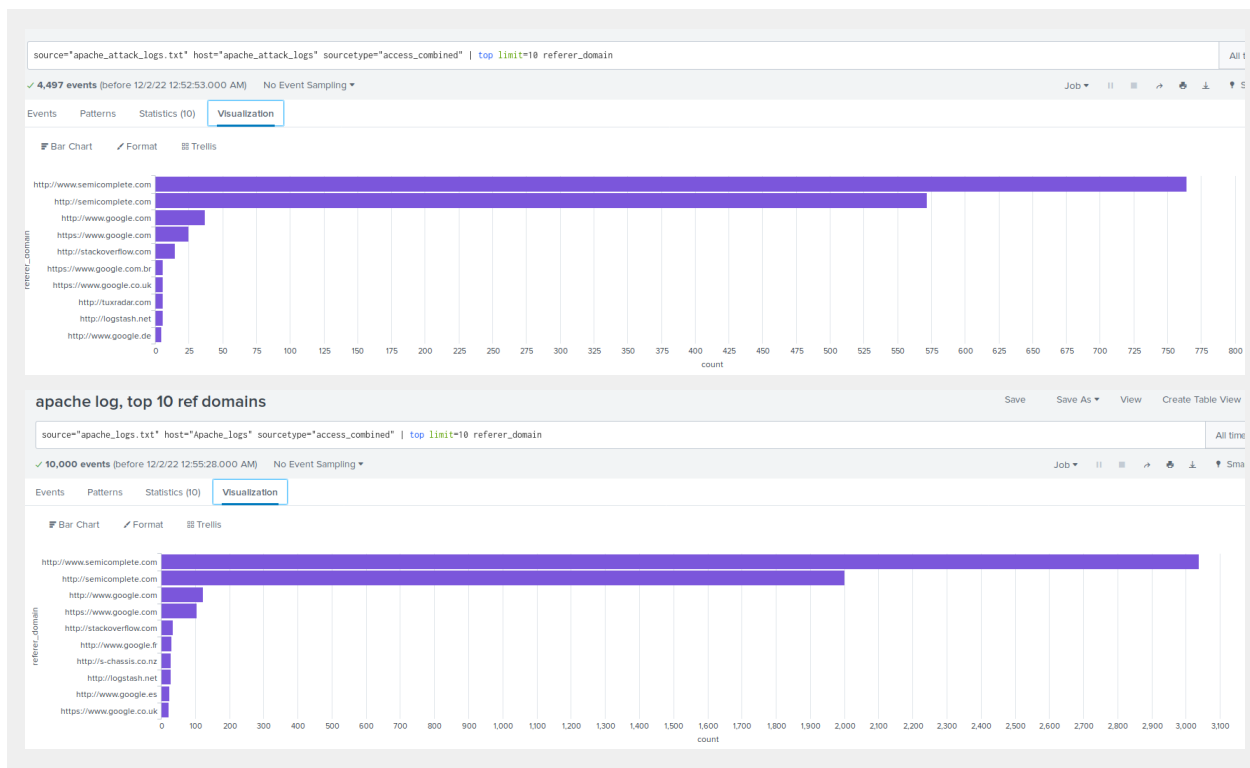
- What is that method used for?

The GET method used to retrieve data, and the POST method used to send data to a server to create or update a resource.

## 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, Code “404” increased from 2% to 15% and code “200” decreased from 91% to 83%

source="apache\_attack\_logs.txt" host="apache\_attack\_logs" sourcetype="access\_combined" | top status

4,497 events (before 12/2/22 12:58:39.000 AM) No Event Sampling

Events Patterns Statistics (7) Visualization

20 Per Page Format Preview

| status | count | percent   |
|--------|-------|-----------|
| 200    | 3746  | 83.299978 |
| 404    | 679   | 15.098955 |
| 304    | 36    | 0.800534  |
| 301    | 29    | 0.644874  |
| 206    | 5     | 0.111185  |
| 500    | 1     | 0.022237  |
| 403    | 1     | 0.022237  |

source="apache\_logs.txt" host="Apache\_logs" sourcetype="access\_combined" | top status

10,000 events (before 12/2/22 12:59:40.000 AM) No Event Sampling

Events Patterns Statistics (8) Visualization

20 Per Page Format Preview

| status | count | percent   |
|--------|-------|-----------|
| 200    | 9126  | 91.260000 |
| 304    | 445   | 4.450000  |
| 404    | 213   | 2.130000  |
| 301    | 164   | 1.640000  |
| 206    | 45    | 0.450000  |
| 500    | 3     | 0.030000  |
| 416    | 2     | 0.020000  |
| 403    | 2     | 0.020000  |

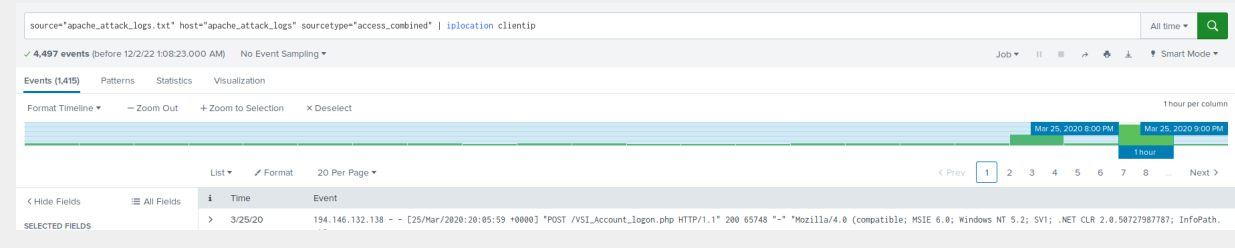
## Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

Yes

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

Between 8pm and 9pm



- Would your alert be triggered for this activity?

Yes

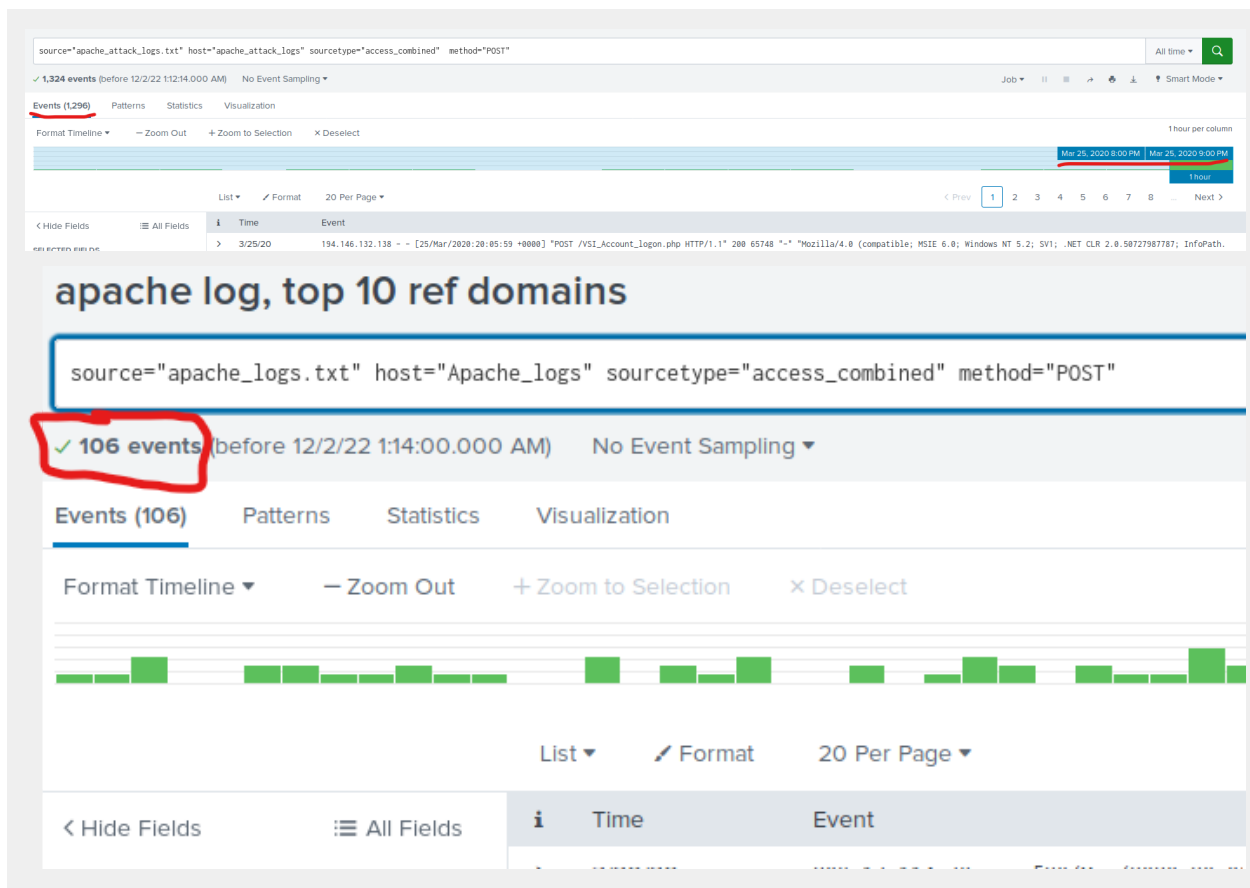
- After reviewing, would you change the threshold that you previously selected?

No our threshold was accurate

## Alert Analysis for HTTP POST Activity

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

Yes, from 106 events it is increased to 1296



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

Between 8pm-9pm

- When did it occur?

March 25, 2020

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

No, our threshold was accurate

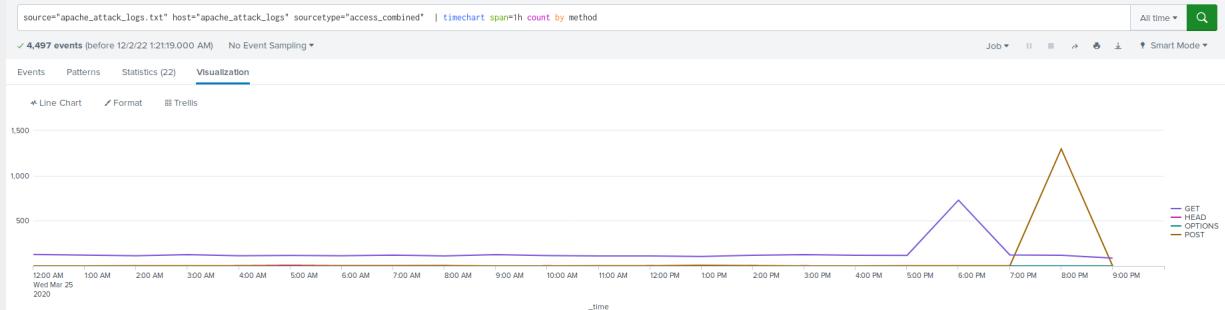
## Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

Yes

- Which method seems to be used in the attack?

## POST and GET



- At what times did the attack start and stop?

GET (attack started at 5pm and stopped at 7pm)

POST (attack started at 7pm and stopped at 9 pm)

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

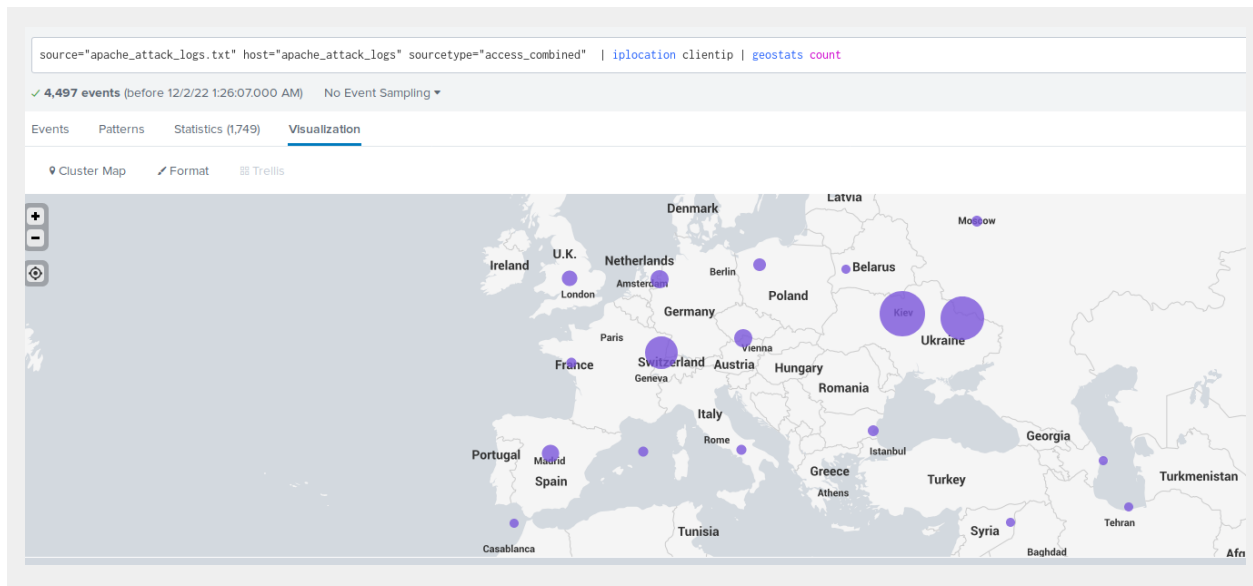
POST (1,296)

GET (729)

## Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

Yes



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

-the city of Washington D.C, United States  
 -the city of NYC, United States  
 -the city of Kiev, Ukrain  
 -the city of Kharkiv, Ukrain  
 -the city of Strasbourg,France

- What is the count of that city?

-the city of Washington D.C - 714  
 -the city of NYC - 549  
 -the city of Kiev - 439  
 -the city of Kharkiv - 433  
 -the city of Strasbourg - 84

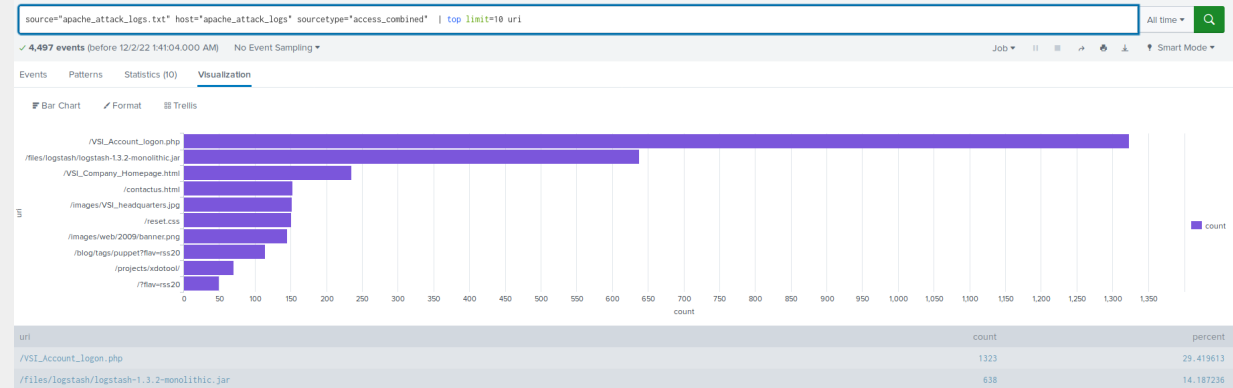
## Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

Yes

- What URI is hit the most?

## /VSI\_Account\_logon.php



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

## A Brute Force Attack