Cybersecurity

Project 3 Review Questions

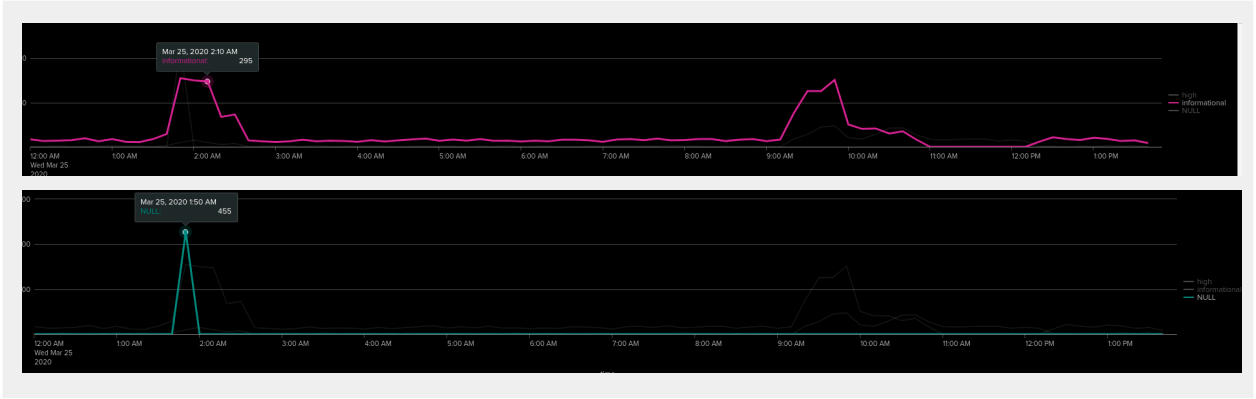
Make a copy of this document before you begin. Place your answers below each question.

Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

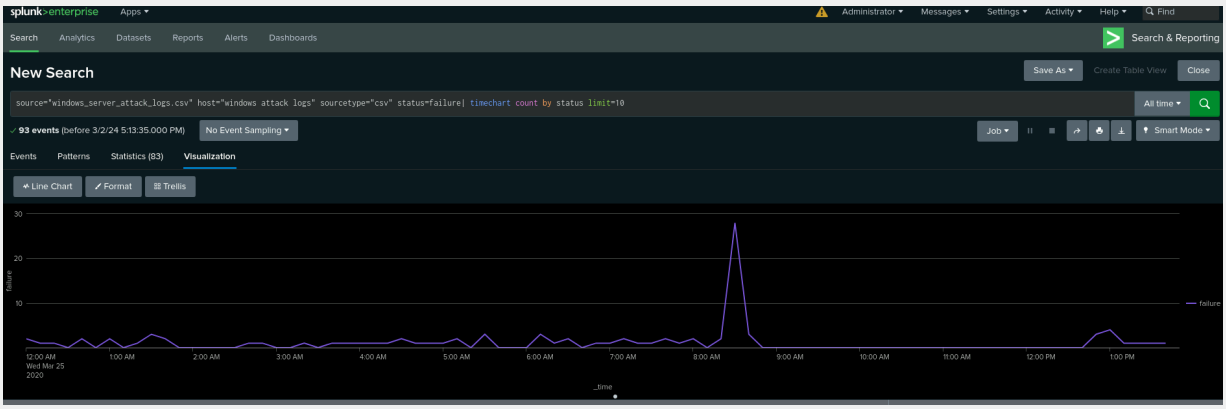
Yes, Severity of Null at 455 counts at 1:50am, we also found Informational count at 295.



Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

Yes, we observed an attack at 8 am, with a count of 28 logins.



Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes the count was at 28
```

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

```
28
```

- When did it occur?

```
Between 8:20am to 8:40pm
```

- Would your alert be triggered for this activity?

```
Yes, because threshold was set at 8
```

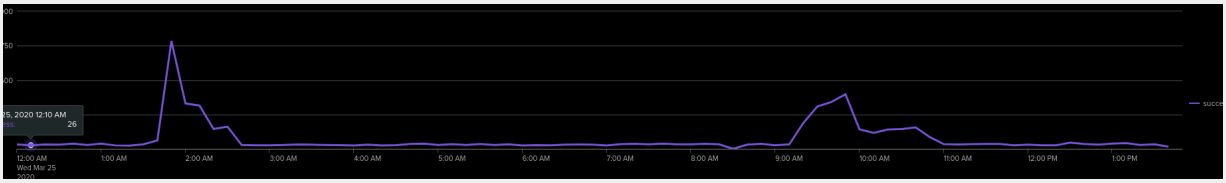
- After reviewing, would you change your threshold from what you previously selected?

```
No, I think 8 is a good threshold
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

Yes, there were two suspicious successful logins.



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

```
1.)    At 1:50 am =785, 2:00am =330, at 2:10am = 315, at 2:20am =
   145,2:30am = 161
2.)    At 9:10am at 33, 9:30am at 308, at 9:50 am at 397, at 10:00am at
   142,at 10:50 at 86
```

- Who is the primary user logging in?

```
User A and user K
```

- When did it occur?

```
User A occur starting at 1:40 to 2:40, User K 9:10 to 11:00
```

- Would your alert be triggered for this activity?

```
Yes
```

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

```
No
```

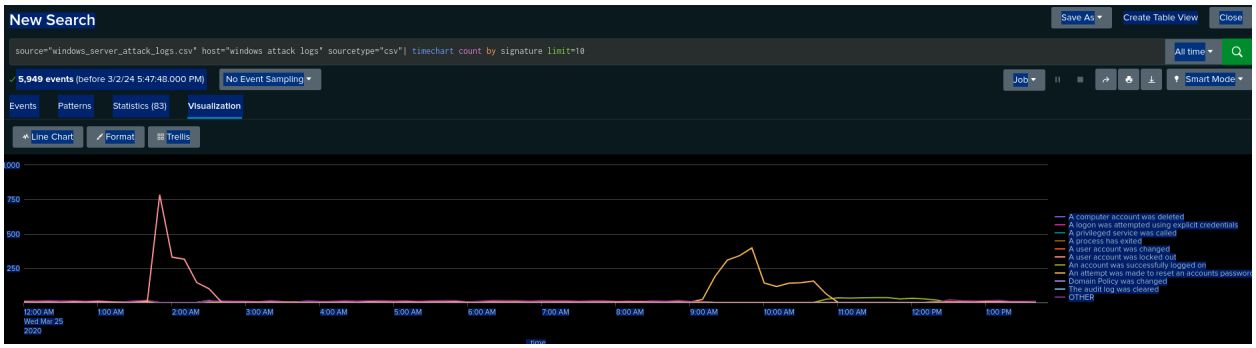
Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
No because my threshold was set to 16, and it doesn't exceed that threshold
```

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 password
```

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

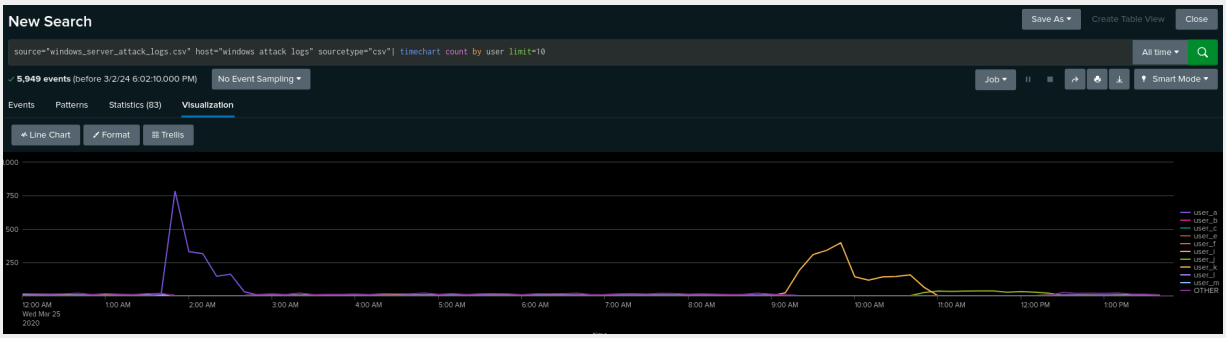
```
1:40 to 2: 40 & 9:10 to 11:00
```

- What is the peak count of the different signatures?

```
An attempt was made to reset an account passport at 397 and a user account was locked out at 785
```

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?

```
It began from 1:40 to 2:40 for user A & 9:10 to 11:00 for user K
```

- What is the peak count of the different users?

```
An attempt was made to reset an account passport at 397 and a user account
was locked out at 785
```

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

- Does anything stand out as suspicious? **Yes**

- 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?

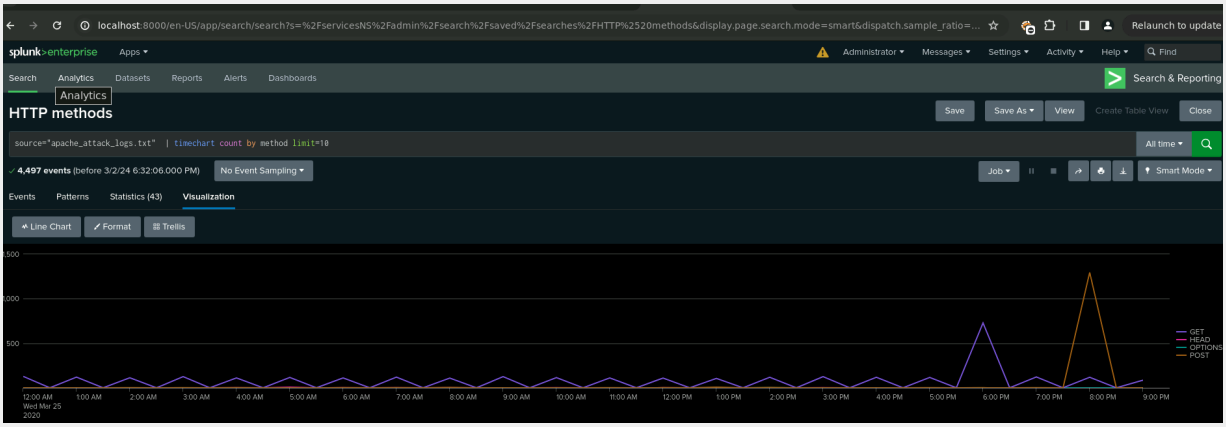
```
The user panels allow you to correlate and see the charts correlate with one another.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

Yes; the Get and Post



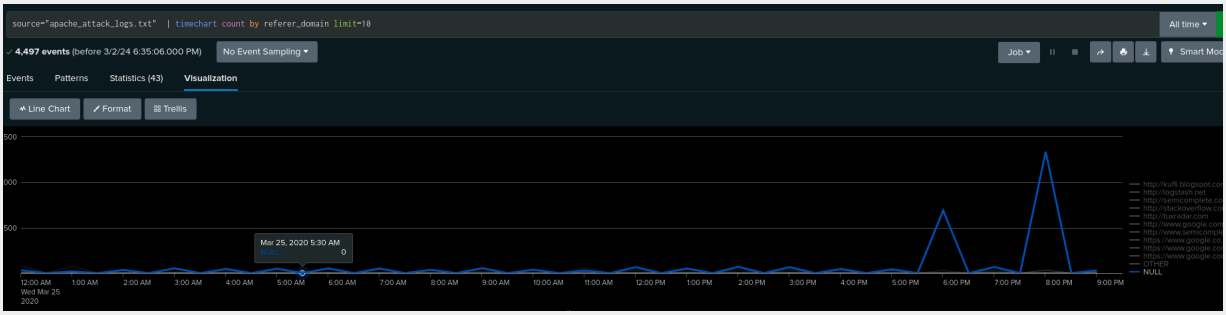
- What is that method used for?

```
Get method allows us to retrieve data from servers, and Post can be used to get data from other servers. Post method never caches data and also sends data along with requesting.
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

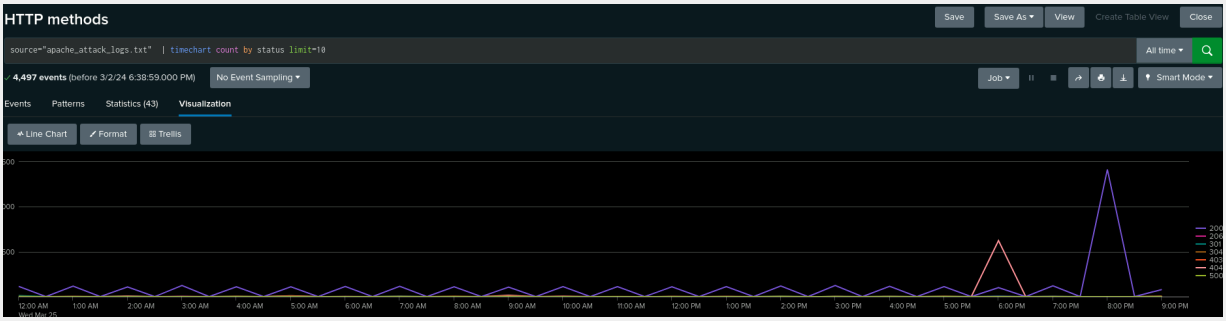
-Yes, its was Null



Report Analysis for HTTP Response Codes

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

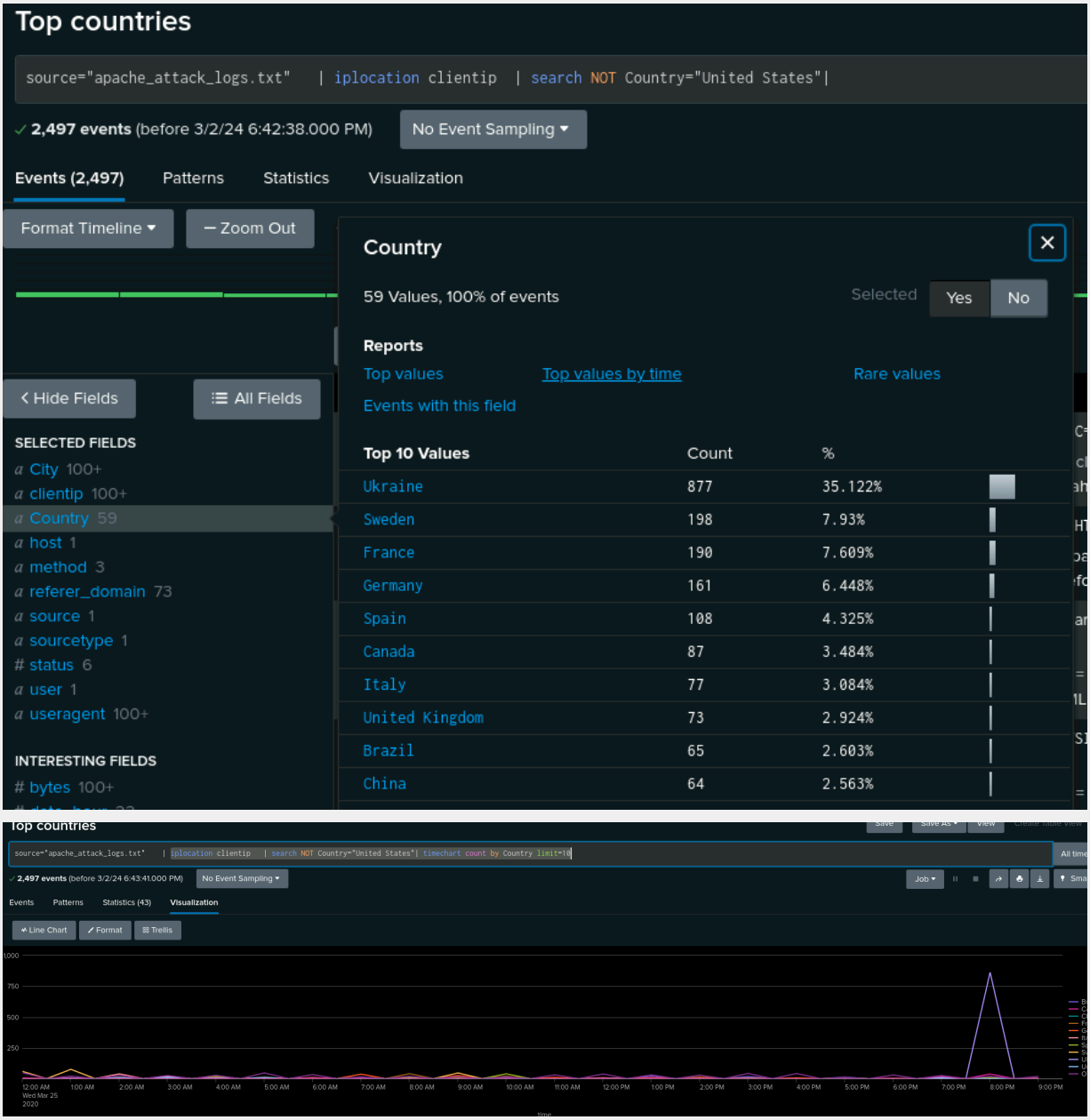
-Yes



Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

Yes, Ukraine from 7:30 to 8:30



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

`At 8pm it was at 864`

- Would your alert be triggered for this activity?

Yes

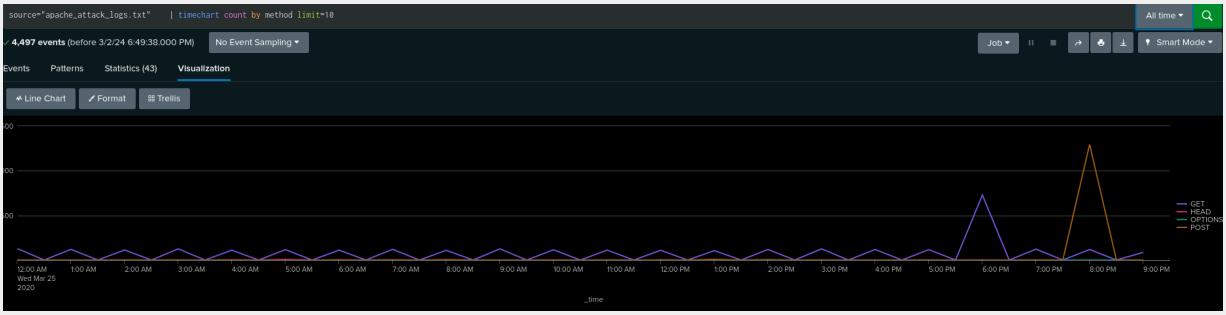
- After reviewing, would you change the threshold that you previously selected?

No

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?

From 7:30 to 8:30 at 1,297

- When did it occur?

March 25 at 8pm

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

no

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
Yes
```

- Which method seems to be used in the attack?

```
Get and Post
```

- At what times did the attack start and stop?

```
Yes, Get was from 6:30 to 7:30 and Post was from 7:30 to 8:30
```

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

```
Get 729 and Post at 1296.
```

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.)

```
New York and Washington DC USA & Kiev Ukraine
```

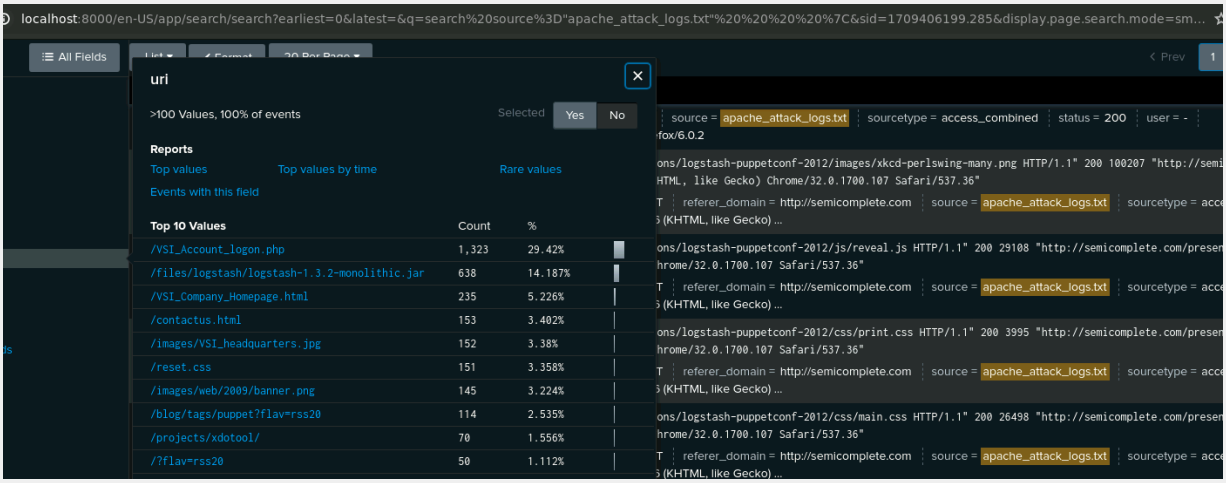
- What is the count of that city?

```
454 for Kiv, and 593 for New York and 724 for Washington
```

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?

```
Based on the URI access and Post request the attacker can potentially be
requesting a Brute force attack and its coming from Ukraine.
```