Cybersecurity

Project 3 Review Questions

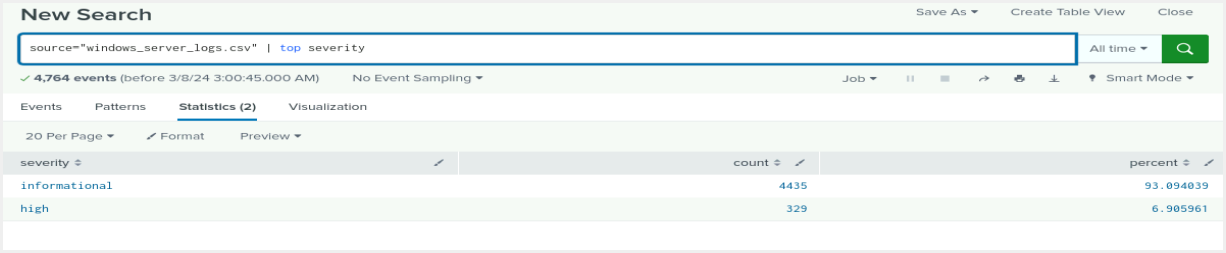
Make a copy of this document before you begin. Place your answers below each question.

Windows Server Log Questions

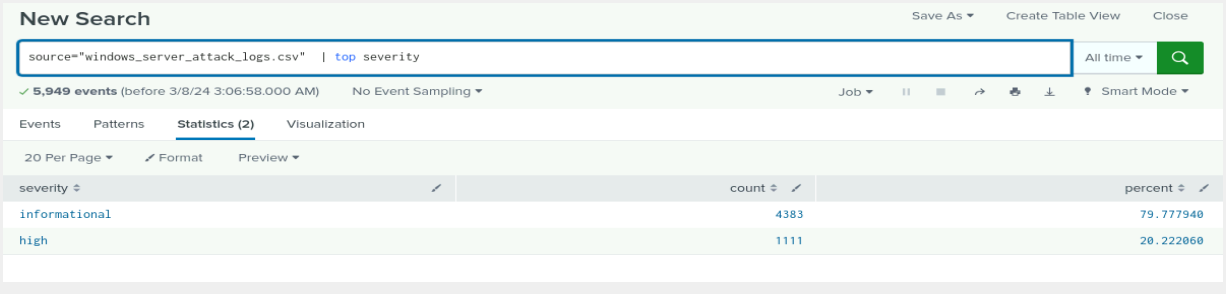
Report Analysis for Severity

- Did you detect any suspicious changes in severity?

Yes, from around 300 to 1100 HIGH severity events per day
Normal:



Attack:



Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
Yes, failure events spiked over 50/hr, though typically average 6/hr
Normal activity:
```


```
Suspicious Event:
```

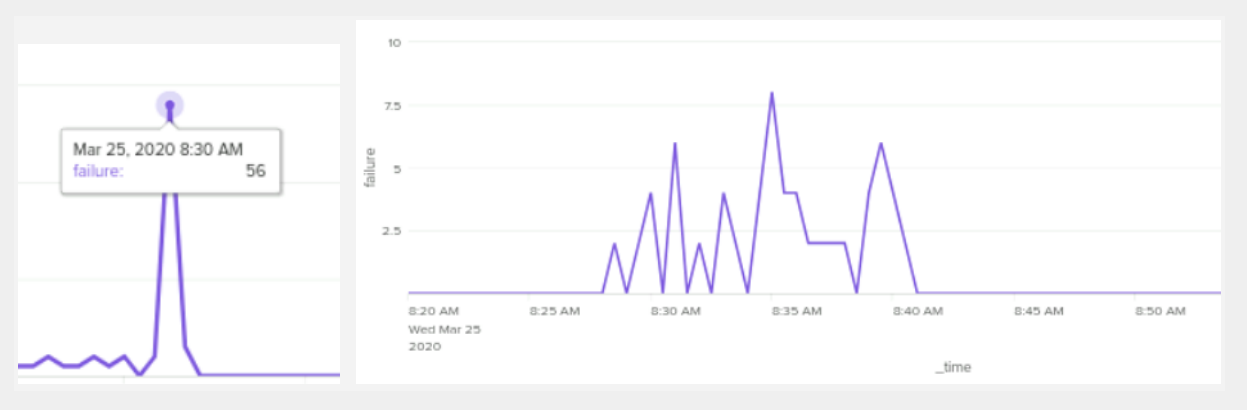
Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes. Failures spiked over 50/hr
```

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

```
The count of events at 8:00 am on 3-25-2020 was 50 failed Windows
activities, which is significantly higher than any other hour.
```



- Would your alert be triggered for this activity?

Yes, my alert would be triggered by this activity because the count of 50 is higher than my threshold of 12.

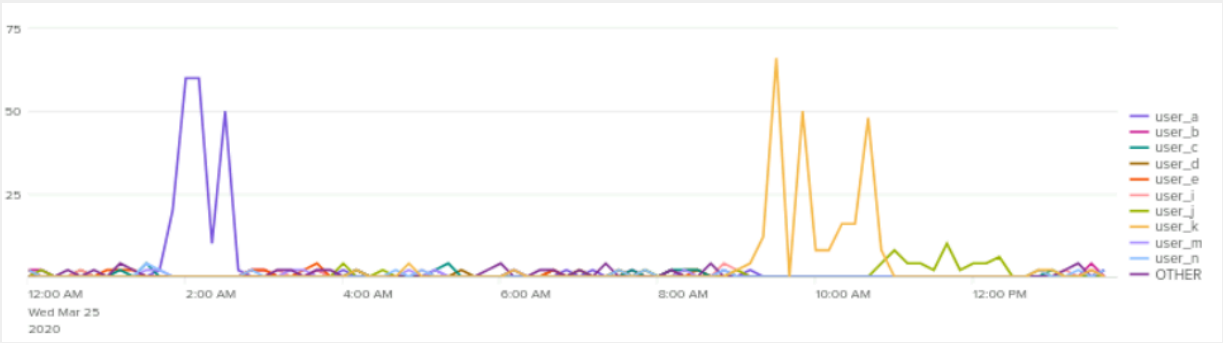
- After reviewing, would you change your threshold from what you previously selected?

No, I felt that our threshold was set correctly to prevent the SOC supervisor from overflowing with messages and still detecting outliners. Email would have triggered for only the 8 o'clock hour, so it seems appropriately placed.

Alert Analysis for Successful Logins

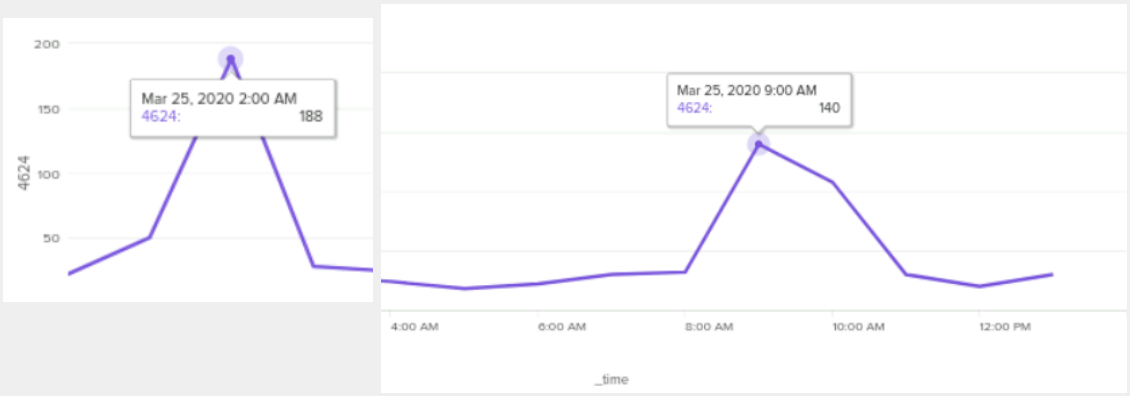
- Did you detect a suspicious volume of successful logins?

Yes, suspicious login activity occurred at 2am and 9-10am on March 25th. The activity of user_j around 11am-1pm the same day also stands out.



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

There were 188 logins around 2am and 140 and 108 for 9 and 10 am



The values of 30, 20 and 30 for the hours between 11 and 1 also seem high.

- Who is the primary user logging in?

The primary users logging on successfully were user_a at 2am, user_k at 9&10am, and user_j at noontime

- When did it occur?

March 25th, 2020

- Would your alert be triggered for this activity?

We set the alert to trigger at 30 successful logins, so it would have triggered for 2, 9 and 10am as well as 11am and 1pm. This might seem like a lot of alerts, but user_j being responsible for 30 logons alone at 11am makes me feel like its good we set the bar low enough to be alerted to this activity

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

No changes are necessary, but we might change the alert to count by user instead of counting totals, so we can set the threshold a little lower and make sure to be aware of events like those from 11-1pm.

Alert Analysis for Deleted Accounts

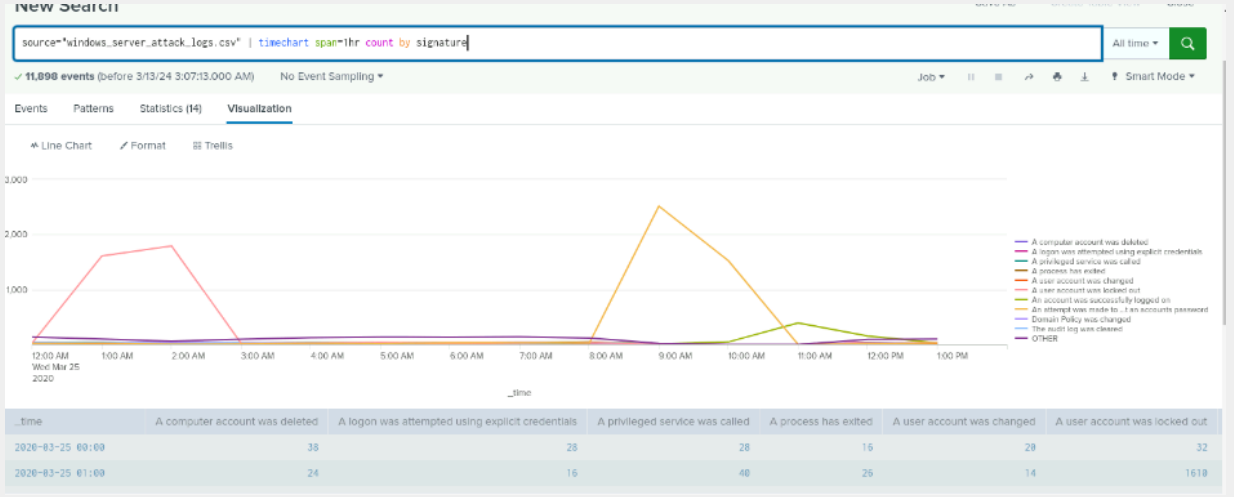
- Did you detect a suspicious volume of deleted accounts?

```
Yes, on the 25th of March at 9 am, there was a spike of 150 accounts deleted
in that hour.
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
Yes there were some suspicious activities, first user lockouts (pink), then
password reset attempts (gold), and lastly a total count of logins (green)
```



- What signatures stand out?

```
First user account lockouts are shown in pink above, then password reset
attempts in gold, and lastly a total count of successful logins in green.
```

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

```
For the signature “a user account was locked out” had a spike from 12 am to
3 am and the signature “an attempt was made on a user account.” had a spike
from 8 am to 11 am.
```

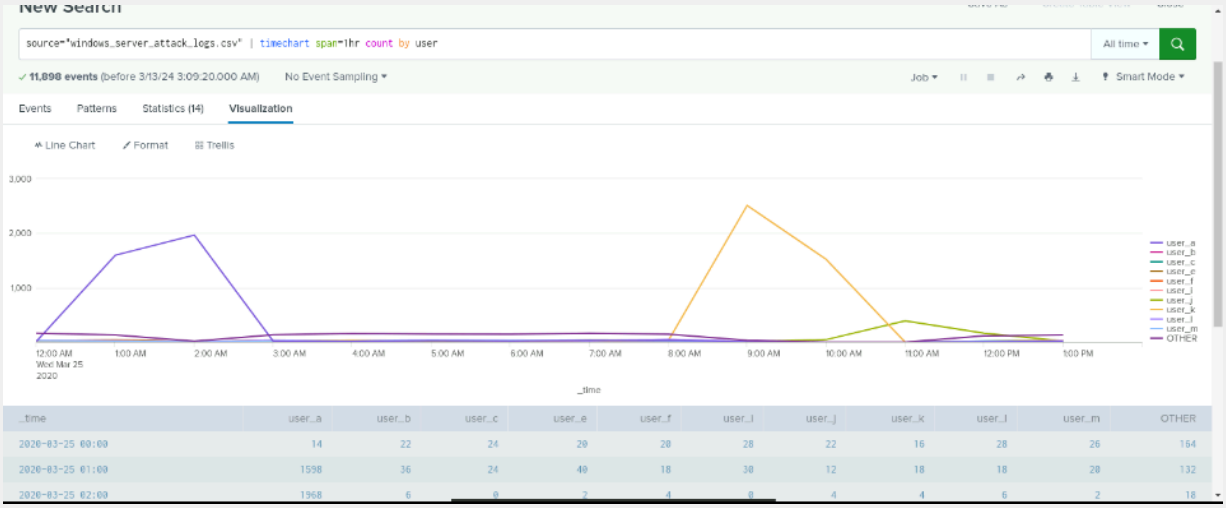
- What is the peak count of the different signatures?

```
The peak for each signature are as follows “a user account was locked out” peaked at 1,792 activities and the signature for “an attempt was made on a user account.” peaked at 2,516 activities. There was also a peak of successful logons at 392 activities.
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

Yes



- Which users stand out?

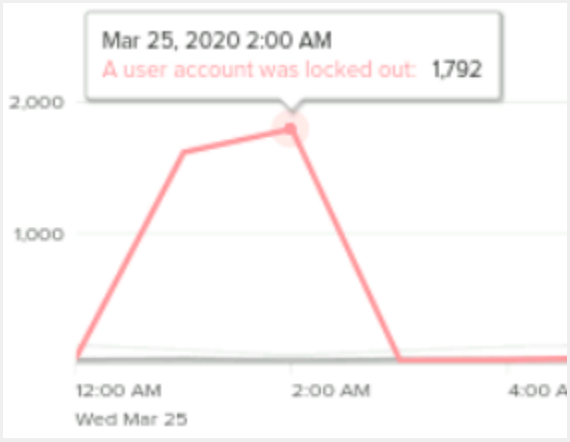
```
User_a and user_k mostly, also somewhat user_j
```

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

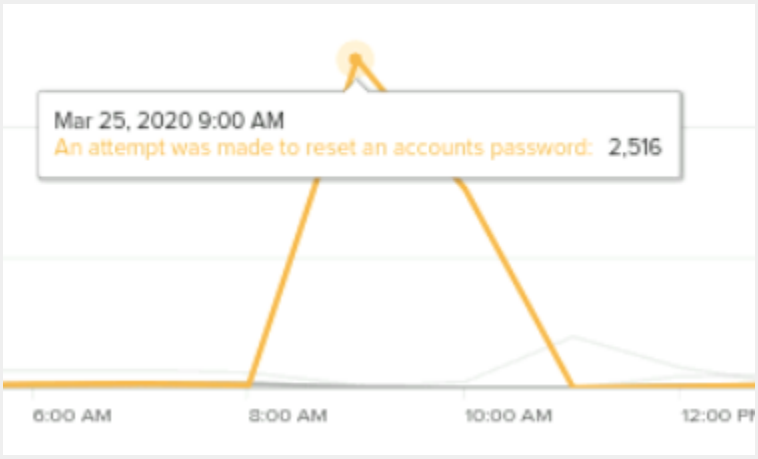
```
Between 1:00 am to 2:30 am, User_a had increased in activity
Between 9:00 am to 10:00 am, User_k had increased in activity
Between 11:00 am and 1:00 pm, User_j had increased in activity
Both were on March 25th, 2020
```

- What is the peak count of the different users?

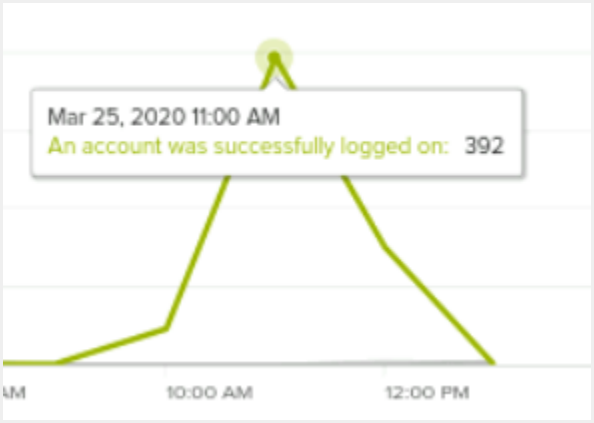
User_a peaked at 1,792 at 2 am



User_k peaked at 2,510 (six events were not user_k) at 9 am



User_j peaked at 392/hr at 11am



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

- Does anything stand out as suspicious?

```
Yes, there is a very significant increase in two signature types: an attempt
was made to reset an account password and a user account was locked out.
```

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

```
Yes they do match.
```

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

- Does anything stand out as suspicious?

```
Yes, when you look at the graph, you can see increased activity from user_a,
user_k, and user_j.
```

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

```
Yes, it did match our findings in the time chart for users.
```

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 of using a statistical time chart for signatures and users is
that we can quickly find the count for each event and user per hour. The
only disadvantage of using these over the bar graph and pie chart is that it
isn't obvious where there was a change in activity.
```

Apache Web Server Log Questions

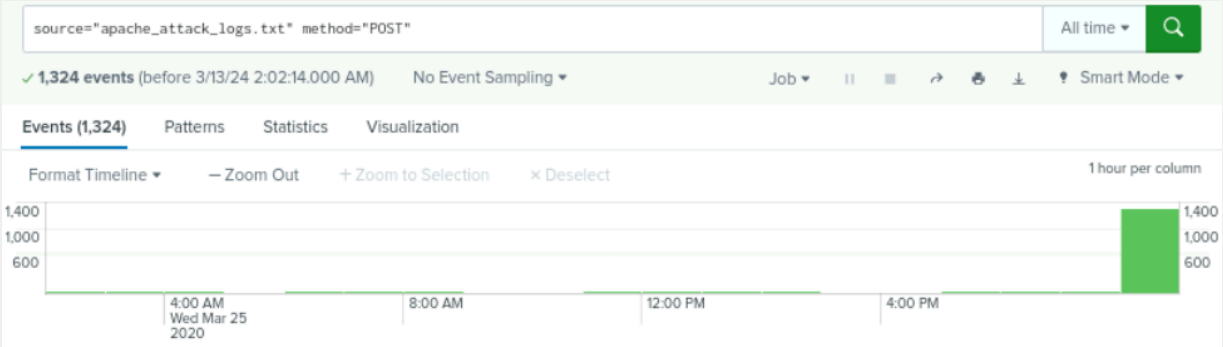
Report Analysis for Methods

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

Yes, activity during a normal day reaches around 10,000 connections with 98% of those being GET, POST making up only 1% of them. However, on 5/25/2020 we see out of 4,497 events 1,324 of them were POST requests. This makes up almost 30% of events for the day as well as a 12.5x increase from the normal percentage. Additionally, these POSTs all took place during the same *second*, at 8:05:59.

- What is that method used for?

POST requests are used to send data to a server. These can be used maliciously to slow down/stop a server in a DOS attack, and when a lot occur in a short time frame can be used to identify potential brute force attacks.

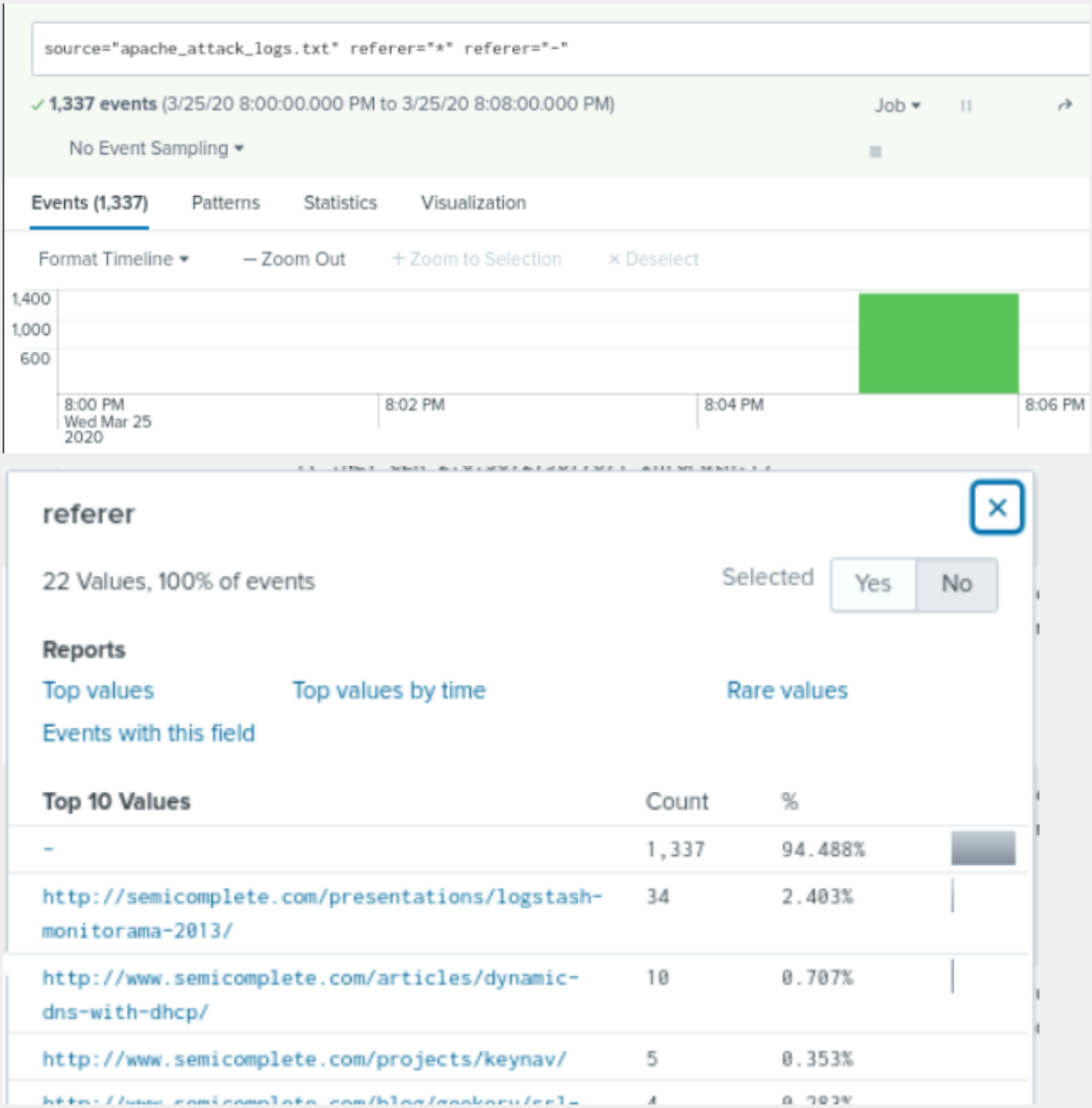


Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

There was nothing overtly suspicious in the domains during the attack. Although there is a new website that appears in the referrer domains, the requests are very low as to not be of note.

During the spike in POST activity, the vast majority of events list “-” (hyphen) as the value of the ‘referer’ field.



Report Analysis for HTTP Response Codes

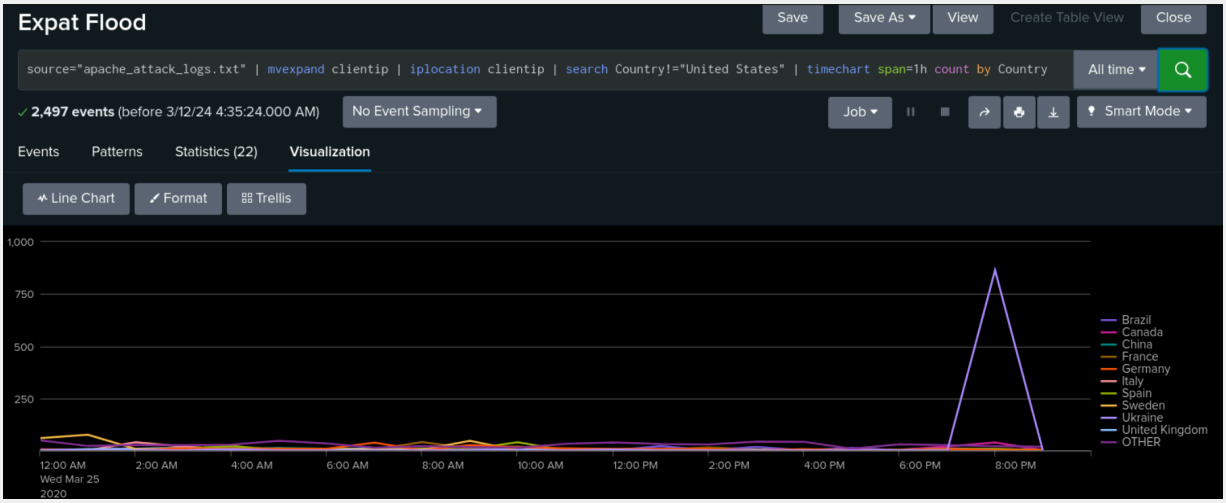
- Did you detect any suspicious changes in HTTP response codes?

There was a 2.5x increase in 404 requests during the time of the attack which would coincide with the increase in POST requests that were also occurring. Typically a failed post request is returned as a 404 error.

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?

Ukraine had a peak of 864 events in an hour

- Would your alert be triggered for this activity?

Yes, we set the threshold to 150 while during the attack Ukraine peaked at 864.

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

No changes are necessary.

Alert Analysis for HTTP POST Activity

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

Yes, the total number of post requests went from 106 to 2,648.

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

```
2,592 post requests occurred between 8 and 9pm, specifically 8:05:59
```

- When did it occur?

```
These requests occurred March 25th, 2020
```

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

```
With the threshold set to 15 we would have caught the attack while still
being well above the baseline of 3 per hour, so no changes are necessary.
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
Yes, there was suspicious activity in the HTTP method time charts in the
method “POST” from 8:00 p.m. on Wednesday, March 25th.
```

- Which method seems to be used in the attack?

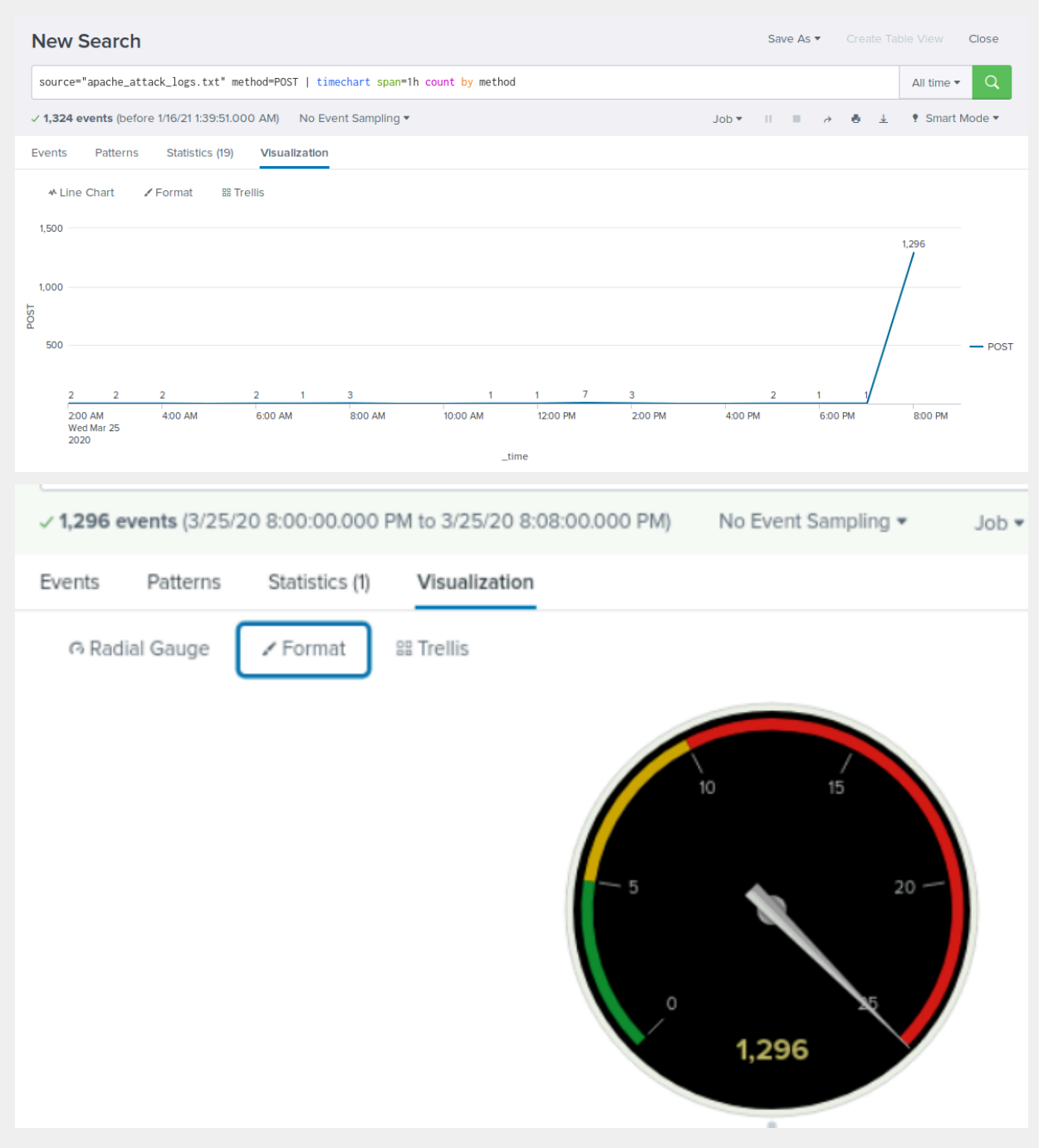
```
POST was the method used in the attack.
```

- At what times did the attack start and stop?

```
It appears to have occurred at 8:05:59 pm
```

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

```
The peak count was 1296
```

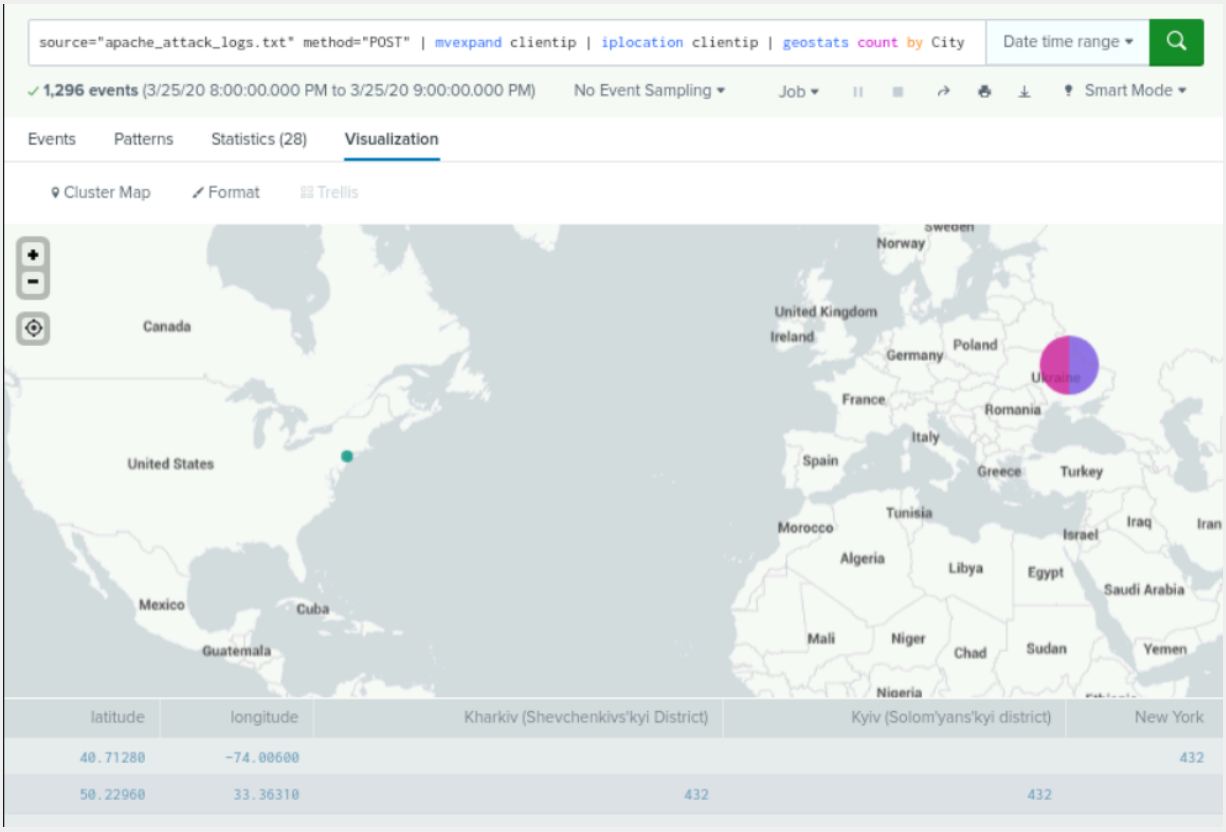


Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Yes, There is suspicious activity in the country of Ukraine, especially in
the cities of KIEV and Kharkiv, as well as a flood of POST requests from New
```

York City. Out of 1,296 POST events from exactly 8:05:59 pm, these attribute to 432 events each coming from clientip: 194.105.145.147, 194.146.132.138, and 79.171.127.34. This single second of exclusively POST events makes up more than 91% of all activity between 8 and 9 pm, and can be geolocated to Kharkiv, Kiev, & New York, NY.



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

Kyiv (Solom'yans'kyi dist.) & Kharkiv (Shevchenkivs'kyi dist.) in Ukraine, and New York, NY all had an increase in activity.

- What is the count of that city?

Kyiv: 432
Kharkiv: 433
New York: 440

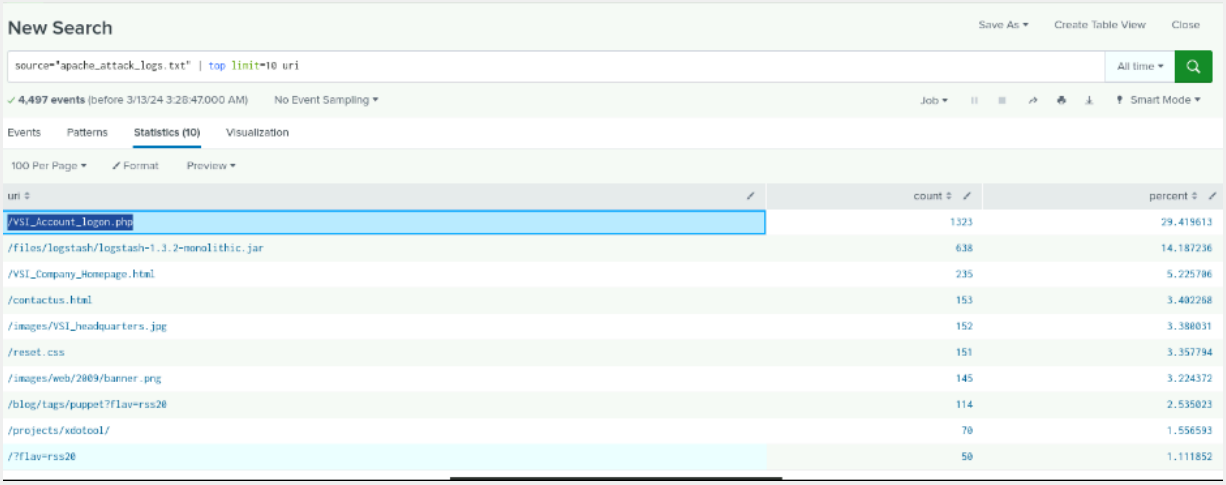
Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

There was suspicious activity with the URI “/files/logstash/logstash-1.3.2-monolithic.jar” from 6:00 p.m. to 7:00 p.m. on Wednesday, March 25th and with the URI “/VSI_Account_logon.php” from 8:00 p.m. to 9:00 p.m. on Wednesday, March 25th.

- What URI is hit the most?

/VSI_Account_logon.php was hit the most with 1323 hits from that URI



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

Based on the URI being accessed, the attacker could be trying to brute force attack or SQL injections on the VSI login page.