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, High severity went from a count of 329 and 6.914% up to a count of 1111
and 20.229%.
```

2 results 20 per page

	severity	count	percent
1	informational	4429	93.085330
2	high	329	6.914670

	severity	count	percent
1	informational	4381	79.770575
2	high	1111	20.229425

Report Analysis for Failed Activities

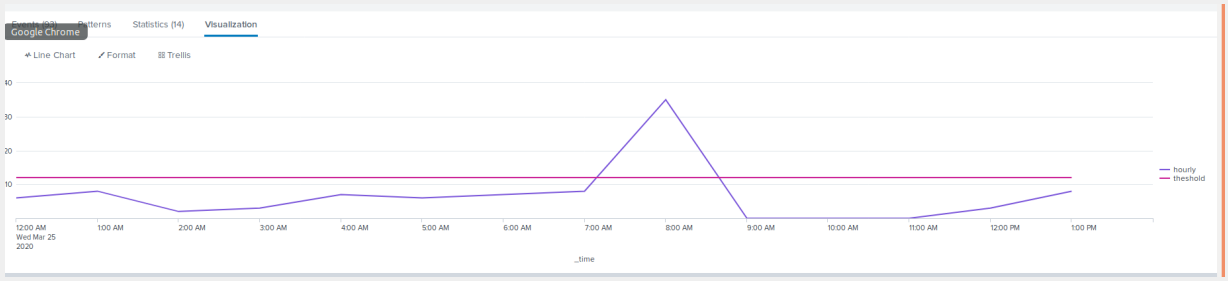
- Did you detect any suspicious changes in failed activities?

```
Yes, there was a spike in failed activity and 3 large spikes in successful
activity
```

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

```
Yes. There was a 5X increase in failed activity from average usage at 08:00 25/3/20 resulting in 35 failed activities. The threshold for alert is set at 12.
```



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

```
35
```

- When did it occur?

```
08:00 25/03/2020
```

- Would your alert be triggered for this activity?

```
Yes, Threshold is set at 12
```

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

```
No.
```

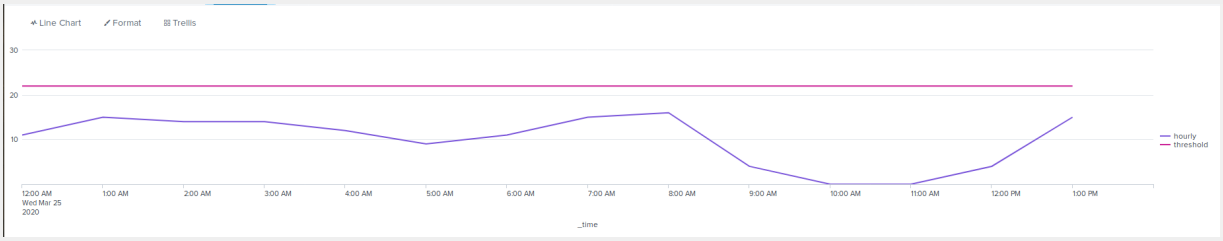
Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

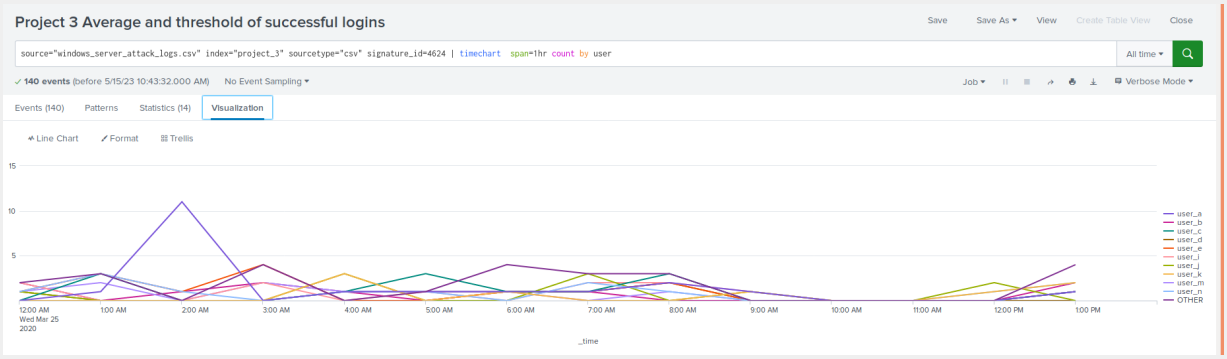
```
Yes
```

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

We know a large number of failed activities took place at 08:00 and there was a steep decline in successful logins after that.
09:00 returned 4, 10:00 returned 0, 11:00 returned 0 and 12:00 returned 4.

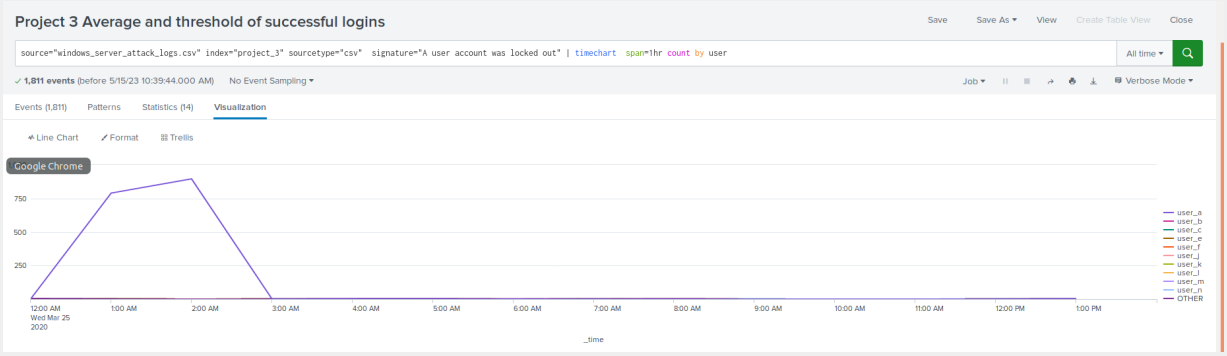


However when interpreting the logs sorted by user it shows an odd instance where user_a has a deviation from normal activity at 02:00.

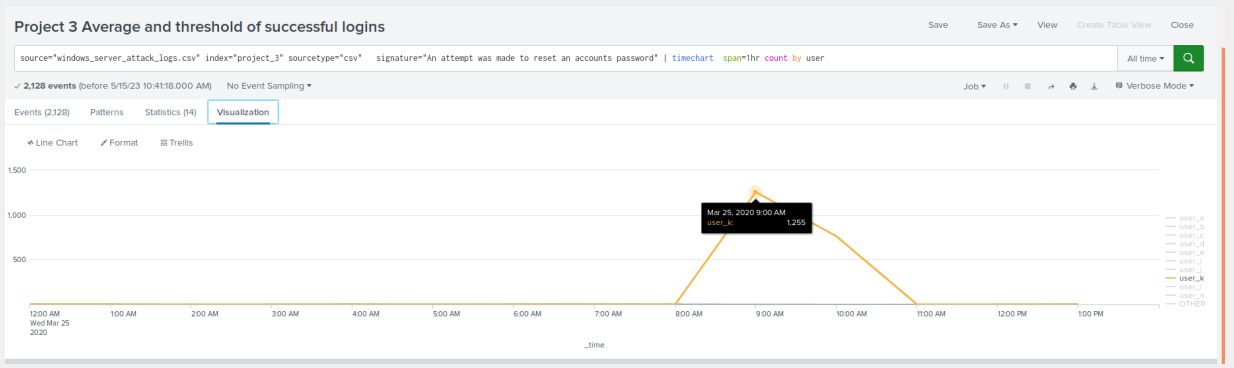


- Who is the primary user logging in?

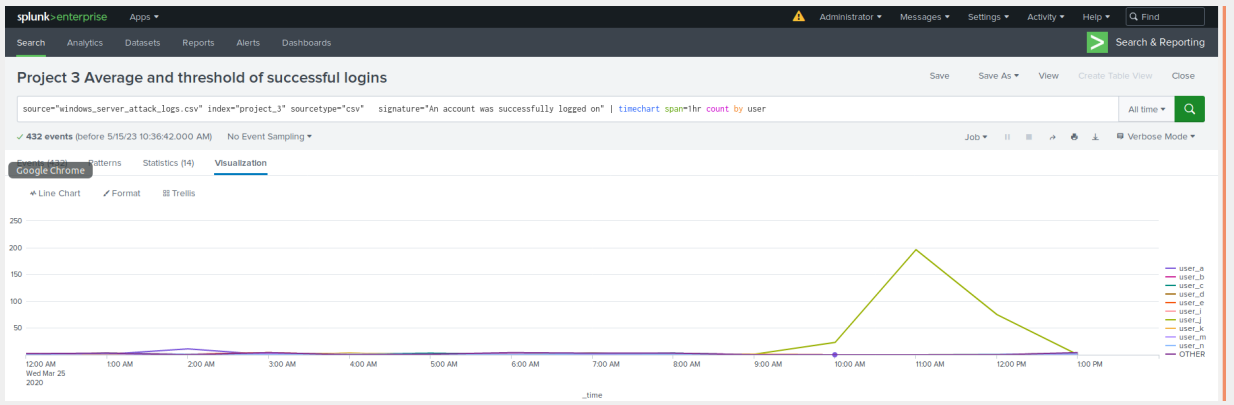
Between 01:00 and 02:00 user_a had 1686 Lockouts implying an attempted bruteforce attack.



Between 08:00 and 11:00 user_k made 2016 attempts to reset their account password.



Finally between 09:00 and 13:00 user_j made 294 successful logins showing great abnormality to standard behaviors if it is not an anomaly in the logs.



If this is not an anomaly user_j has the most significant logins within this log.

- When did it occur?

Began at 09:00 and returned to baseline at 13:00

- Would your alert be triggered for this activity?

With the way these logs digest, no.

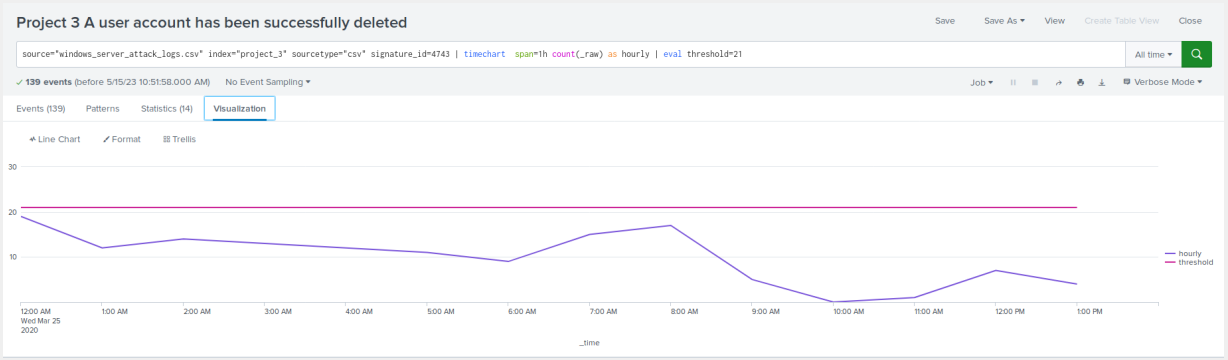
- After reviewing, would you change your threshold from what you previously selected?

No, as these logs appear to have been scrubbed.

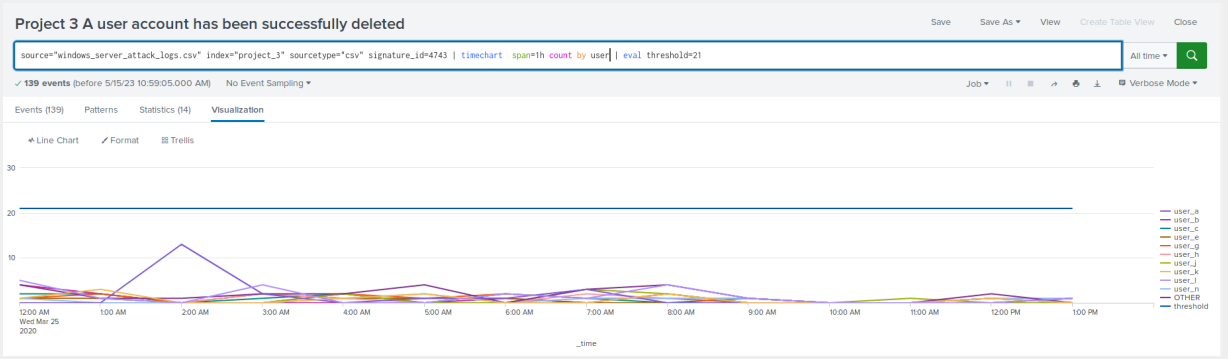
Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

Yes there was a complete dropout of returns around the same period.
09:00 returned 5, 10:00 returned 0 and 11:00 returned 1.
This indicates to me that someone has managed to scrub the logs.



However changing the alert to count by user returns some suspicious activity on user_a again



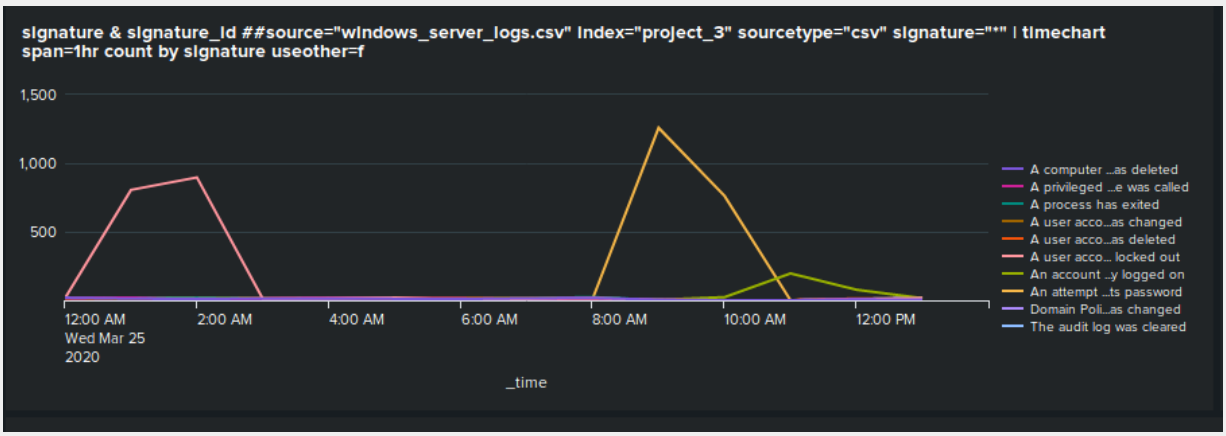
Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

Yes, large bursts of activities in both signatures and users over time.

- What signatures stand out?

3 major points of activity. “A user account was locked out”, “an attempt to reset an accounts password was made” and “An account was successfully logged on”.



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

```
12:00 to 03:00 for user account lockout.
08:00 to 10:00 for password reset attempts.
10:00 to 12:00 for user accounts successfully logged on.
```

- What is the peak count of the different signatures?

```
User account lockout - 896 at 02:00
Password reset attempt - 1258 at 09:00
Successful login - 196 at 11:00
```

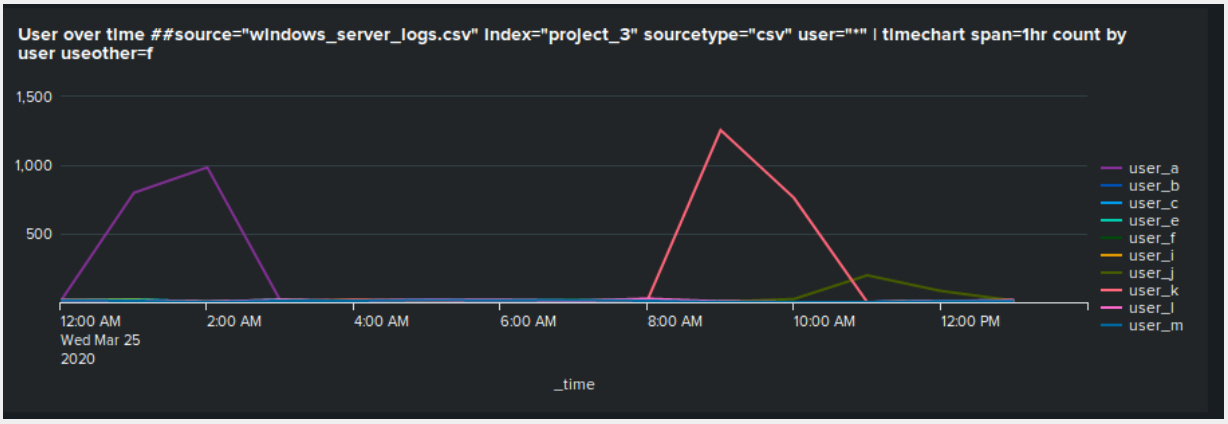
Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes, 3 large results.
```

- Which users stand out?

```
User_a, user_k and user_j
```



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

```
User_a 12:00 to 03:00
User_k 08:00 to 11:00
User_j 10:00 to 12:00
```

- What is the peak count of the different users?

```
User_a is 984
User_k is 1256
User_j is 196
```

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

- Does anything stand out as suspicious?

```
Yes, The animated donut graph can be observed in 24 seconds.
```

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

```
Yes. However I will admit that not as quickly as the line graphs. However it
does catch your attention with the sudden change when a spike is present.
For reference it is Animated Chart Viz.
```

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

- Does anything stand out as suspicious?

```
Yes, This one was represented as a bar graph that can be observed in the same period.
```

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

```
Yes. (same comment as the last section)
```

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?

```
Using the reports does show a good snapshot however the dashboard was configured to interpret the attack logs configuration compared to the alerts and reports.
The Information was far easier to determine what happened and when which resulted in far less time being taken to get to the same result.
The report.
While using the line graph in this configuration it was far easier to determine the 3 points of interest and determine potential methods of attack.
The disadvantage with my selection of visualizations was the time it took to determine the same amount of information compared to the timechart line graphs.
The alerts on the other hand weren't effective in the method that they were constructed as it appeared the logs may have been sanitized.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
Yes. Post requests increased by 28.38% to 1324 results up from 106 results and Get requests dropped by 28.30% to 3157 results from 9851
```

- What is that method used for?

```
Post requests are trying to make changes to the server-side data. E.G Trying to create files or update them.
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
Yes. Within the top 10 results there was a large drop in traffic across all referrers.
Before attack logs, total = 5437
After attack logs , total = 1442
```

Report Analysis for HTTP Response Codes

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

```
Yes. A significant drop in 200 response codes, a slightly less significant drop in 304/301 response codes and a drop in others except from 404 response code which increased.
200 response code before attack - 9126
200 response code after attack - 3746
301 response code before attack - 164
301 response code after attack - 29
304 response code before attack - 445
304 response code after attack - 36
404 response code before attack - 213
404 response code after attack - 679
```

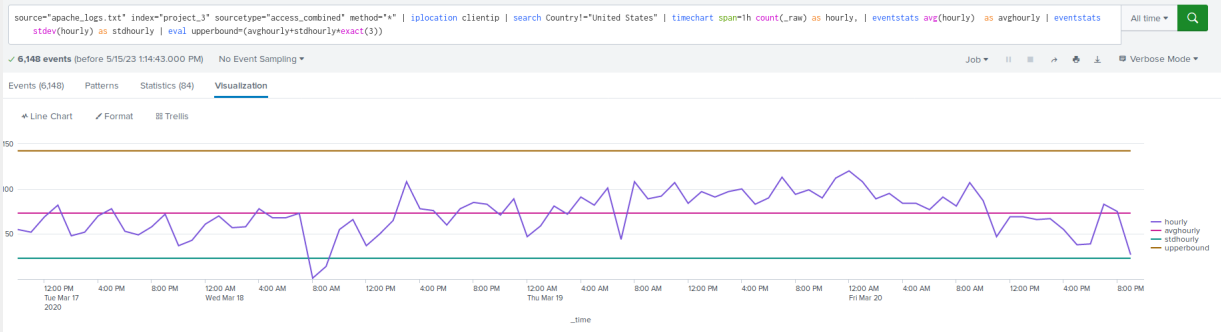
Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

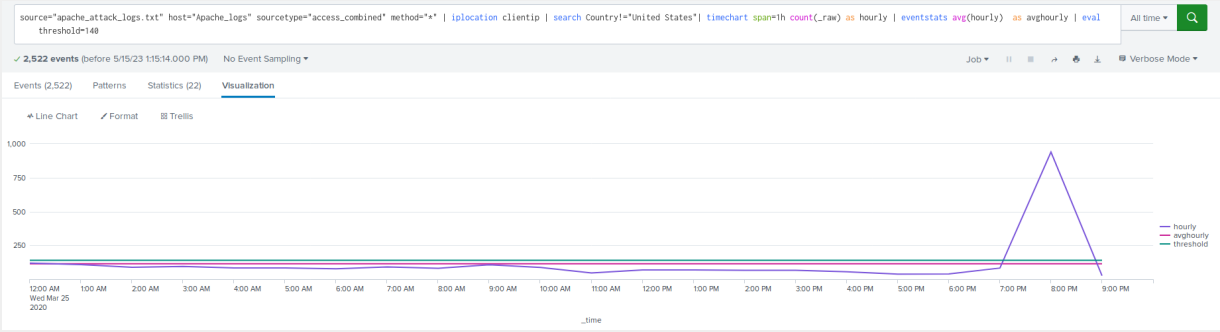
```
Yes, there is a large spike in activity beginning at 19:00
```

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

The attack began at 19:00 with a standard count of 83 which increased to a count of 939 at 20:00 and dropped back down to a count of 27 at 21:00
Pre attack



Post attack



- Would your alert be triggered for this activity?

Yes, The threshold is set to 140 for alert.

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

No, the threshold functioned as intended so it was an effective measure. In this instance the only way to increase effectiveness is to decrease polling times to a closer interval.

Alert Analysis for HTTP POST Activity

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

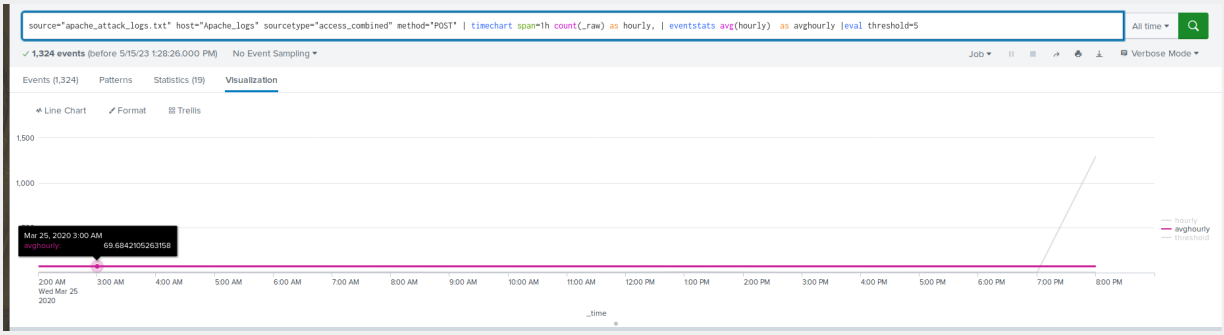
Yes. A large spike beginning at 19:00

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

Count was a 1296 at 20:00

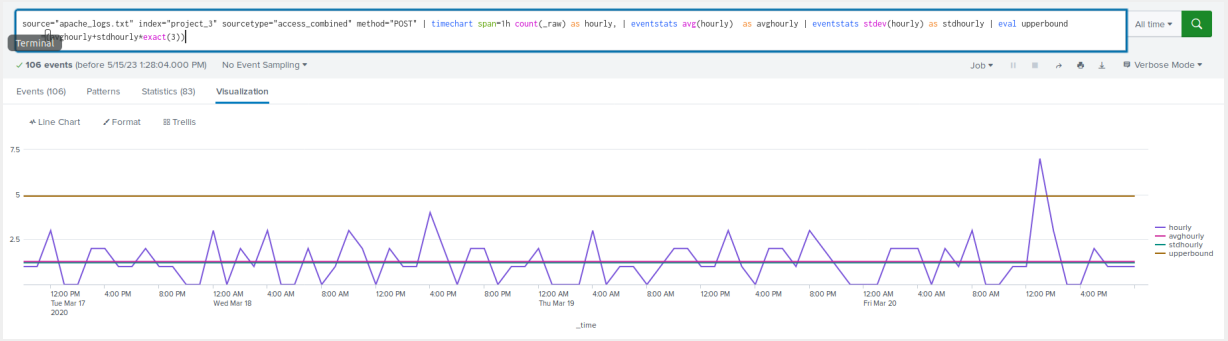
- When did it occur?

The attack begins at 19:00 and the logs finish at 20:00 so limited data. Post attack.



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

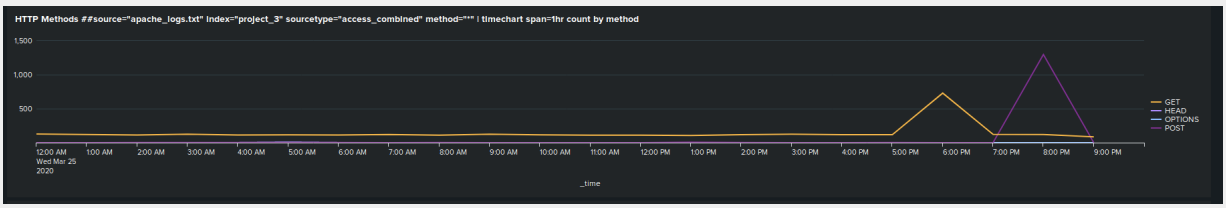
No, The threshold would function as intended since it is set to 5 and the only way to increase efficacy is to decrease the polling intervals.
Pre attack does have 1 alert however with 99.7% coverage with avg+stdev*3, this outlier is representative of .3% of standard use so will take that as a false positive over setting it higher.



Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

Yes. An increase in get requests beginning at 17:00 and finishing at 19:00 then an increase in post requests beginning at 19:00 and ending at 21:00.



- Which method seems to be used in the attack?

```
GET leading into POST
```

- At what times did the attack start and stop?

```
17:00 and finishing at 21:00
```

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

```
POST at 1296 at 20:00
```

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.)

```
Zooming in on the larger areas show considerable activity from 2 ip's
appearing to originate from the Ukraine in Kiev 194.105.145.147 and Kharkiv
79.171.127.34. As well as a single connection in Kharkiv 178.137.5.235 -
Possible slip by hacker?
```

- What is the count of that city?

```
Kiev is 438 and Kharkiv is 432/3
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes. Account login page has elevated access counts as well as logstash.jar
```

- What URI is hit the most?

```
/VSI_Account_logon.php with 1323 access counts
Followed by /files/logstash/logstash-1.3.2-monolithic.jar with 638 access
counts.
```

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

```
The elevated usage on the login page is pretty evident that a high volume of
login attempts are being made - possibly bruteforcing given correlation with
other logs.
Whereas accessing logstash indicates that changes have been made to logs and
presuming the logs are being used for monitoring and given the oddities in
the other log results shown previously, It would indicate the hacker tried
to cover their tracks by altering the logs.
```