



Cybersecurity

Project 3 Review Questions

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

Windows Server Log Questions

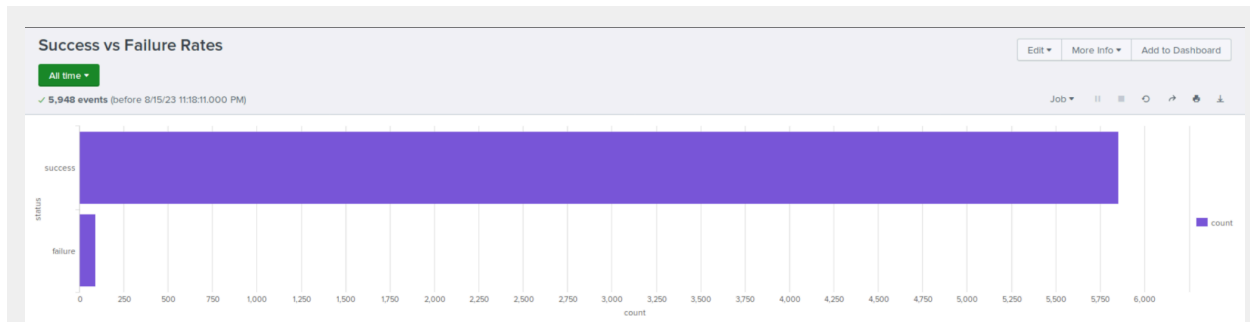
Report Analysis for Severity

- Did you detect any suspicious changes in severity?



Report Analysis for Failed Activities

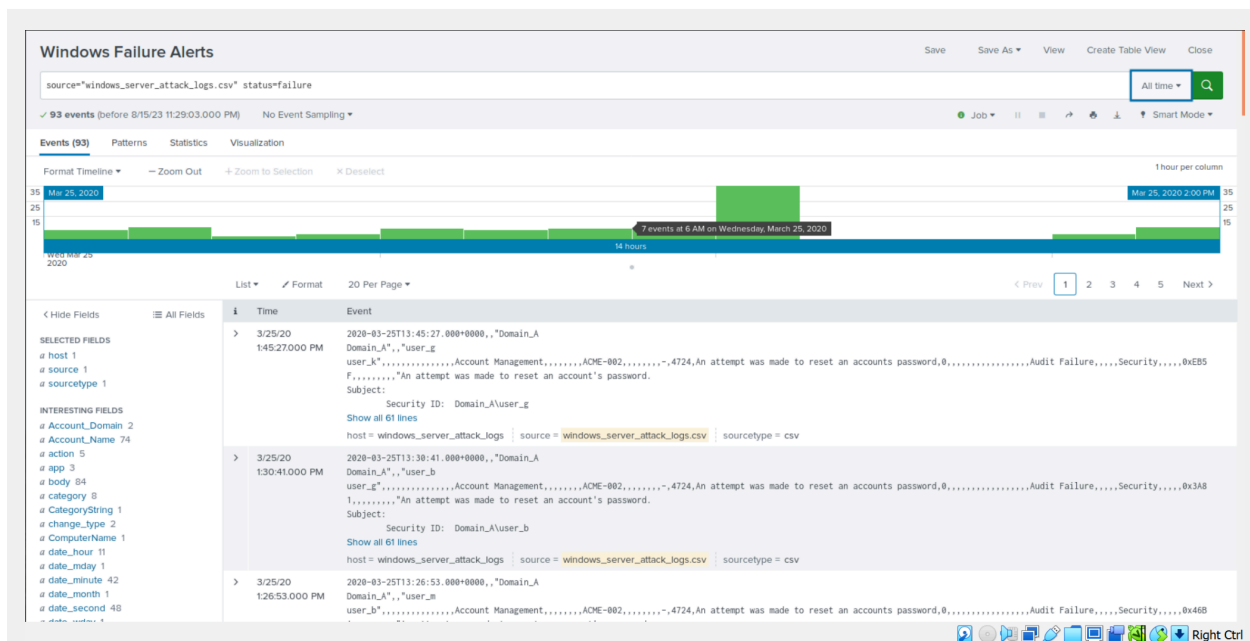
- Did you detect any suspicious changes in failed activities?



Looking at the Windows server attack log file, there was a decrease in the amount of failed activities.

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?



We did detect suspicious activity using the alert that we had created. As can be seen in the events that had occurred in the image above.

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

There were 35 events that occurred at 8:00 AM Wednesday, March 25th, 2020

- When did it occur?

8:00 AM, Wednesday, March 25th, 2020

- Would your alert be triggered for this activity?

Our alert would be triggered for this activity because the threshold that we had set was 6. SO this would have triggered an email to be sent.

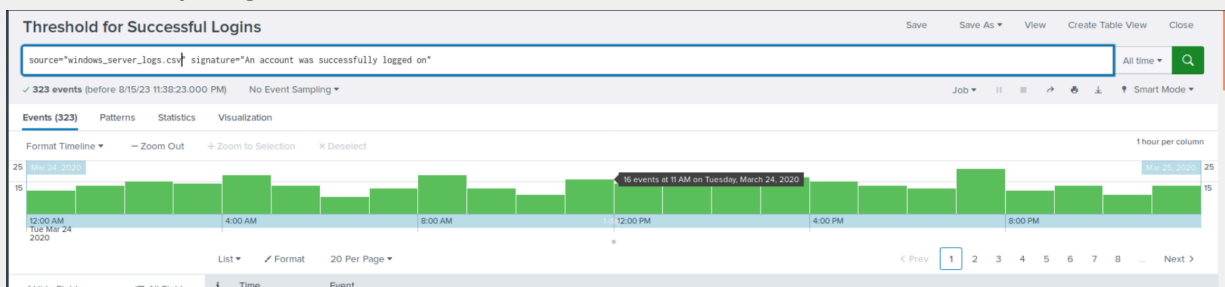
- After reviewing, would you change your threshold from what you previously selected?

I would keep the threshold the same as it was able to capture suspicious activity that had occurred as well as data that we were able to further review.

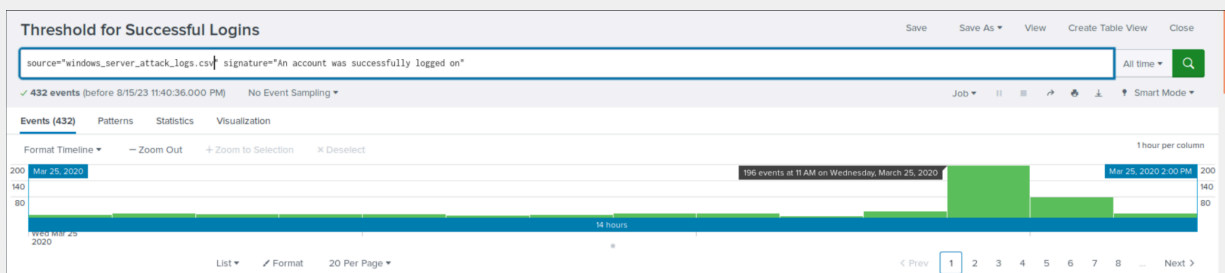
Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

Previous day Log Data March 24th



March 25th Data

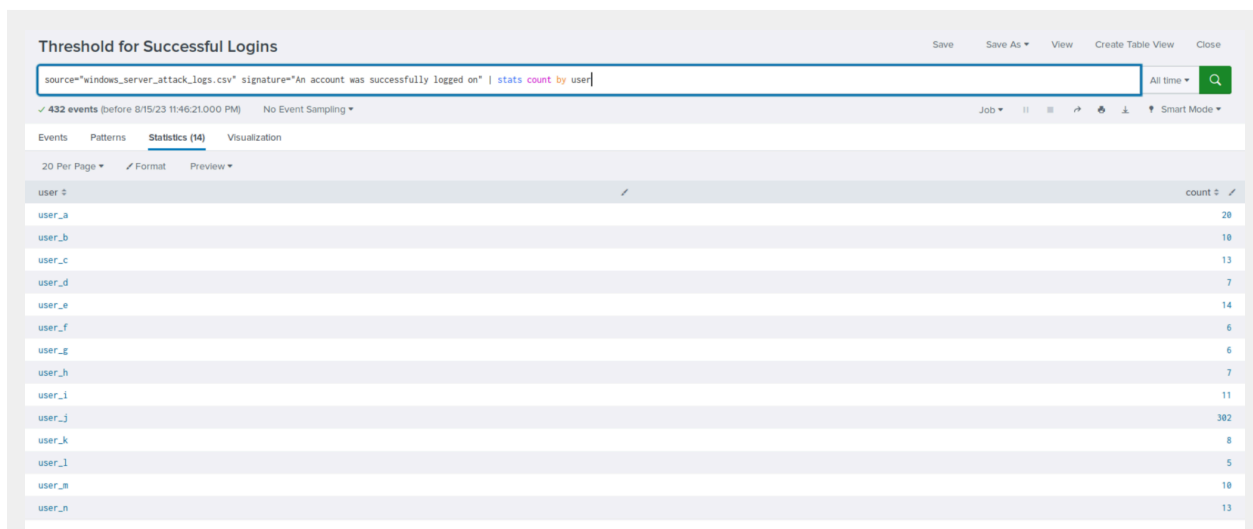


As seen in the images above, we were able to identify numerous logins on March 25th compared to the previous day.

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

The count of events that occurred at 11am March 25th was 196 events, compared to 16 events at the same time the previous day.

- Who is the primary user logging in?



The screenshot shows a Splunk search interface with the title "Threshold for Successful Logins". The search bar contains the query: `source="windows_server_attack_logs.csv" signature="An account was successfully logged on" | stats count by user`. Below the search bar, it indicates "432 events (before 8/15/23 11:46:21.000 PM)" and "No Event Sampling". The results are displayed in a table with two columns: "user" and "count". The table lists 14 users, with "user_j" having the highest count of 302.

user	count
user_a	28
user_b	18
user_c	13
user_d	7
user_e	14
user_f	6
user_g	6
user_h	7
user_i	11
user_j	302
user_k	8
user_l	5
user_m	18
user_n	13

The primary user logging in was user j at 302 times.

- When did it occur?

This event activity occurred at 11am Wednesday, March 25th, 2020.

- Would your alert be triggered for this activity?

The alert would be triggered for this activity, as the threshold was set to 15 based on the baseline activity from the previous day.

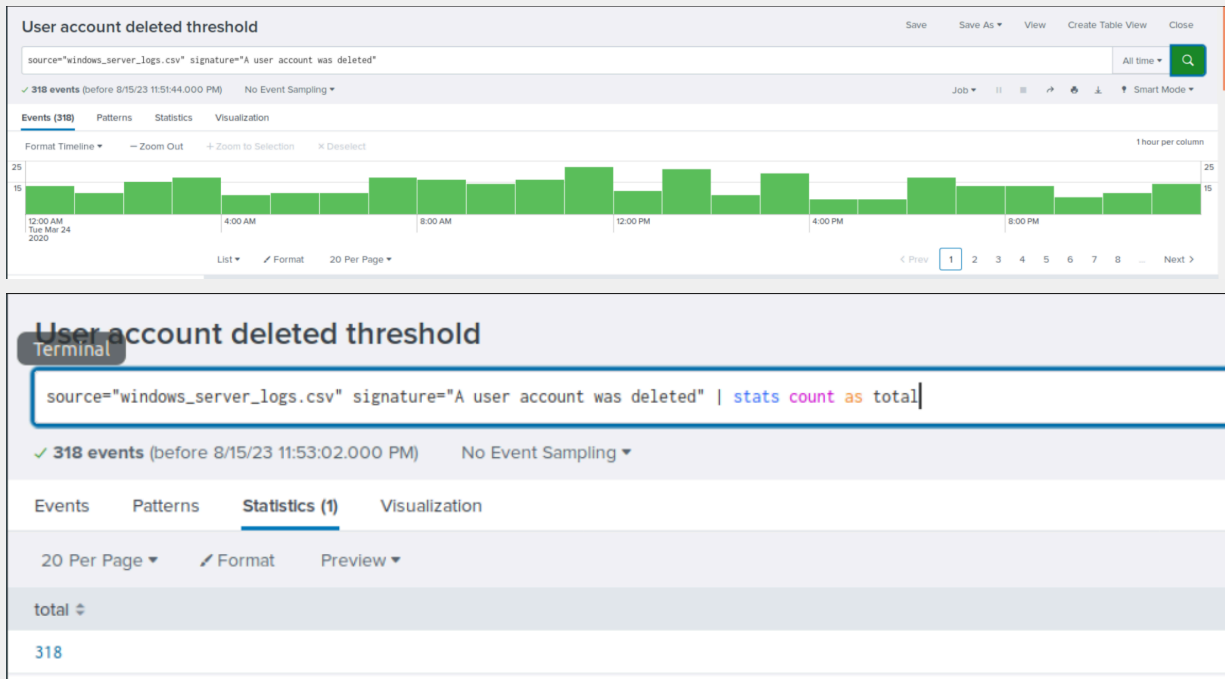
- After reviewing, would you change your threshold from what you previously selected?

I would not change my threshold as it did capture a large amount of data and the baseline that has been determined is accurate for VSI daily activity.

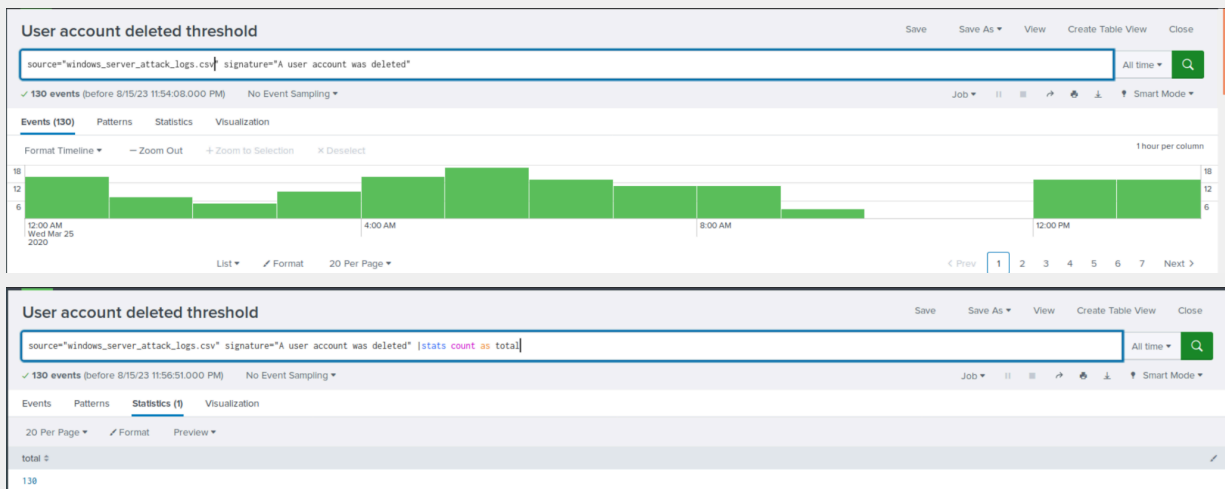
Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

Previous day Activity March 24th



March 25th Data



We did not detect a suspicious volume of deleted accounts. The only slight

variation we were able to see was the number of accounts deleted between 4:00am and 6:00am March 25th compared to March 24th at the same time range.

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

The number of users that have been locked out has risen a significant amount compared to the previous day. There is also an increase in the signature “an attempt was made to reset an account's password”.

- What signatures stand out?

The two signatures that stand out are “an attempt was made to reset an account's password” and “A user account was locked out”.

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

The time “A user account was locked out” began at 12:00am and ended at 3:00am. The signature “an attempt was made to reset an account's password” began at 8:00am and ended at 11:00am.

- What is the peak count of the different signatures?

The peak count for “A user account was locked out” was 896 at 2:00am, and the peak count for the signature “an attempt was made to reset an account's password” was 1,258 at 9:00am.

Dashboard Analysis for Users

- Does anything stand out as suspicious?

User a and user k have activity that mirrors the signature activity recorded above.

- Which users stand out?

User a stands out as well as user k.

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

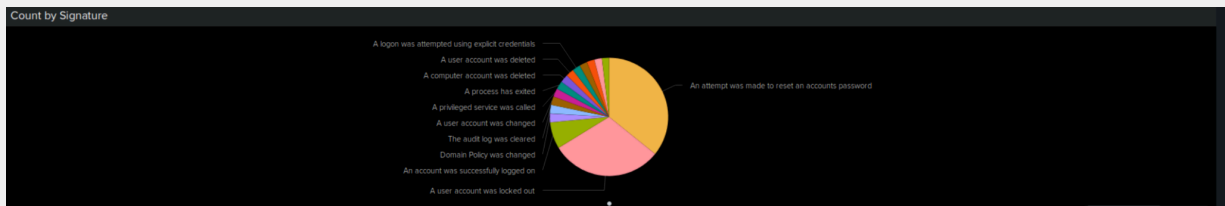
The time that it began for user a was 12:00am and ended at 3:00am and for user k their activity began at 8:00am and ended at 11:00am.

- What is the peak count of the different users?

The peak count for user 8 is 984 and the peak count for user k is 1,256.

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

- Does anything stand out as suspicious?



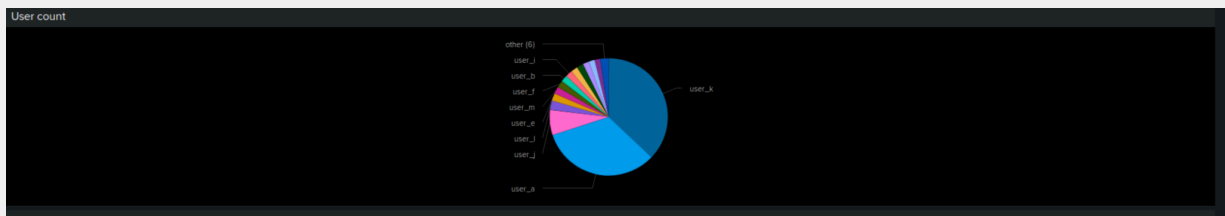
The two things that stand out as suspicious are that there have been numerous attempts to reset account passwords, as well as user accounts being locked out.

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

The results do match the findings that we discovered in the time charts for the signatures.

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

- Does anything stand out as suspicious?



User a and user k have a disproportionately large amount of activity compared to other users.

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

The results do match the findings of the time chart for users, as both user a and user k appear in both.

Dashboard Analysis for Users with Statistical Charts

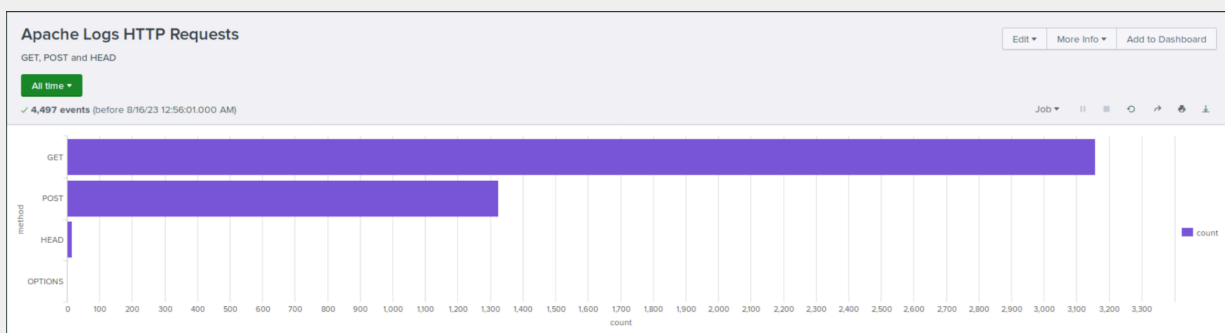
- What are the advantages and disadvantages of using this report, compared to the other user panels that you created?

The advantage of using this report compared to the other user panels that were created is that it is easy to access all the panels, which can be used for quick comparisons. I don't see the disadvantages.

Apache Web Server Log Questions

Report Analysis for Methods

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



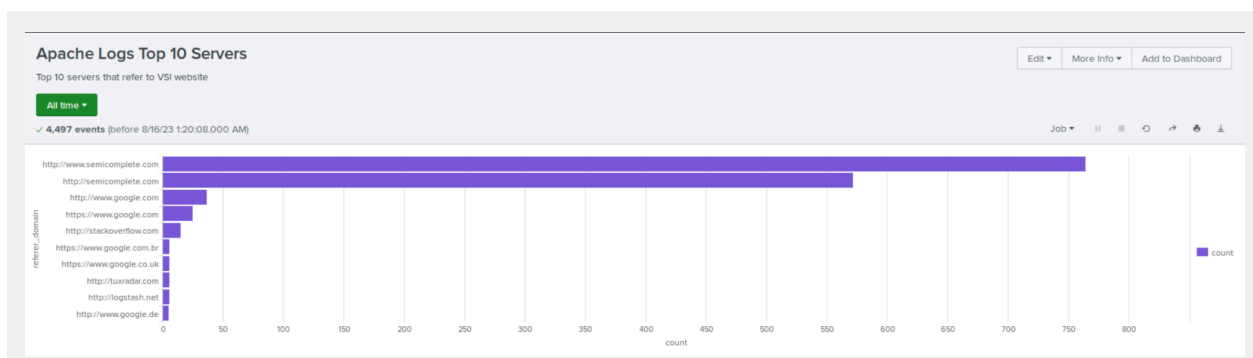
There has been a large increase in HTTP POST requests.

- What is that method used for?

POST request is a type of HTTP (Hypertext Transfer Protocol) request method used to send data from a client to a server.

Report Analysis for Referrer Domains

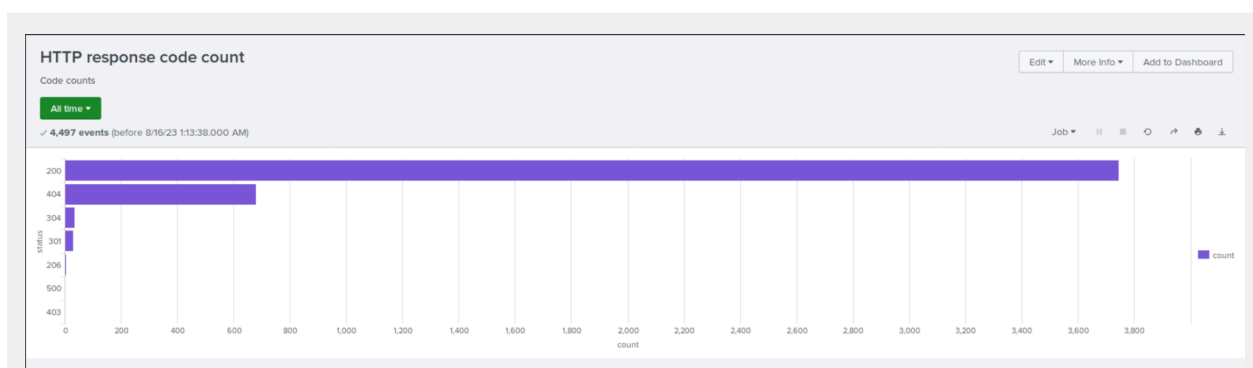
- Did you detect any suspicious changes in referrer domains?



There was not a noticeable change in referrer domains compared to the previous day.

Report Analysis for HTTP Response Codes

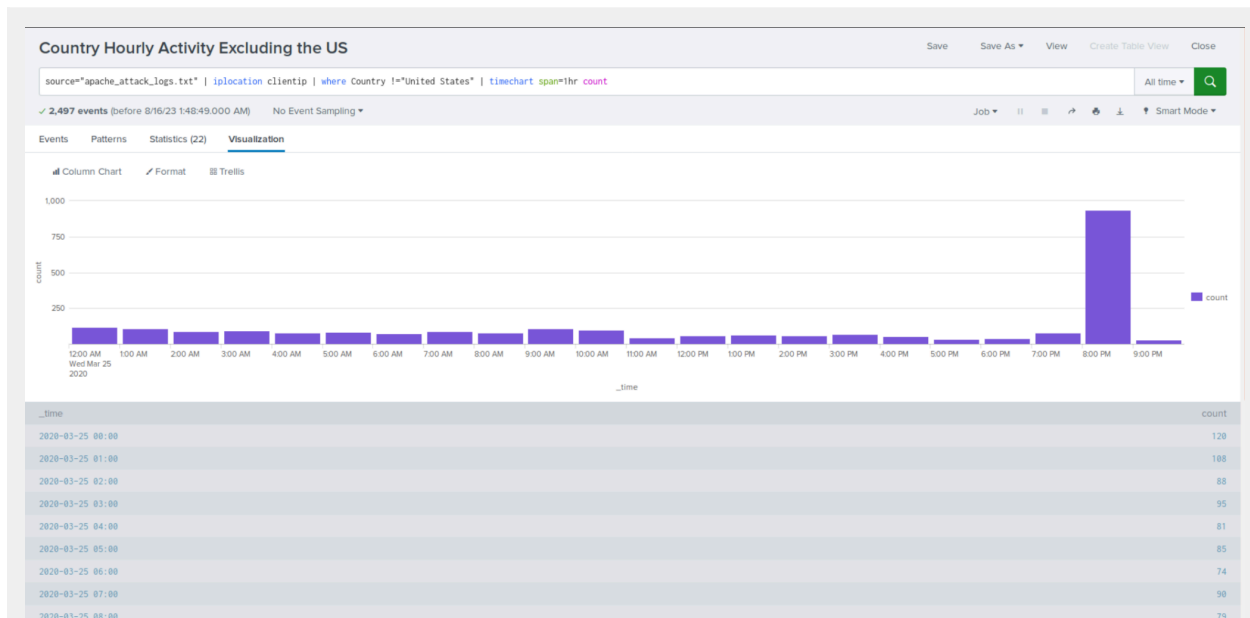
- Did you detect any suspicious changes in HTTP response codes?



There has been an increase in 404 error codes.

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?



There was a large amount of international activity that occurred on March 25th, 2020 at 8:00pm

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

It happened at 8:00pm and lasted one hour. The total count of activity was 937.

- Would your alert be triggered for this activity?

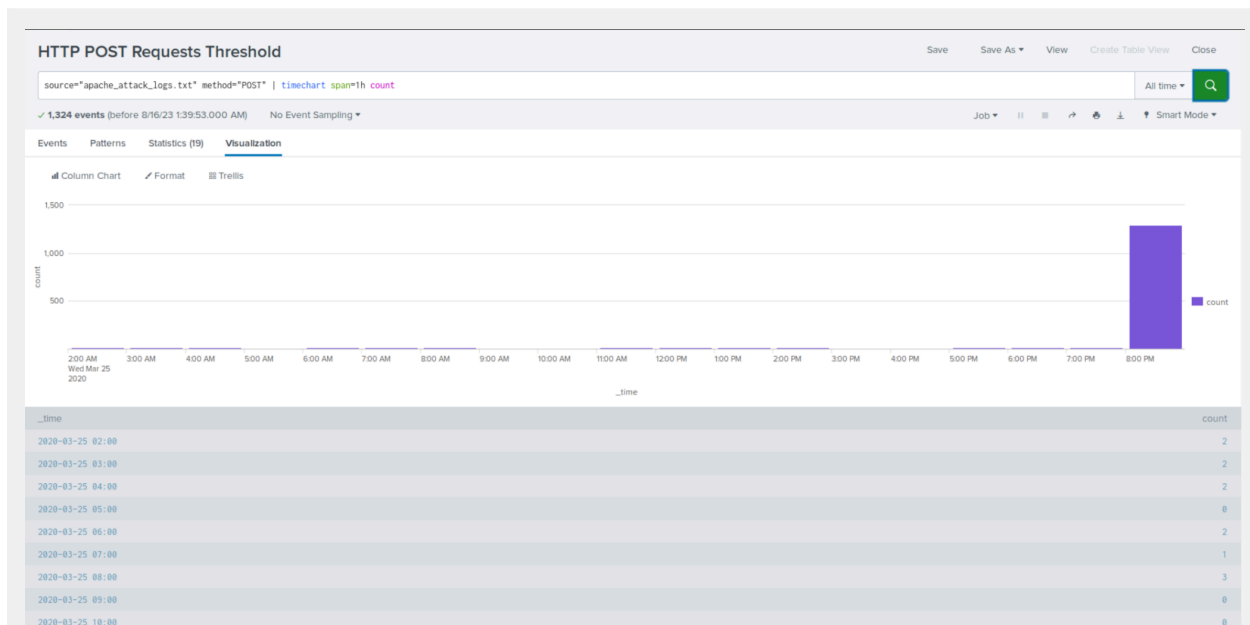
My alert would be triggered for this activity as it was set to 60.

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

I could increase my threshold a little more to ensure that smaller notifications are not triggered.

Alert Analysis for HTTP POST Activity

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



We did detect a very high amount of suspicious HTTP POST requests at 8:00pm March 25th, 2020.

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

There were 1,296 POST requests made on March 25th 2020 at 8:00pm.

- When did it occur?

March 25th 2020 at 8:00pm

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

I would not change the threshold that I had set because it would be sufficient to capture this unusual activity.

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

There was a large increase in GET and POST requests.



- Which method seems to be used in the attack?

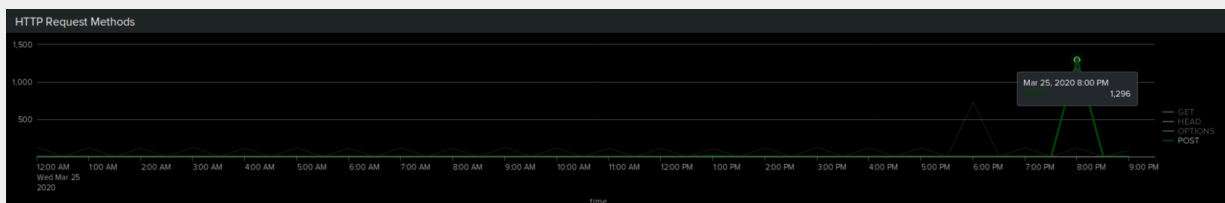
The HTTP request method was user during the attack. In this case, it was specifically GET and POST requests indicating a DDos attack.

- At what times did the attack start and stop?

The attacks using the GET request started at 5:30pm and stopped at 6:30pm. The attacks using the POST requests started at 7:30pm and stopped at 8:30pm.

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

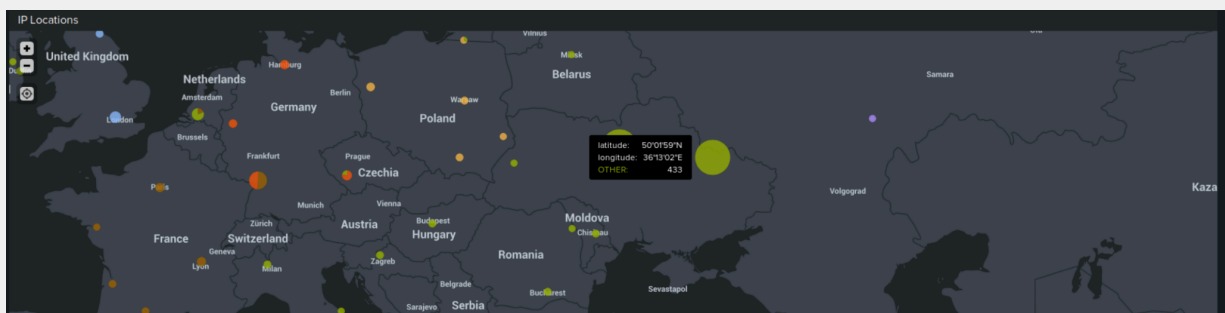
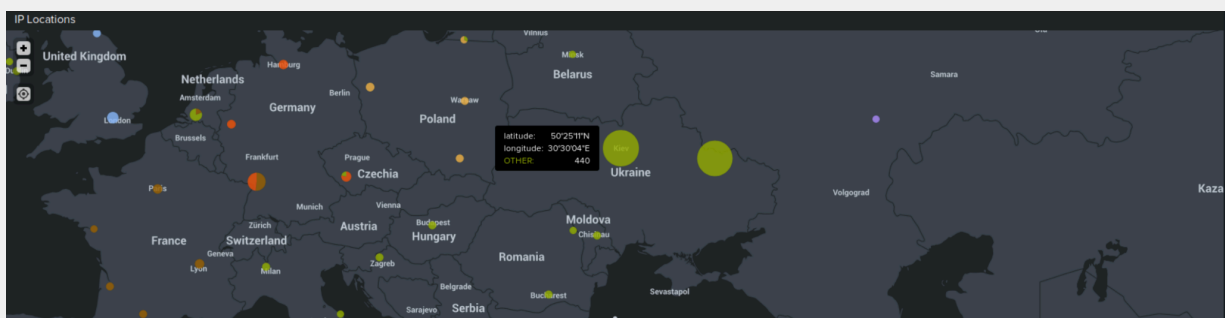
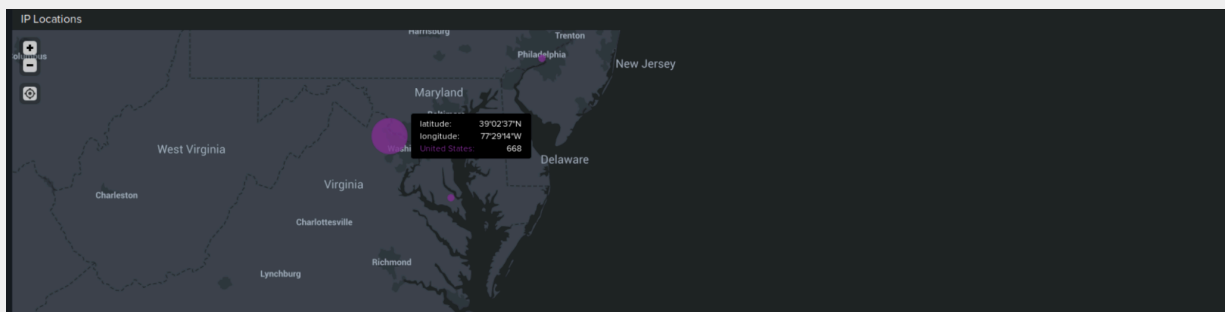
The peak count of the POST requests user was 1,296 at 8:00pm on March 25th, 2020.



Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

There has been a spike in activity within two countries and cities. Looking at the map, we can see a spike within the US, specifically Ashburn, Virginia. The second country that has had a spike is Ukraine, specifically Kyiv. (using the coordinate provided, the city is Ashburn and not Washington DC)

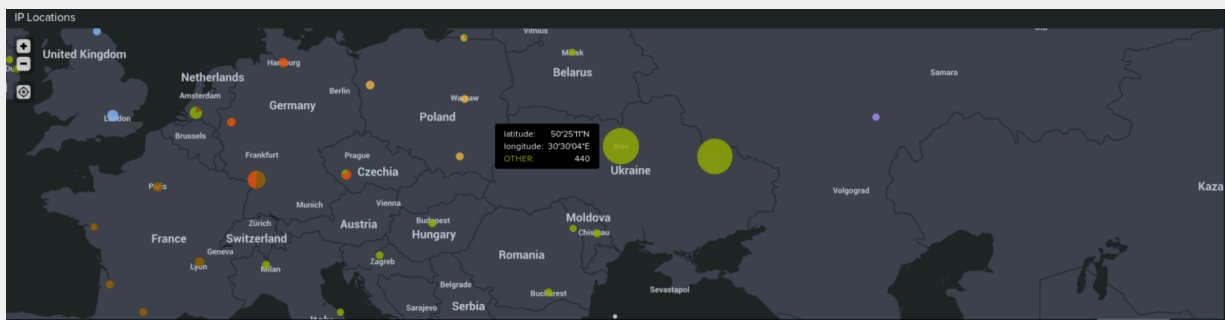
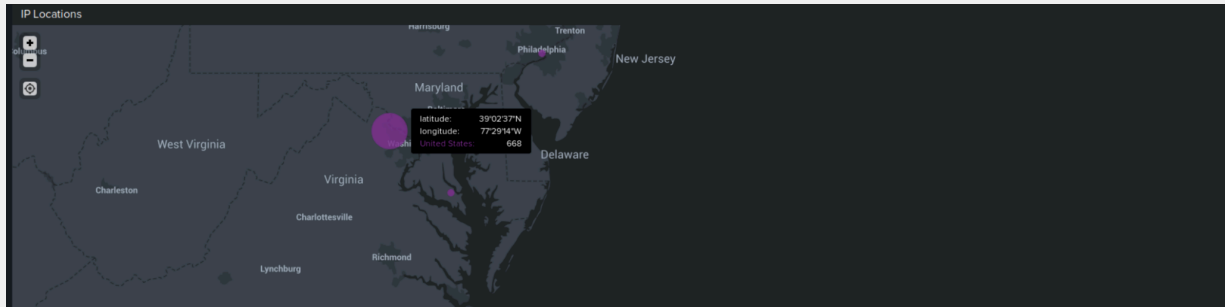


- Which new location (city, country) on the map has a high volume of activity?
(Hint: Zoom in on the map.)

The two cities that have a noticeable amount of activity are Ashburn, Virginia and Kyiv, Ukraine. (using the coordinate provided, the city is Ashburn and not Washington DC)

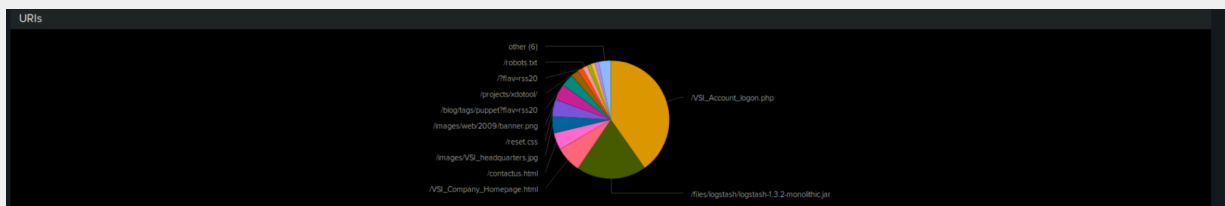
- What is the count of that city?

Ashburn has a count of 668 and Kyiv has a count of 440.



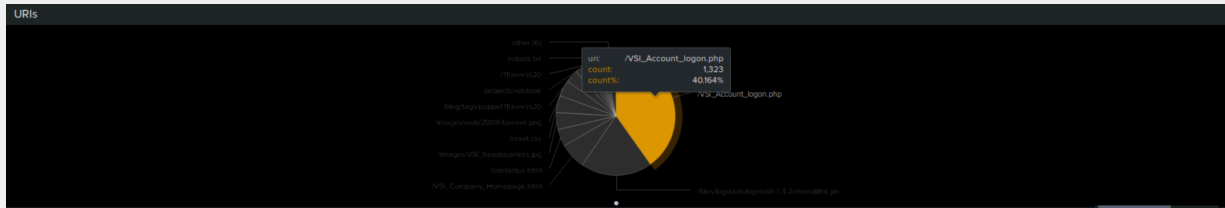
Dashboard Analysis for URI Data

- Does anything stand out as suspicious?



The two things that stand out as suspicious are the increase in VSI_Account_login.php and /files/logstash/logstash-1.3.2-monolithic.jar.

- What URI is hit the most?



The URI that is the most is the VSI_Account_logon.php with a count of 1,323.

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

This is most likely a brute force attack or a DDoS attack.