Cybersecurity

Project 3 Review Questions

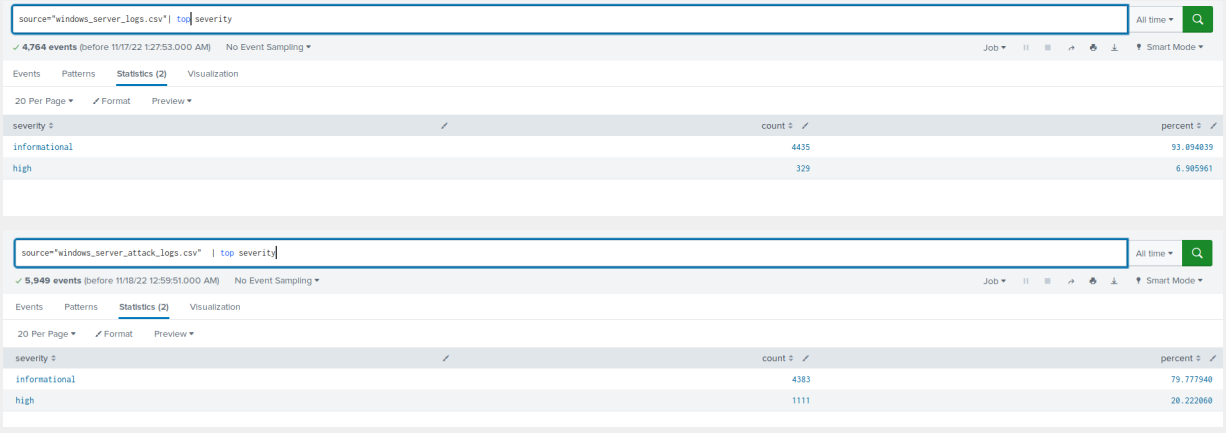
Make a copy of this document before you begin. Place your answers below each question.

Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

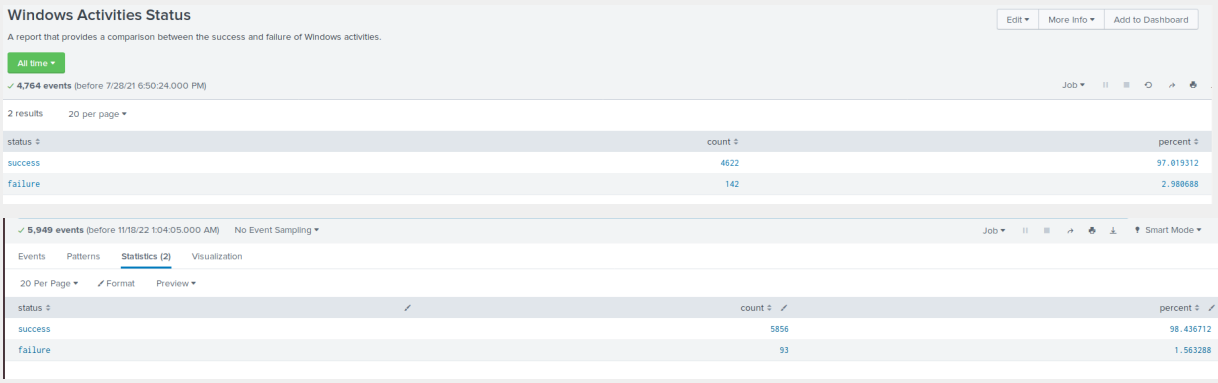
Yes, the high severity field has grown from 329 to 1111 or from 6.91% of the total severity fields to 20.22%.



Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

Yes, the amount of failures has dropped from 142 to 93 but the successes have increased from 4616 to 5854. This indicates that the attackers have been successful in accessing a user account and making
many changes including deleting accounts.



Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

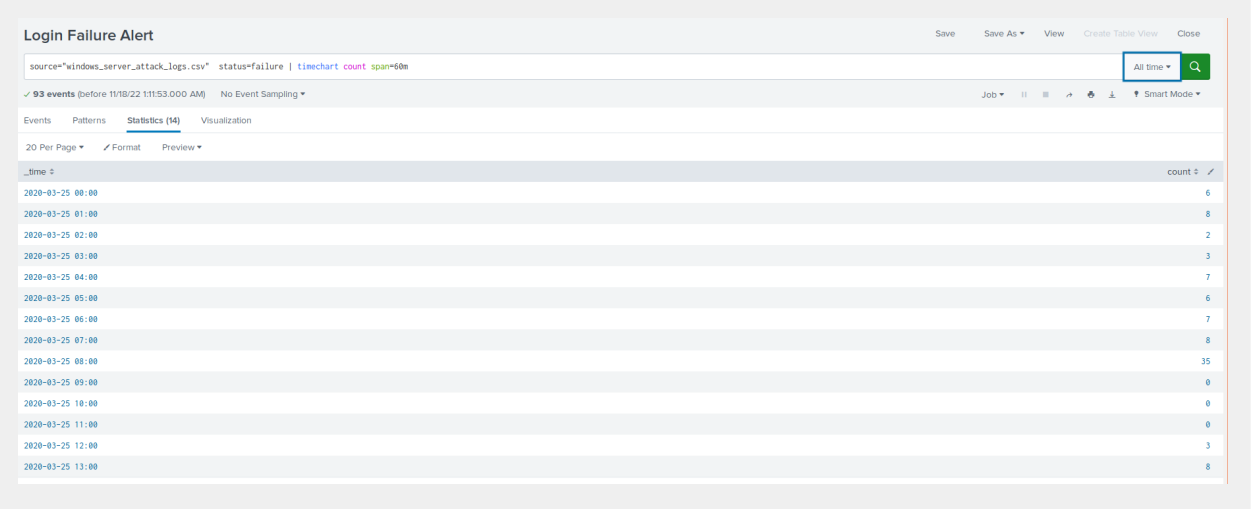
```
Yes, alert did detect a suspicious volume of failed Windows activity
```

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

```
There was a large spike of 35 failures at 8:00am
```

- When did it occur?

```
08:00 AM on 2020-03-25
```



- Would your alert be triggered for this activity?

```
Yes, the threshold is still relevant and the alert would have triggered. It was set very low, 8.
```

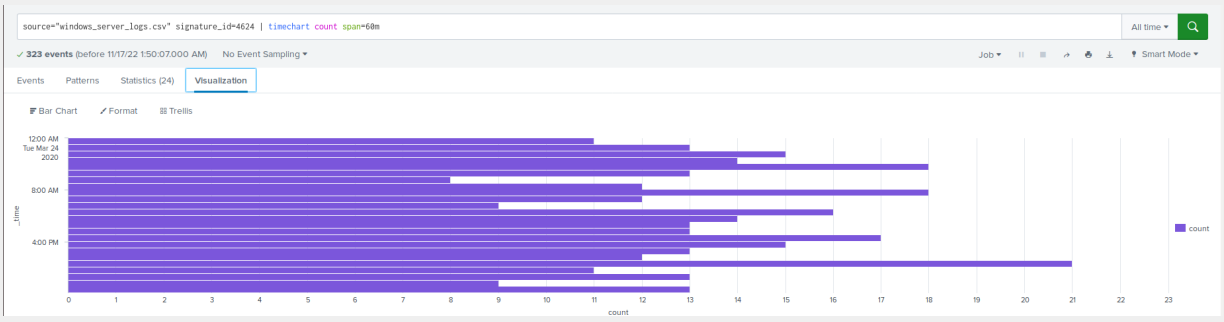
- After reviewing, would you change your threshold from what you previously selected?

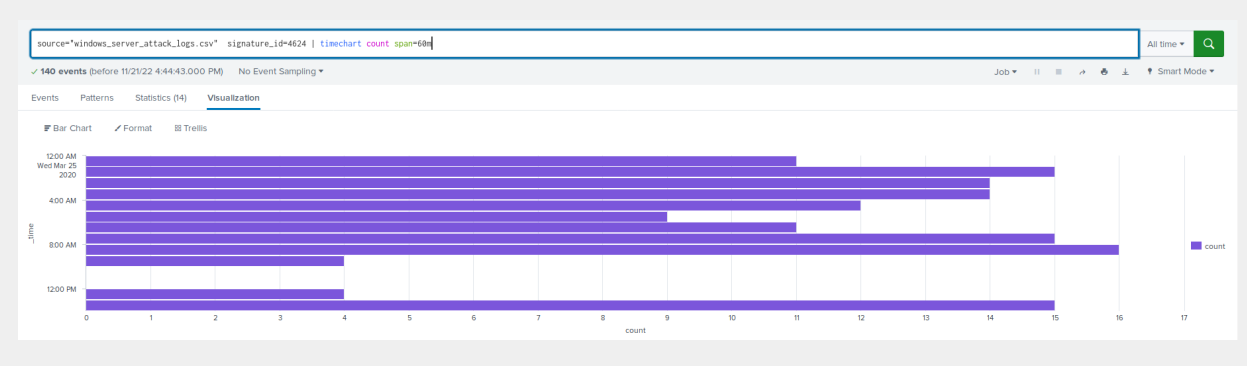
```
No at this stage. Very low and it would detect activity.
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

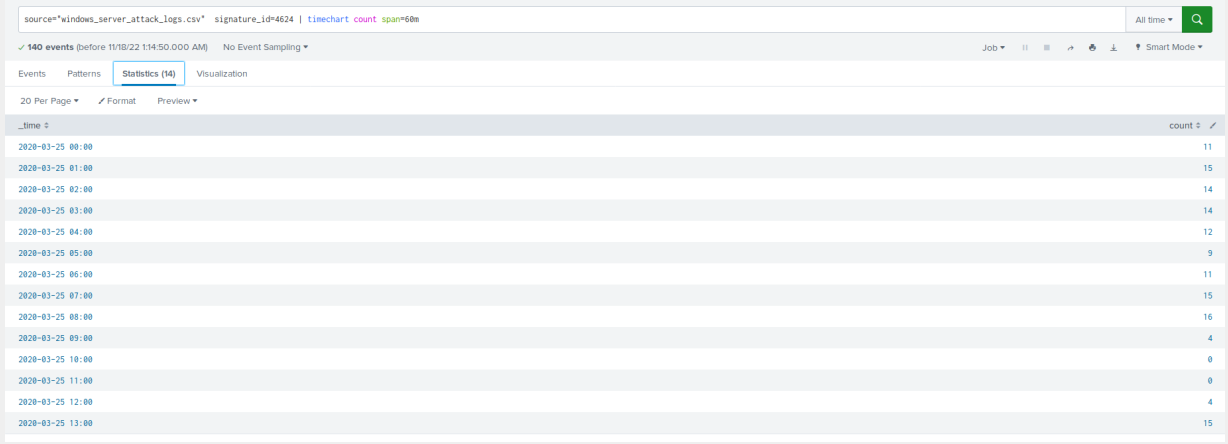
```
There is little difference between the 24-03-2020 and 25-03-2020 which indicates that there was not a great change to the normal level of successful logins. There was actually a drop in the logins at 10:00 AM to 0.
```





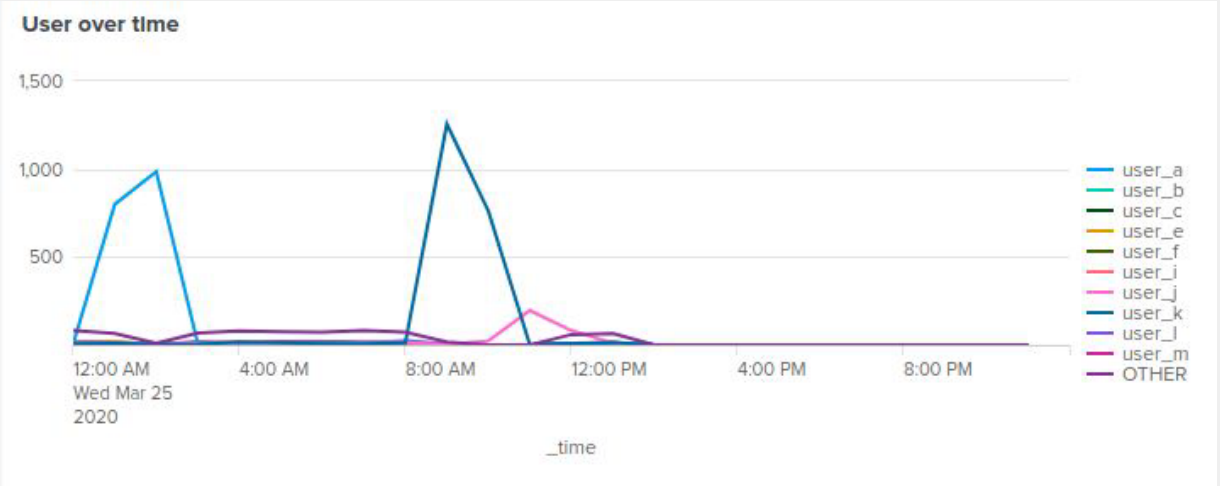
- If so, what was the count of events in the hour(s) it occurred?

There were 2 hours with no successful logins, 10:00 and 11:00.



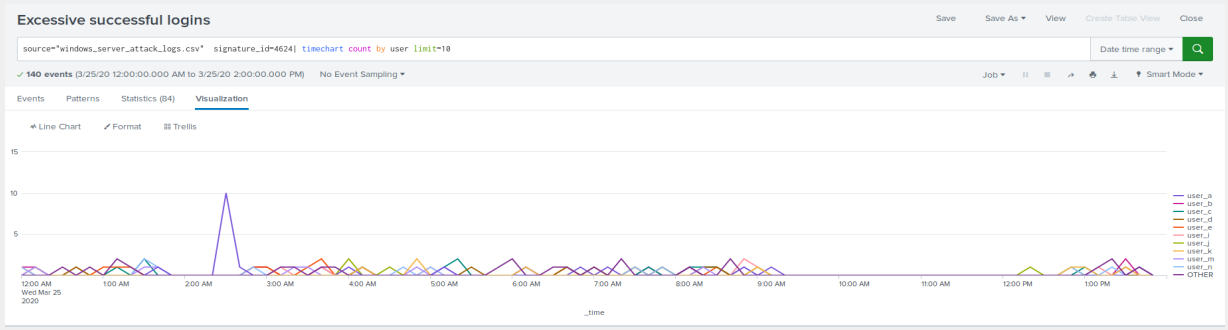
- Who is the primary user logging in?

User_a was the primary user.



- When did it occur?

Around 02:00 AM on the 25-03-2020



- Would your alert be triggered for this activity?

The alert would not have triggered as there were only 14 successful logins and the threshold was greater than 14.

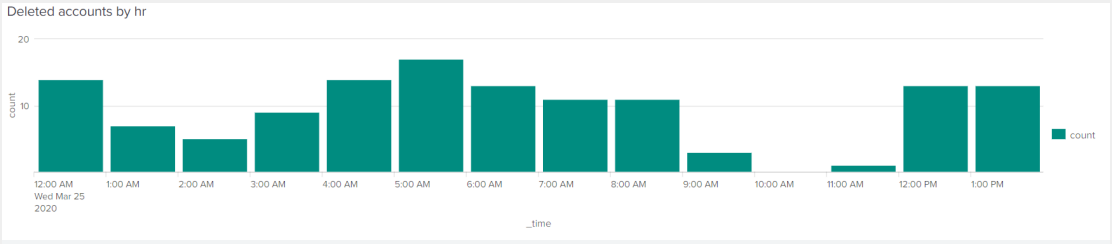
- After reviewing, would you change your threshold from what you previously selected?

The threshold is still relevant but knowing what we now know, the threshold should have been greater than 13.

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

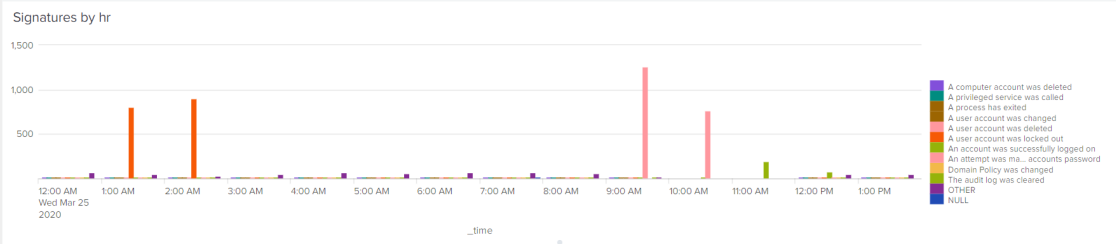
From the logs of attacks, there was a significant drop on deleted accounts between 09:00 AM and 12:00 PM. Although it is not suspicious.



Dashboard Analysis for Time Chart of Signatures

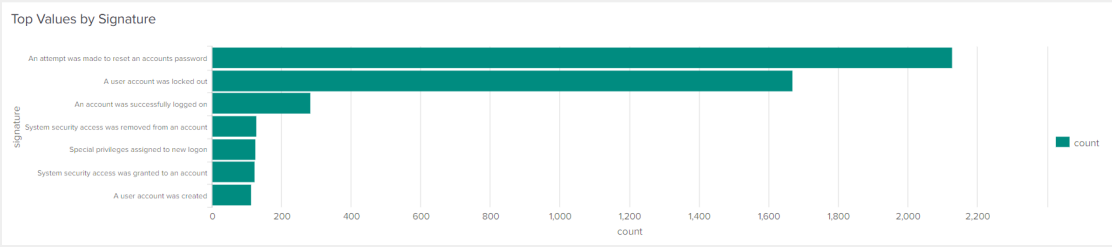
- Does anything stand out as suspicious?

Yes, from that dashboard, there are various "An attempt was made to reset an accounts password", "A user account was locked out" and "An account was successfully logged on". All of them in hours when other suspicious activity was happening.



- What signatures stand out?

➔ "An attempt was made to reset an accounts password" with 2019 attempts.
➔ "A user account was locked out" with 1701



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

➔ `between 09:00 AM and 10:00 AM`
➔ `between 01:00 AM and 02:30 AM`

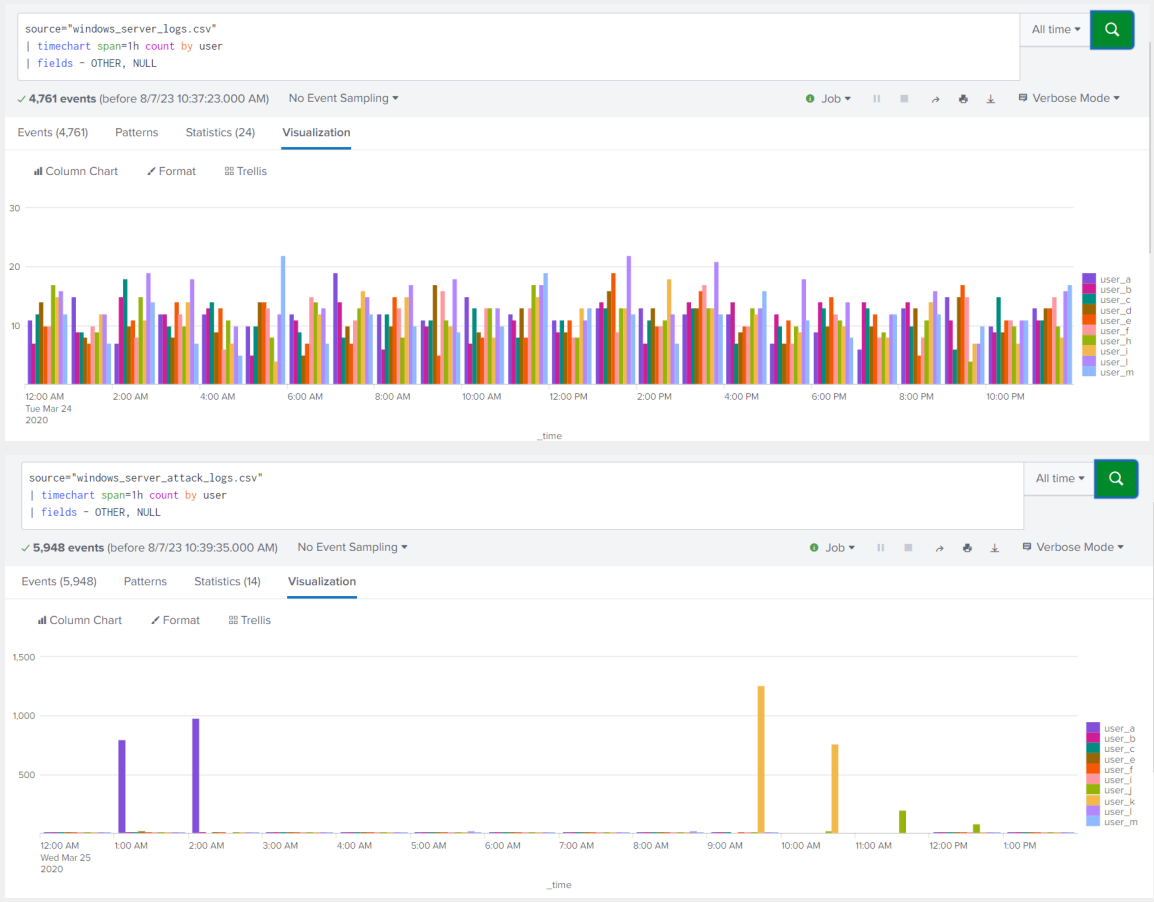
- What is the peak count of the different signatures?

➔ 1258
➔ 896

Dashboard Analysis for Users

- Does anything stand out as suspicious?

Yes. First graph is from the normal logs (excepting for Other and NULL users). Second graph shows anormal activity.



- Which users stand out?

User_k and user_a.

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

User_a between 01:00 AM and 02:30 AM.
User_k between 09:00 AM and 10:00 AM.

- What is the peak count of the different users?

User_a 984
User_k 1256

✓ **5,948 events** (before 8/7/23 10:43:46.000 AM) No Event Sampling

Events (5,948) Patterns **Statistics (14)** Visualization

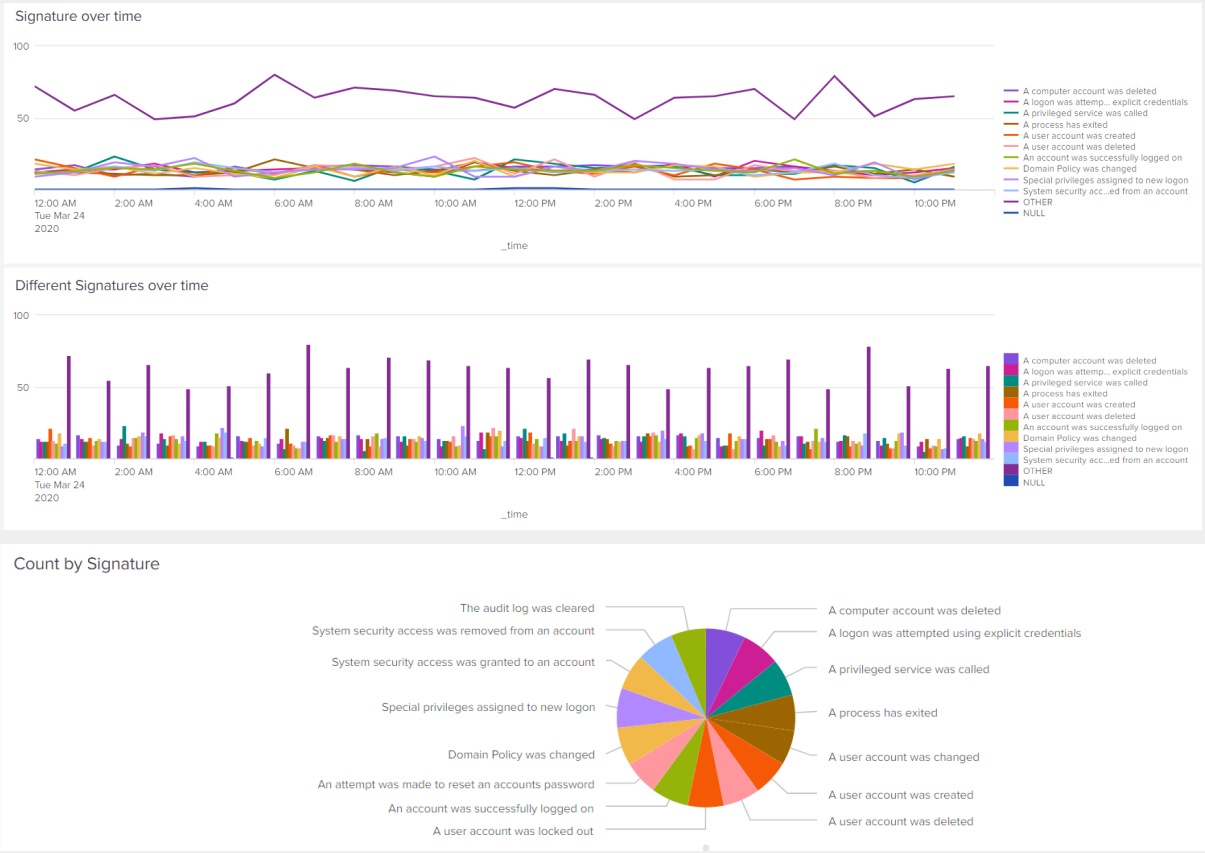
20 Per Page ▾ Format Preview ▾

user_a	user_k	_time
7	8	2020-03-25 00:00
799	9	2020-03-25 01:00
984	2	2020-03-25 02:00
8	4	2020-03-25 03:00
8	16	2020-03-25 04:00
13	13	2020-03-25 05:00
10	7	2020-03-25 06:00
16	7	2020-03-25 07:00
18	12	2020-03-25 08:00
3	1256	2020-03-25 09:00
0	761	2020-03-25 10:00
0	0	2020-03-25 11:00
4	8	2020-03-25 12:00
8	15	2020-03-25 13:00

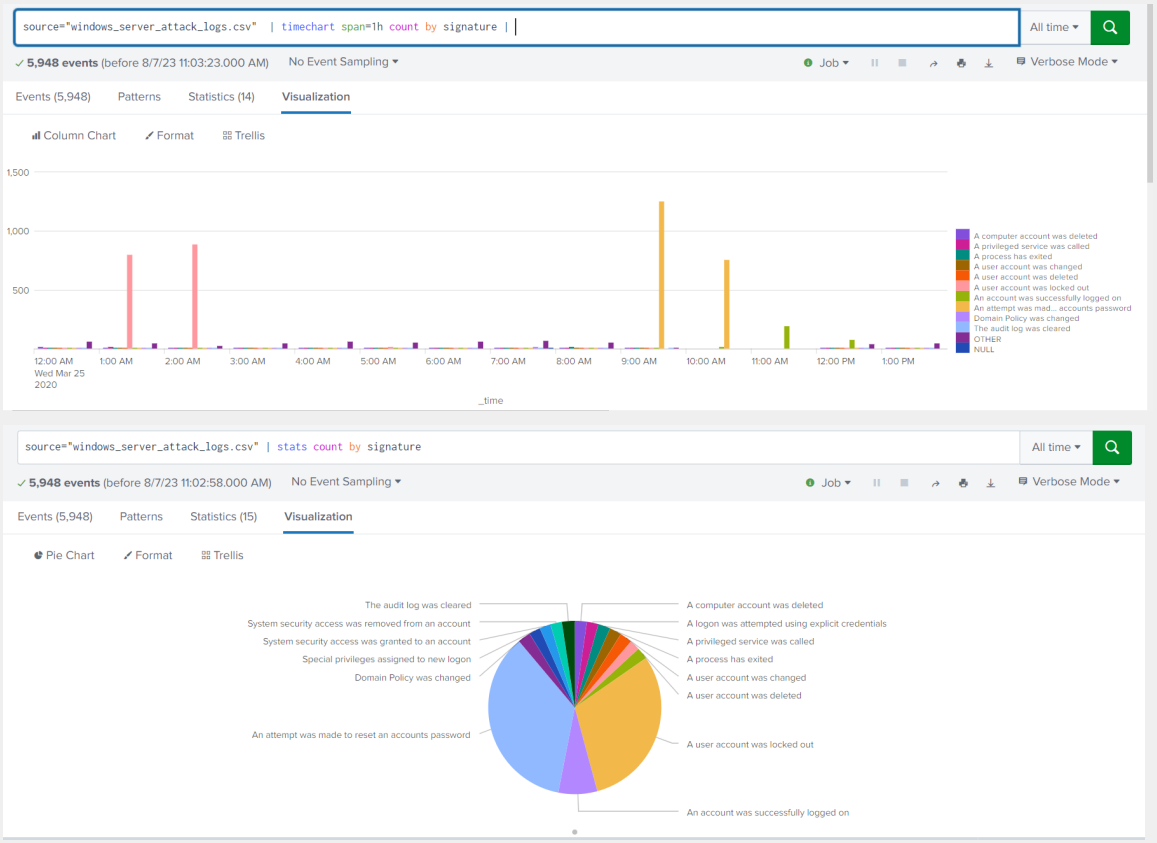
Dashboard Analysis for Signatures with Bar, Graph, and Pie Charts

- Does anything stand out as suspicious?

This is how the normal activity looks like



From the attacks, there are an increase in “A user account was locked out” and “An attempt was made to reset an accounts password”.



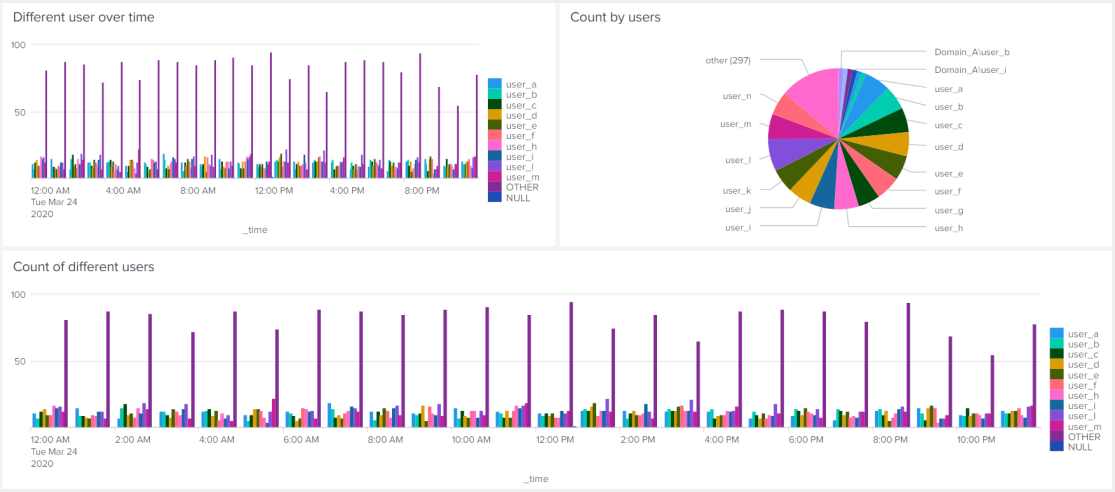
- Do the results match your findings in your time chart for signatures?

Yes, they definitely match.

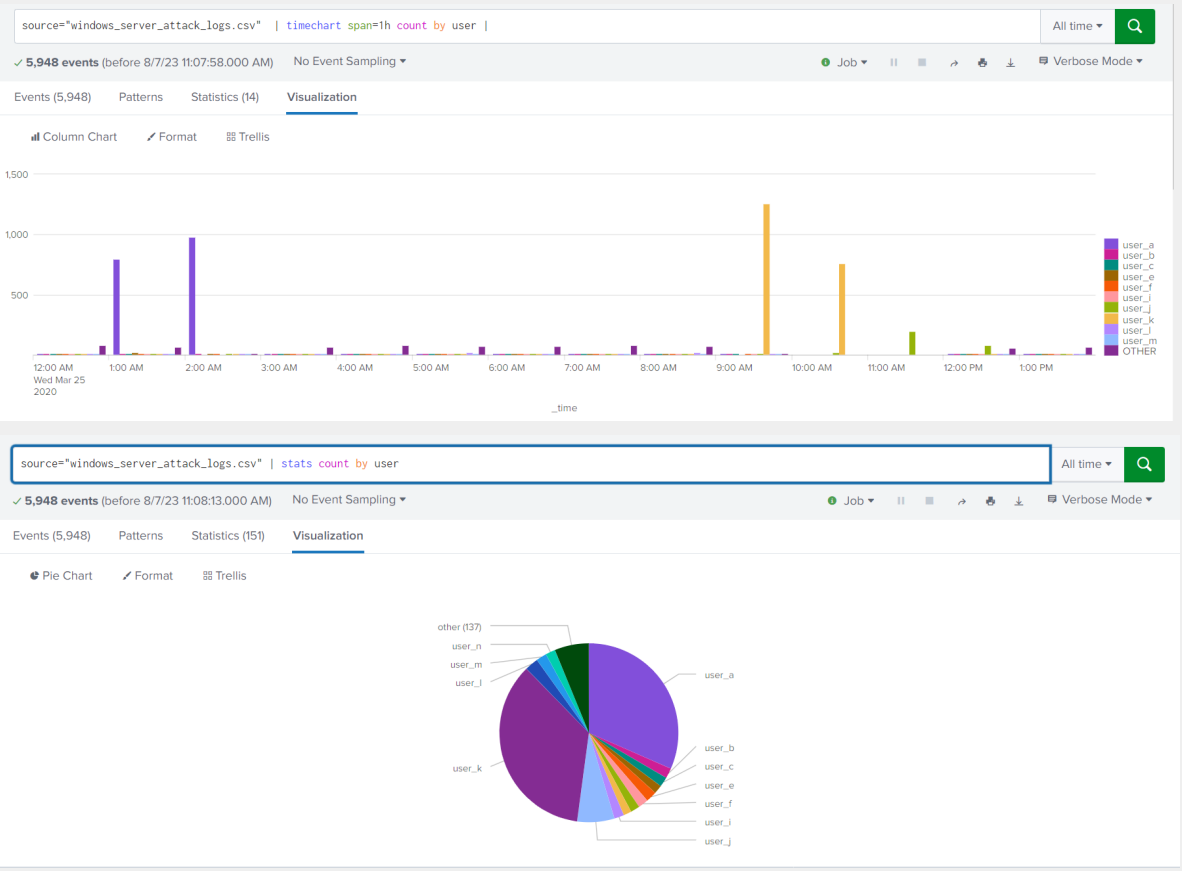
Dashboard Analysis for Users with Bar, Graph, and Pie Charts

- Does anything stand out as suspicious?

From the normal windows log.



From the attack logs.



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

Yes, they definitely match again.

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?

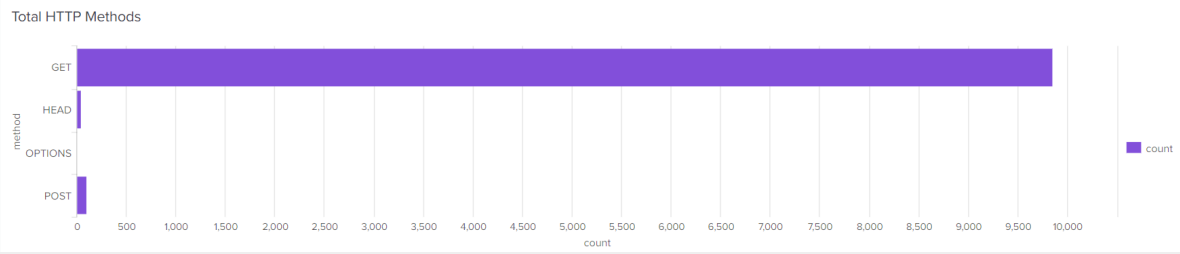
As an advantage, normally with statistical charts it is possible to see a total amount per event, in this case signatures or users . A disadvantage is that it will not show a behavior over time or in a frame time.

Apache Web Server Log Questions

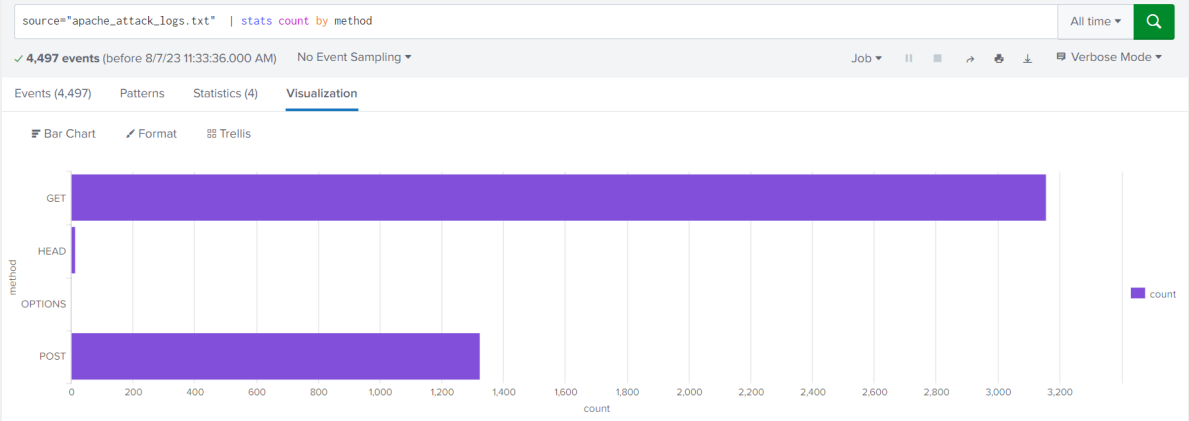
Report Analysis for Methods

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

From the apache logs.



From the attack log, there is an increase of POST method up to 1324.



- What is that method used for?

POST method is used to send data to the server from the HTTP client.

Report Analysis for Referrer Domains

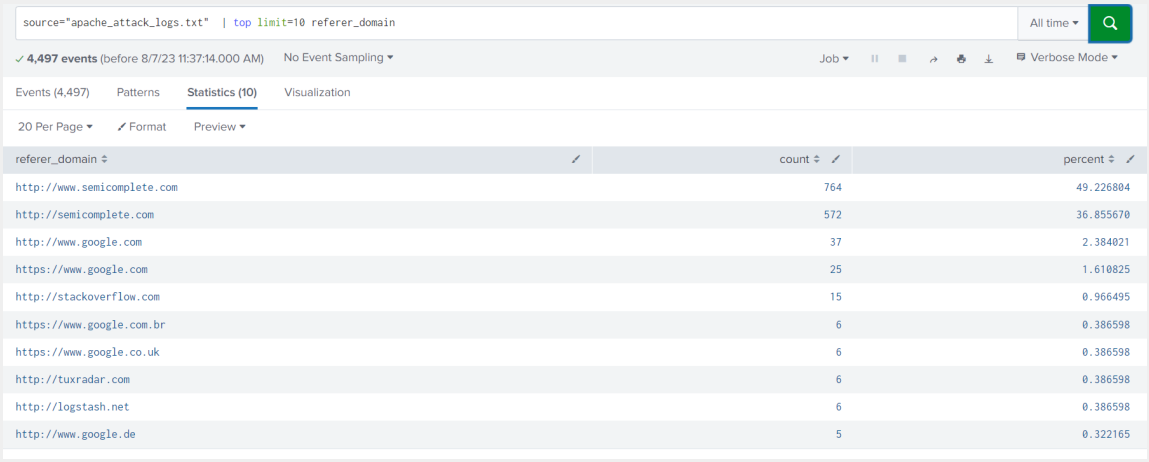
- Did you detect any suspicious changes in referrer domains?

From the apache log (dashboard)

Top 10 Domain Referrers to VSI Website

referer_domain	count	percent
http://www.semicomplete.com	3038	51.256960
http://semicomplete.com	2001	33.760756
http://www.google.com	123	2.075249
https://www.google.com	105	1.771554
http://stackoverflow.com	34	0.573646
http://www.google.fr	31	0.523030
http://s-chassis.co.nz	29	0.489286
http://logstash.net	28	0.472414
http://www.google.es	25	0.421799
https://www.google.co.uk	23	0.388055

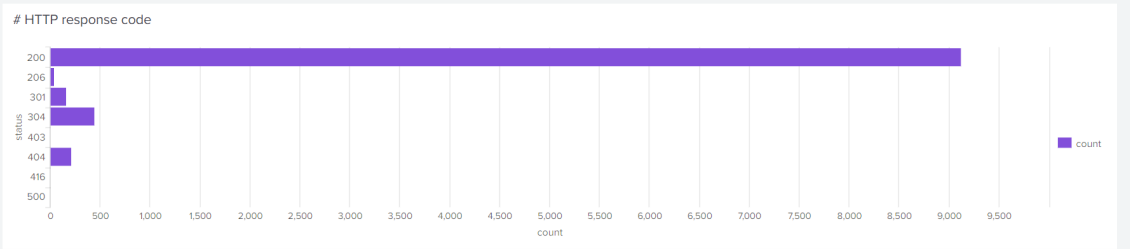
From the attack log, there is no major change.



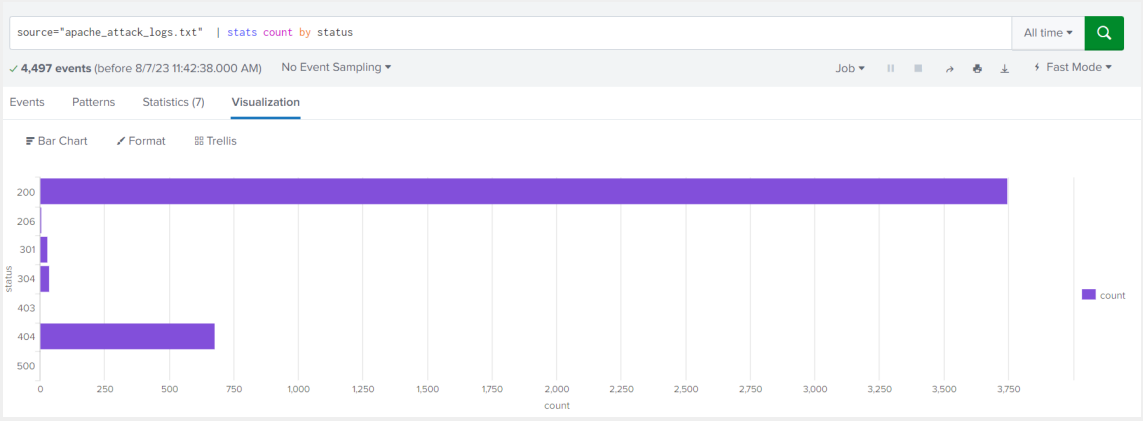
Report Analysis for HTTP Response Codes

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

From the apache log.



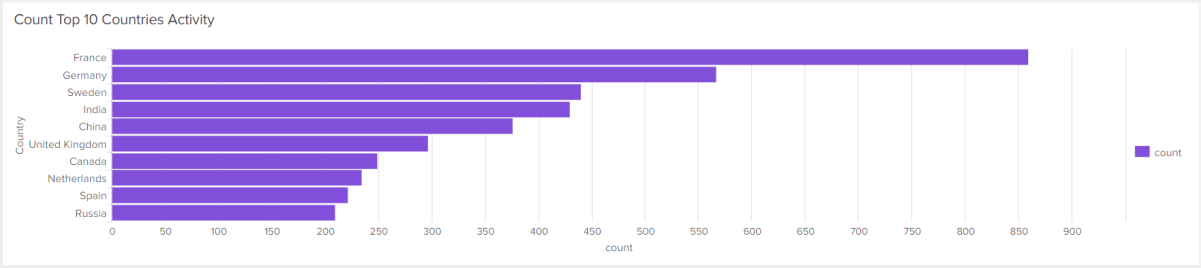
From the attack log, it is possible to detect changes in response code 200 and 404. There is an increase in 404, which indicates that the requested resource could not be found on the server. And a decrease in code 200, which indicates that the client's request has been successfully processed by the server.



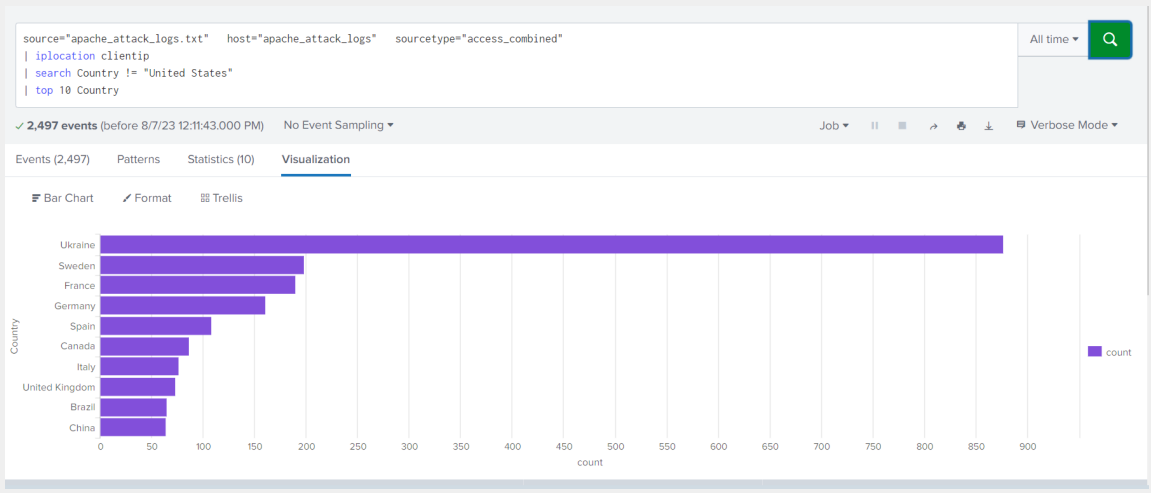
Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

Yes, filter by country and excluding United states, there is a increase in international activity
From normal Apache Logs

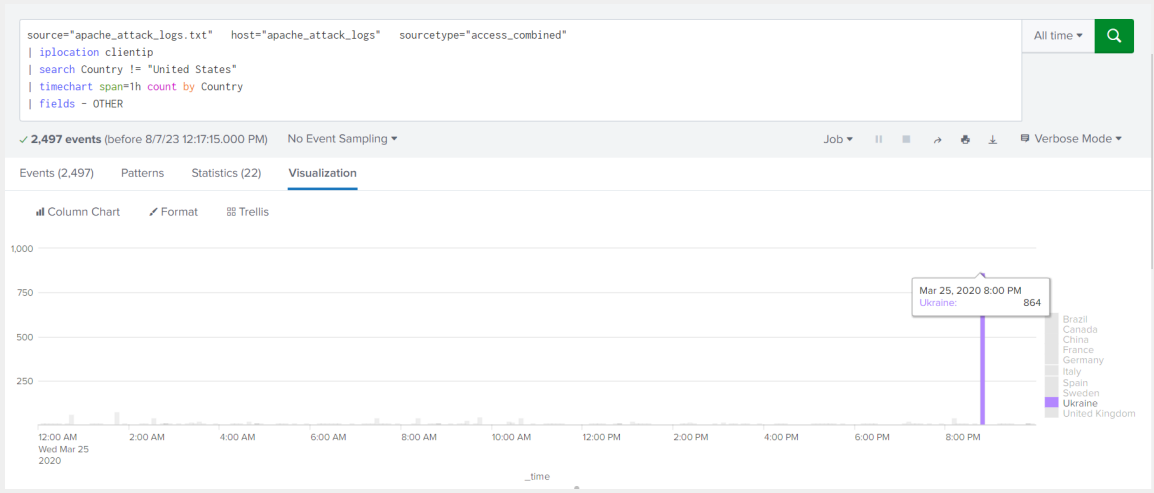


Attack Logs:



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

864 at 20:00 on the 25-03-2020



- Would your alert be triggered for this activity?

No alert was triggered.

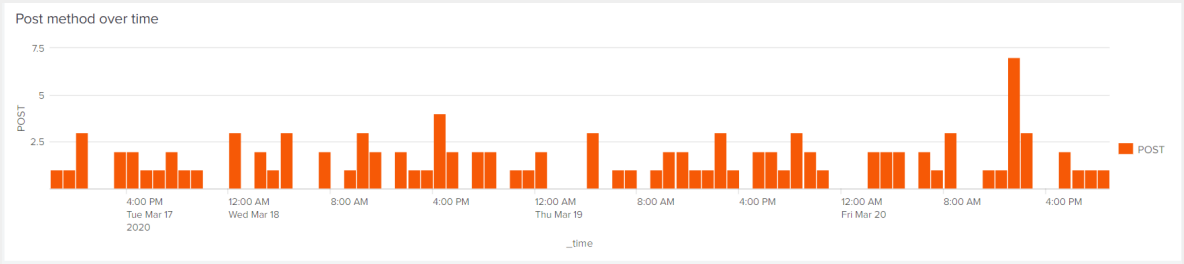
- After reviewing, would you change the threshold that you previously selected?

Yes, considering activities from other countries except from the United States, a new threshold could be set over 200.

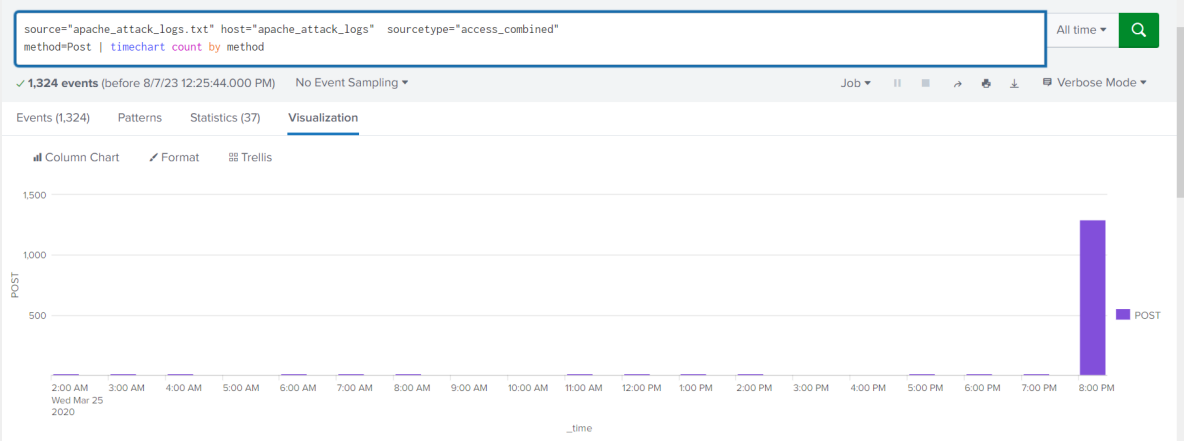
Alert Analysis for HTTP POST Activity

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

Yes
From the server logs, activity is pretty steady.



But from the attack log, there is an increase in POST request.



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

1296

- When did it occur?

At 20:00:00 on the 25-03-2020

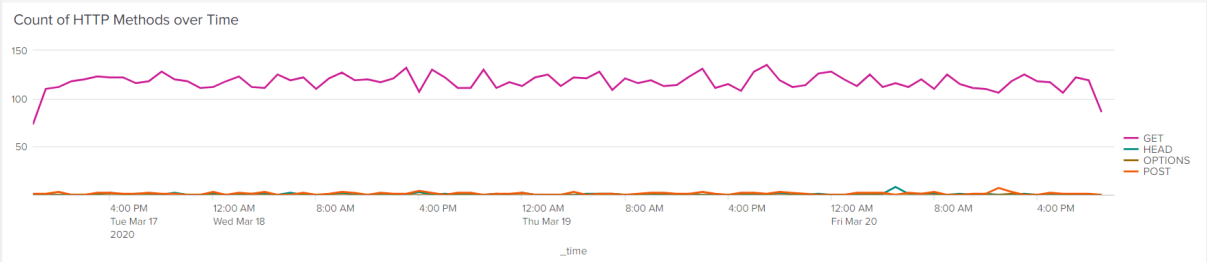
- After reviewing, would you change the threshold that you previously selected?

Yes, in this case anything over 100 POST requests per hour might be suspicious.

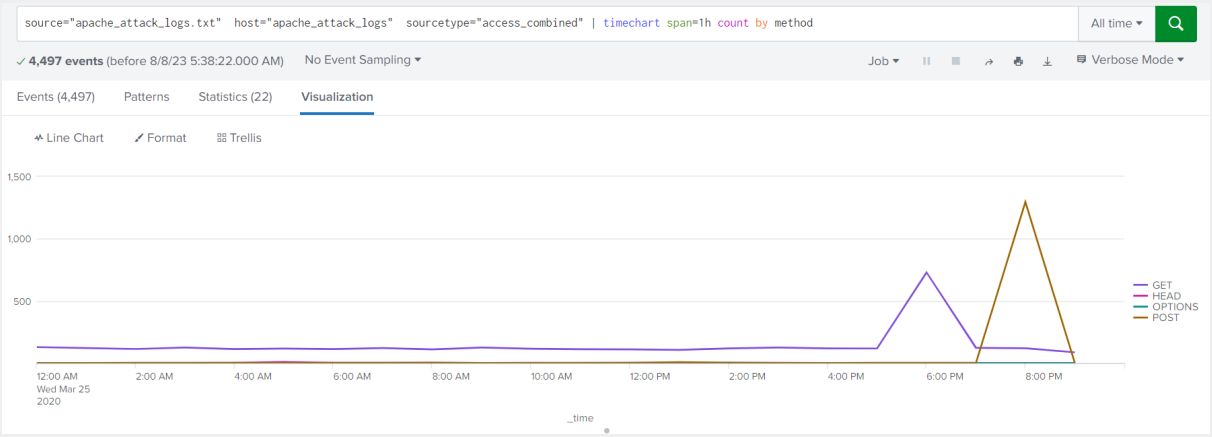
Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

Under normal circumstances, there is a steady behavior of GET requests. The chart looks like



Using the attack log file, there is a very unusual spike of POST requests.



- Which method seems to be used in the attack?

POST

- At what times did the attack start and stop?

Between 20:00 and 21:00

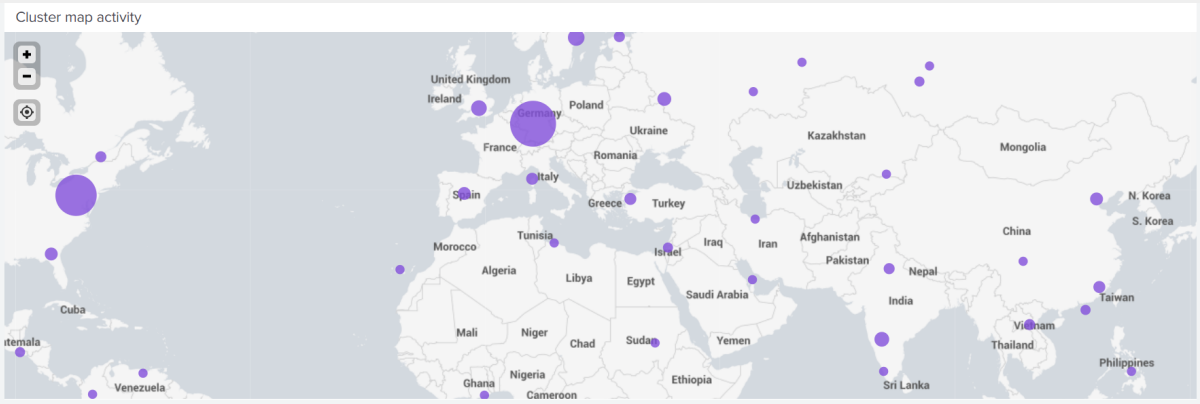
- What is the peak count of the top method during the attack?

1296

Dashboard Analysis for Cluster Map

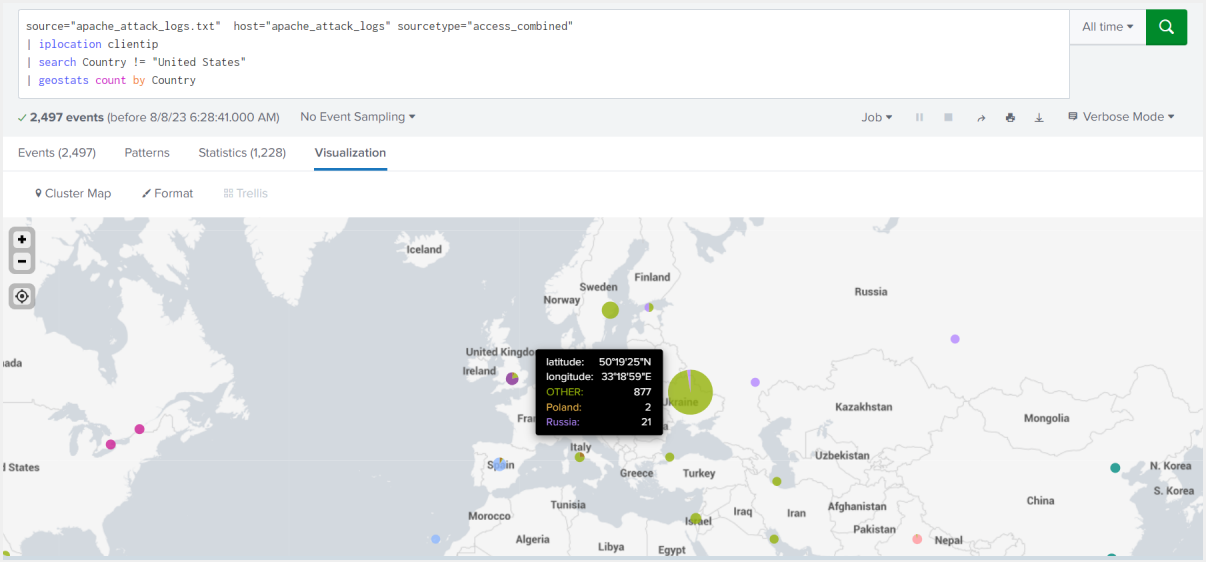
- Does anything stand out as suspicious?

From the dashboard map, normal activity looks like in the image below.



Using the attack log for Apache, excluding the United States in this case,

there is abnormal activity from the Ukraine.



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

From Kiev and Kharkiv in the Ukraine.

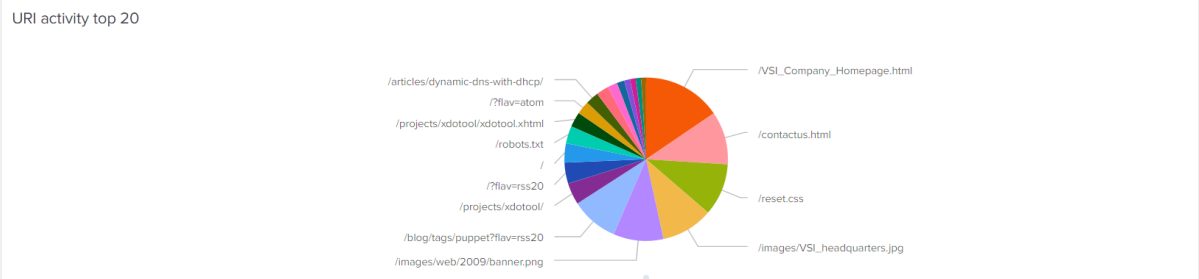
- What is the count of that city?

```
Kiev: 440
Kharkiv: 432
```

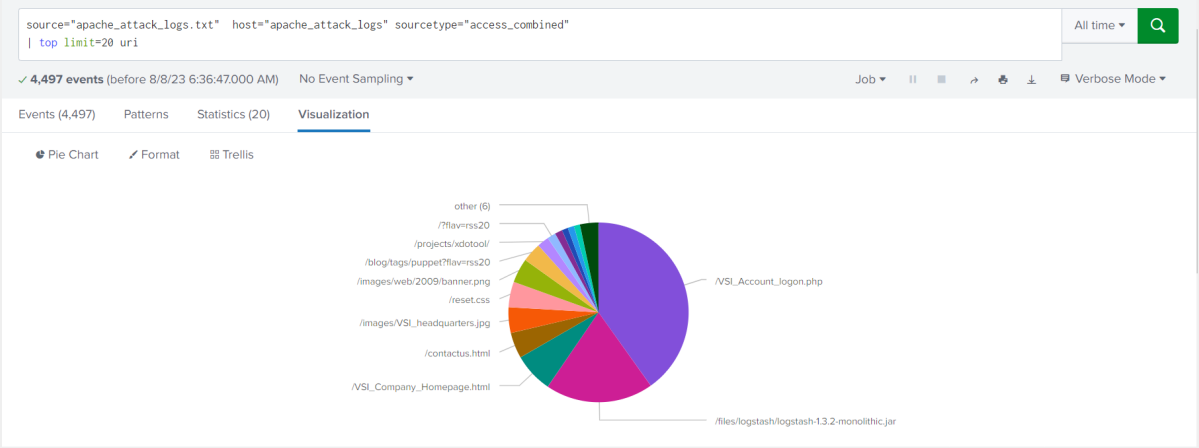
Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

From the Apache log file, normal activity looks like in the image below.



From the attack log file, there is an increase in activity on /VSI_Account_logon.php and /files/logstash/logstash-1.3.2-monolithic.jar. Graph looks like the image below.



- What URI is hit the most?

`VSI_Account_logon.php`

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

Attackers might be trying to login, either using a brute force technique or an injection attack (SQL most likely).