Cybersecurity

Project 3 Review Questions

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

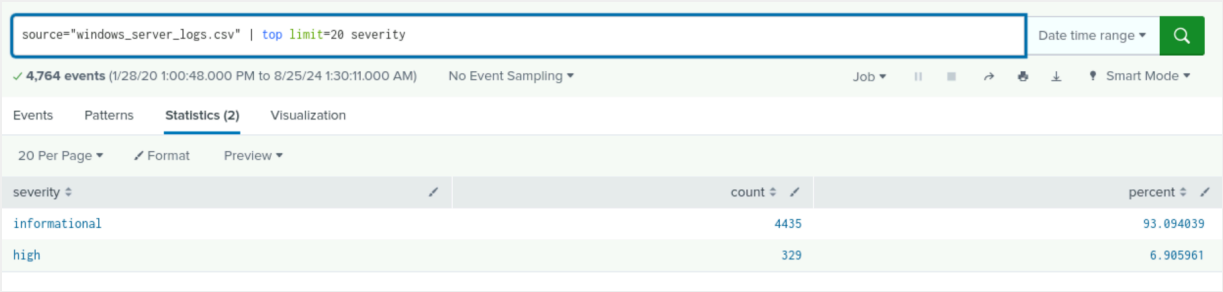
Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

Yes, the change occurred on the high severity scale, the count was 329 and now is 1111 of the count, and the informational severity decreased by 6% of the count.

Windows_logs:

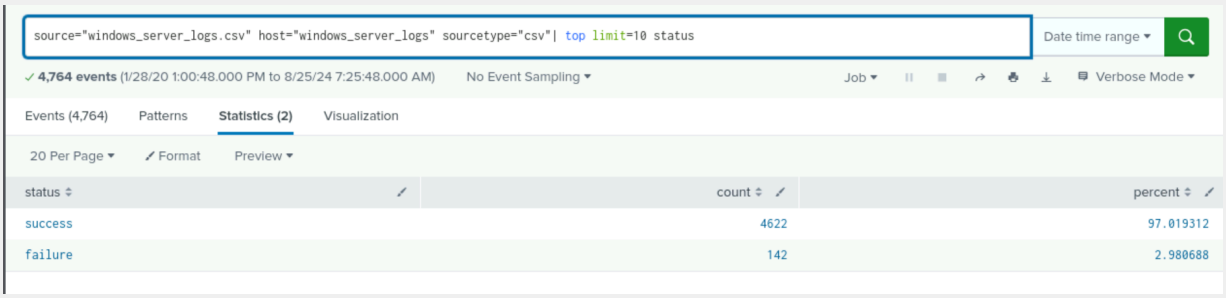


Attack_logs:

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

We noticed some changes between the server_logs and the server_attack_logs, there were more successes than failures after the attack.
Windows_logs:



Attack_logs:

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

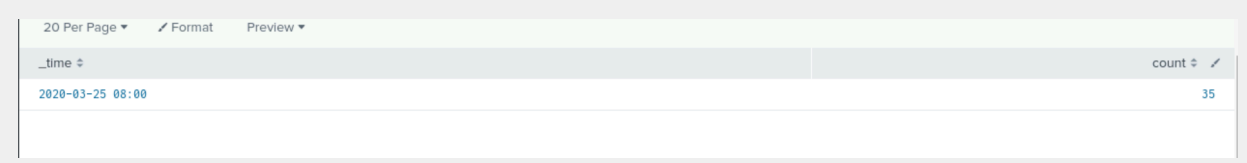
Yes, the alert detected a volume of failed activity

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

35 failed windows activity.

- When did it occur?

March/25/2020 at 8:00



- Would your alert be triggered for this activity?

```
Yes, the alert has been triggered and exceeded our threshold.
```

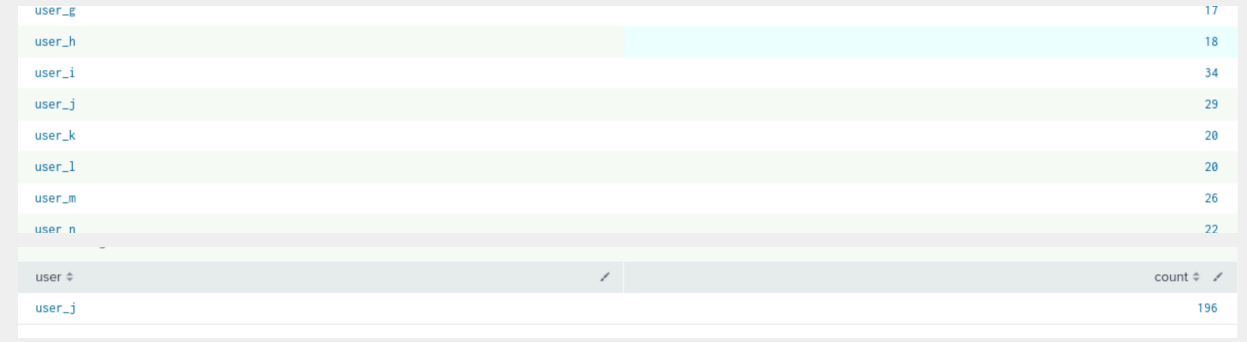
- After reviewing, would you change your threshold from what you previously selected?

```
No, the alert was perfectly set up to be triggered by the attack, so we can have the exact activity without getting any false positives.
```

Alert Analysis for Successful Logins

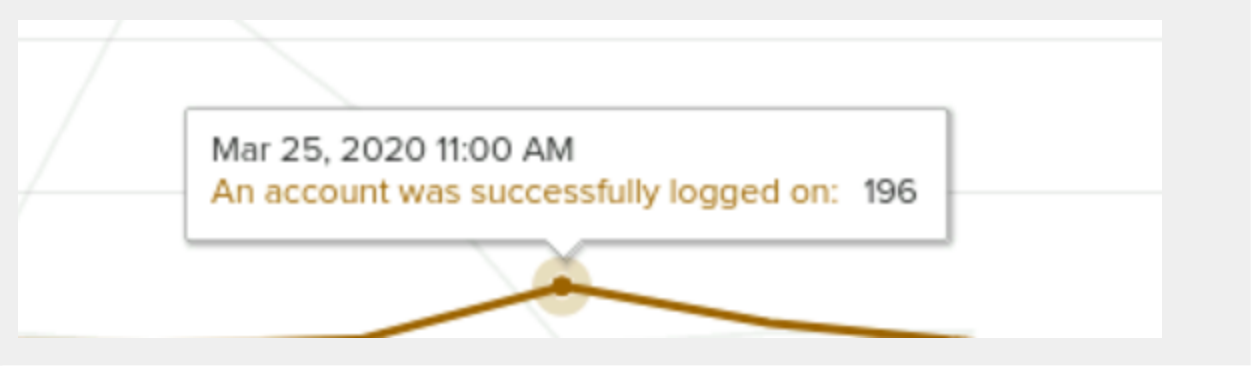
- Did you detect a suspicious volume of successful logins?

```
Yes, there was an increase on the loggins by one user
```



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

```
196 at 11:00 am
```



- Who is the primary user logging in?

```
User_j
```

user	count
user_j	196

- When did it occur?

```
march-25-2020
```

- Would your alert be triggered for this activity?

```
The alert was successfully triggered
```

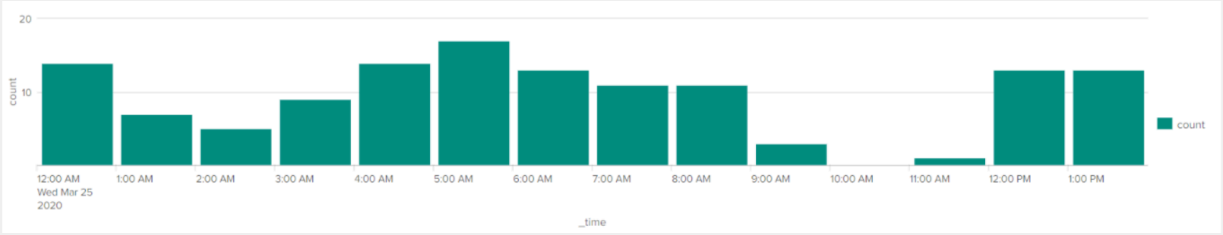
- After reviewing, would you change your threshold from what you previously selected?

```
No, it worked perfectly.
```

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
Yes, there was a suspicious amount of the deleted accounts but not in
excessive numbers.
```

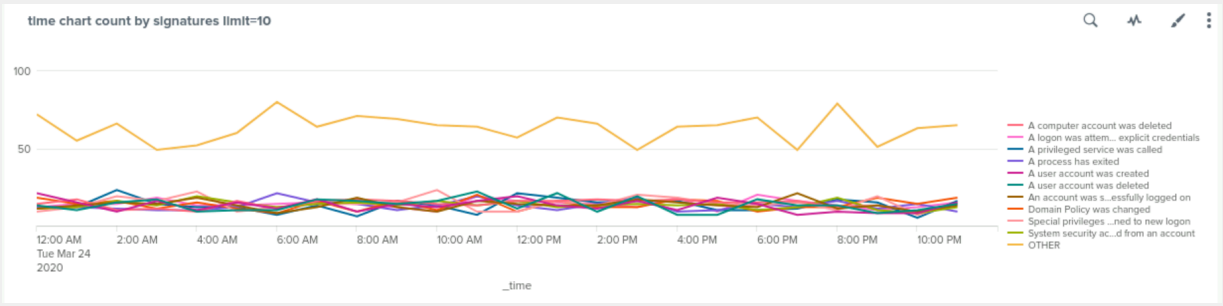


Dashboard Analysis for Time Chart of Signatures

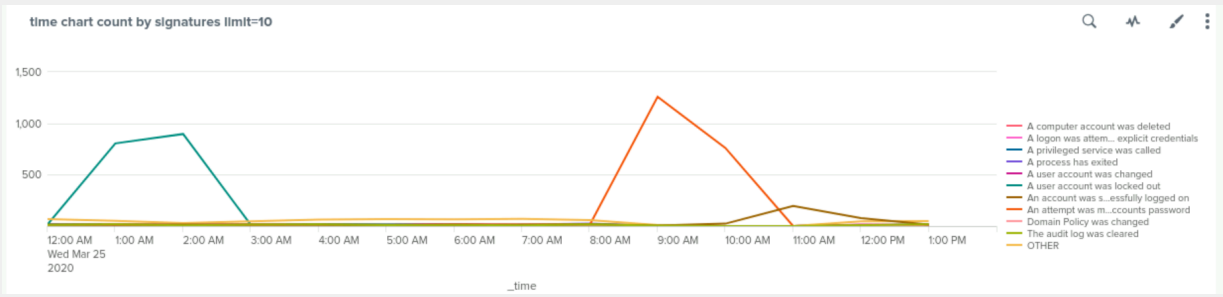
- Does anything stand out as suspicious?

Yes, there was a significant change on the signatures: “An attempt was made to reset an accounts password: 1,258 at 9:00am” and “A user account was locked out: 896 at 2:00am”

Windows_logs:



Attack_logs:



- What signatures stand out?

“An attempt was made to reset an accounts password”, “A user account was locked out”

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

```
A user account was locked out, started: 12:00 am - ended: 3:00 am
An attempt was made to reset an account's password, started: 8:00 am -
ended: 11:00 am.
```

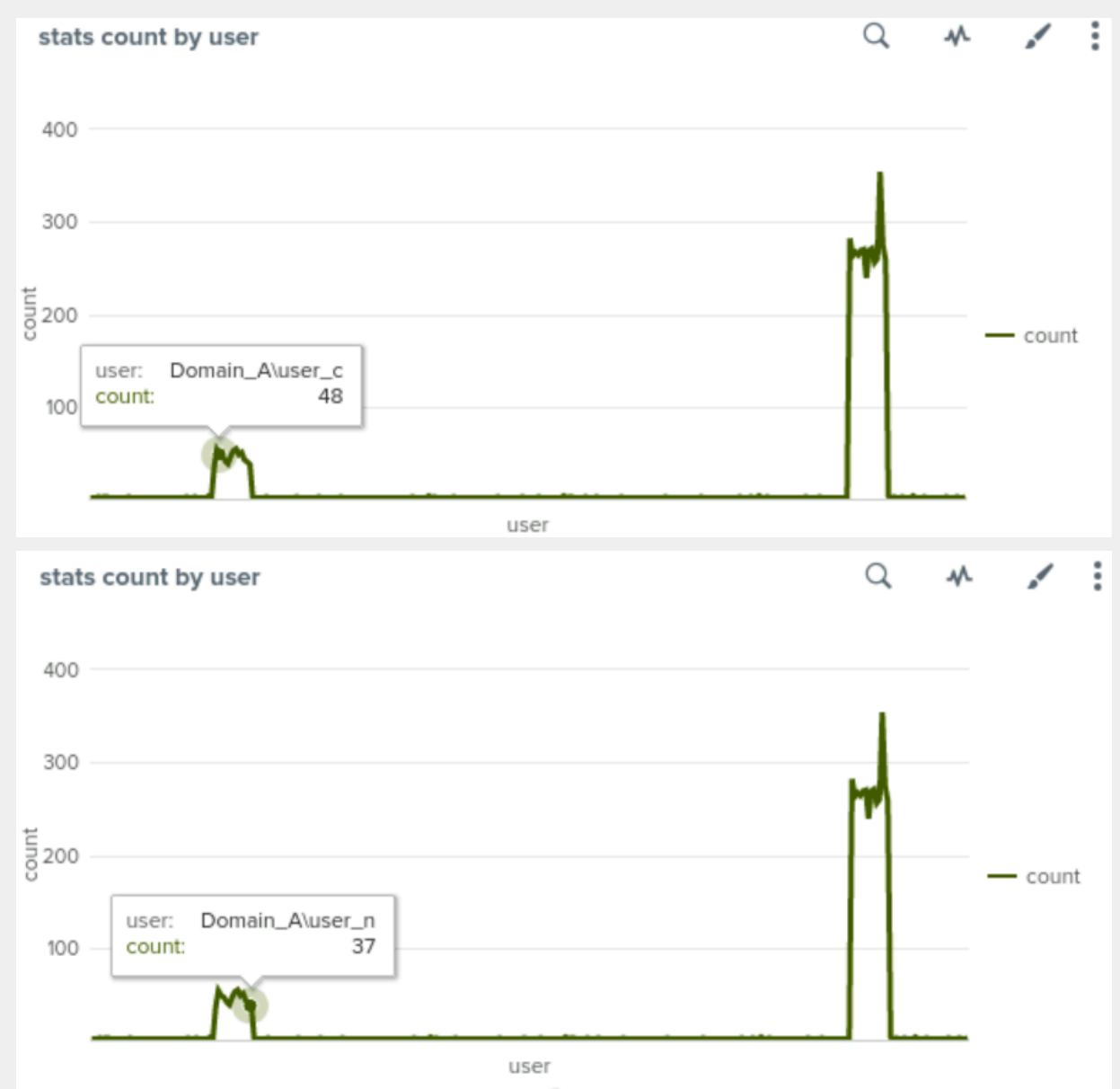
- What is the peak count of the different signatures?

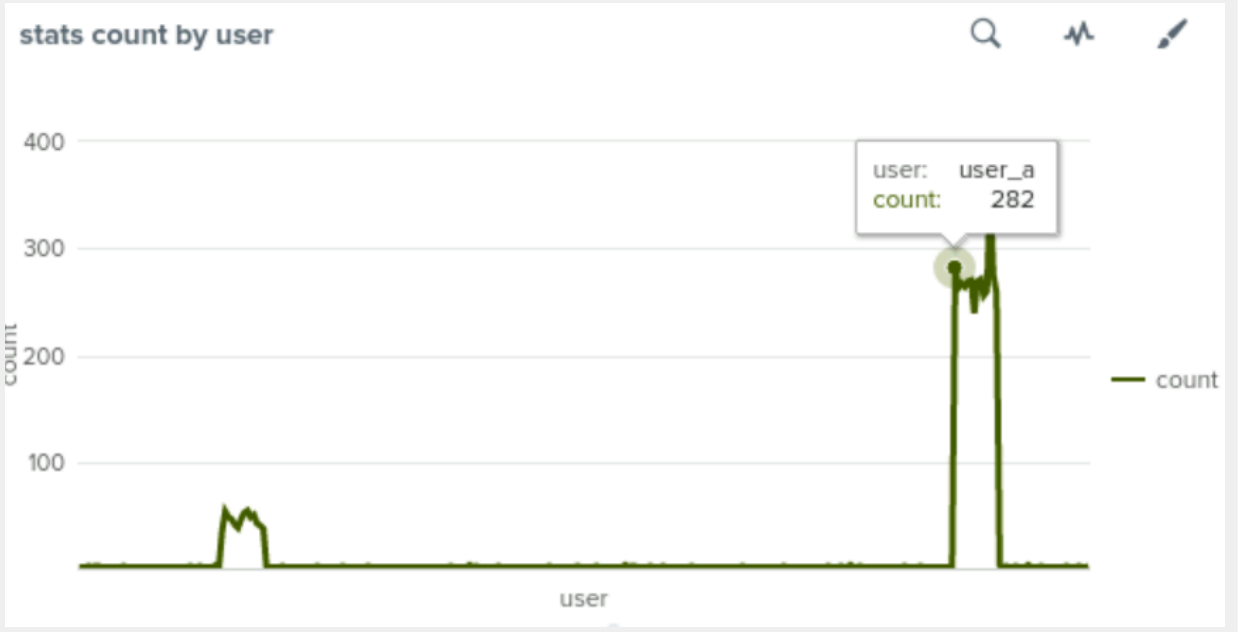
```
“A user account was locked out: 896”
“An attempt was made to reset an accounts password: 1,258”
```

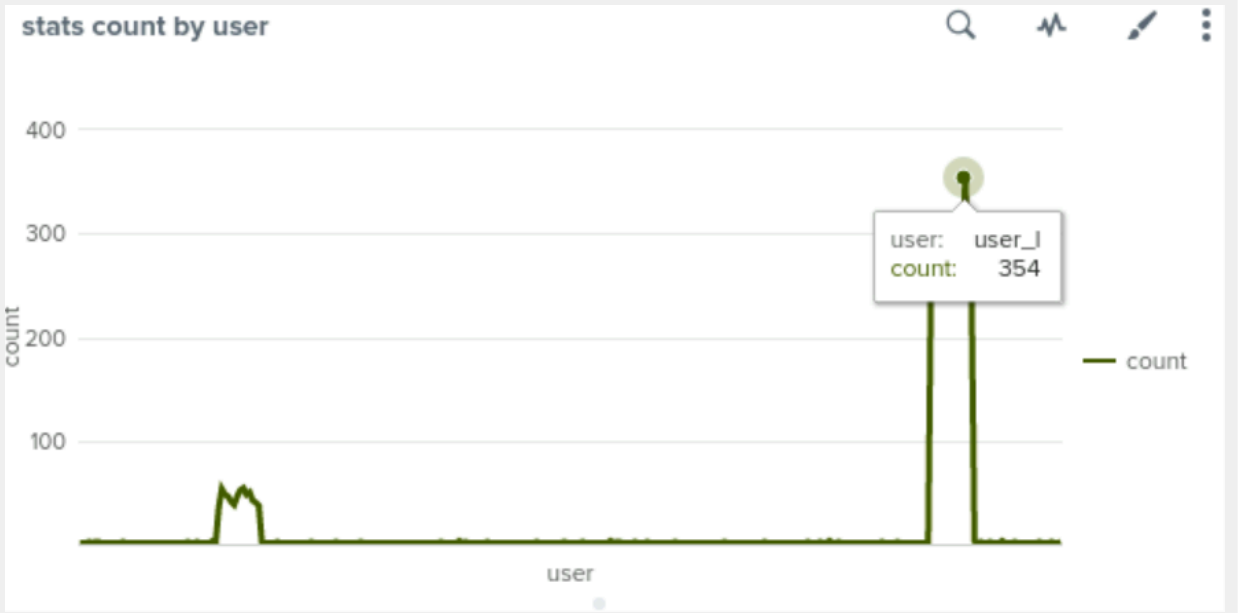
Dashboard Analysis for Users

- Does anything stand out as suspicious?

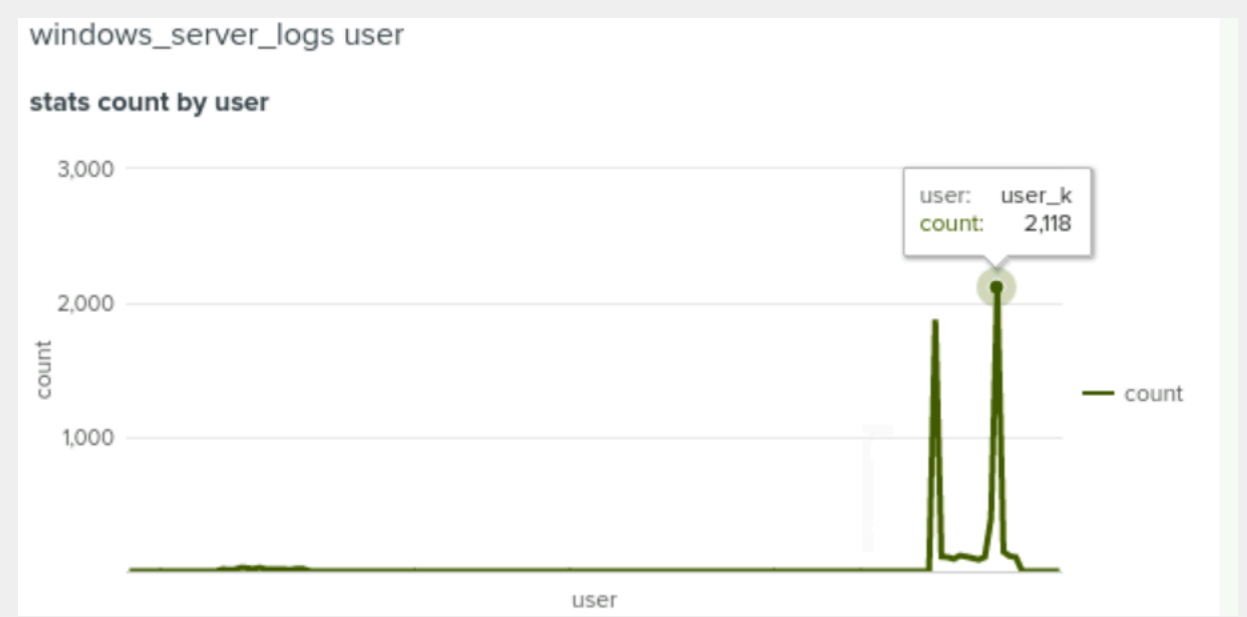
```
There was an increase in the activity of two users.
Windows_logs:
```

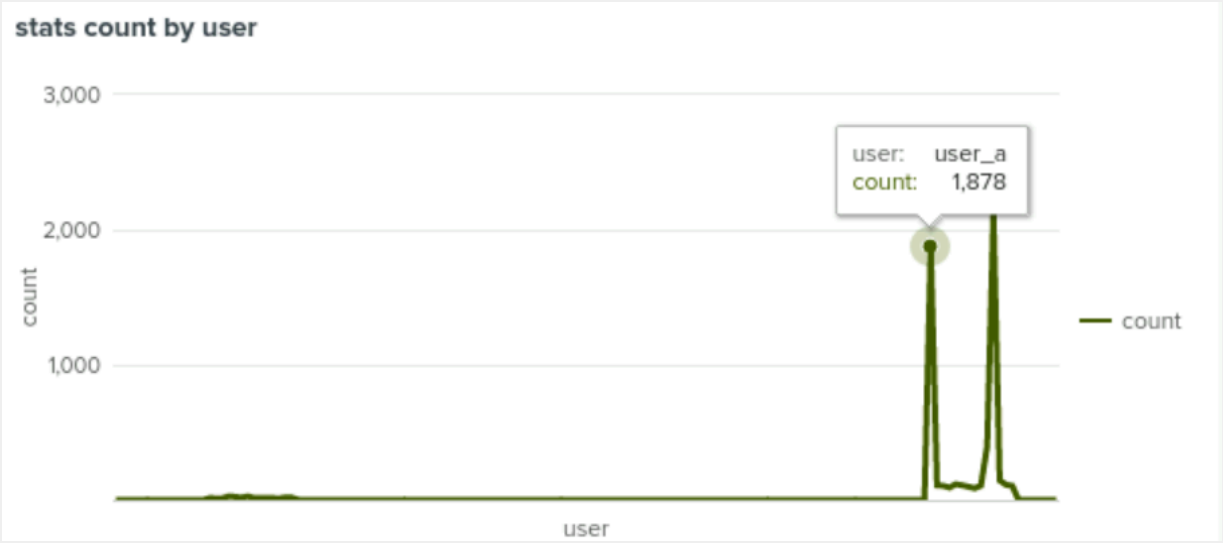

stats count by user
400
300
200
100
count
user: Domain_A\user_c
count: 48
count
user
stats count by user
400
300
200
100
count
user: Domain_A\user_n
count: 37
count
user


stats count by user
400
300
200
100
count
user: user_a
count: 282
count
user


stats count by user
400
300
200
100
count
user: user_l
count: 354
count
user

Attack_logs:





- Which users stand out?

```
User_a and user_k
```

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

```
User_a: between 1:00 am and 2:00am.
User_k: between 4:00 am and 9:00am.
```

_time	OTHER	user_a	user_b	user_c	user_e	user_f	user_i	user_j	user_k	user_l	user_m
2020-03-25 02:00	9	984	3	0	1	2	0	2	2	3	1
2020-03-25 01:00	66	799	18	12	20	9	15	6	9	9	10
2020-03-25 08:00	73	18	14	7	9	12	12	13	12	25	10
2020-03-25 07:00	83	16	11	9	15	14	8	18	7	10	16
2020-03-25 05:00	75	13	6	9	14	9	10	9	13	19	15
2020-03-25 06:00	73	10	9	11	14	14	9	2	7	17	12
2020-03-25 03:00	68	8	13	8	17	9	12	8	4	17	10
2020-03-25 04:00	81	8	10	10	5	15	9	15	16	8	10
2020-03-25 13:00	65	8	5	12	9	8	11	11	15	12	8
2020-03-25 00:00	82	7	11	12	10	10	14	11	8	14	13
2020-03-25 12:00	59	4	8	10	3	6	4	82	8	6	7
2020-03-25 09:00	17	3	1	5	0	1	2	2	1256	5	1

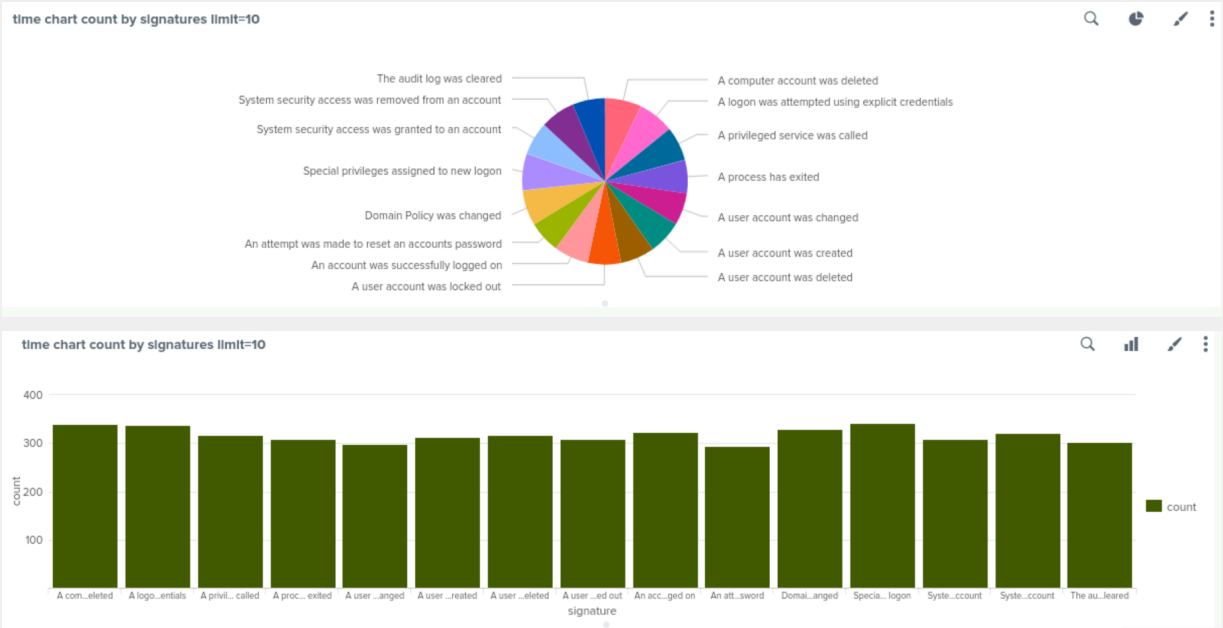
- What is the peak count of the different users?

```
User_a: 1,878.
User_k: 2,118.
```

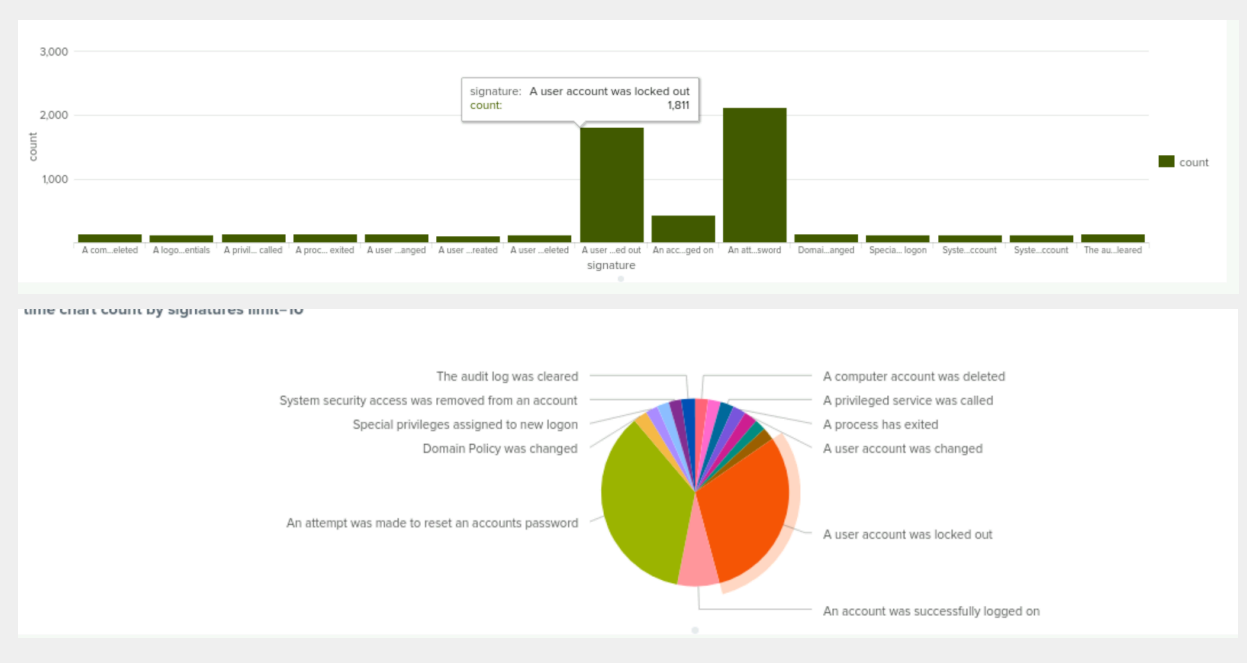
Dashboard Analysis for Signatures with Bar, Graph, and Pie Charts

- Does anything stand out as suspicious?

```
Yes, the previous activity found and a user successfully logged on.
Windows_logs:
```




```
Attack_logs:
```



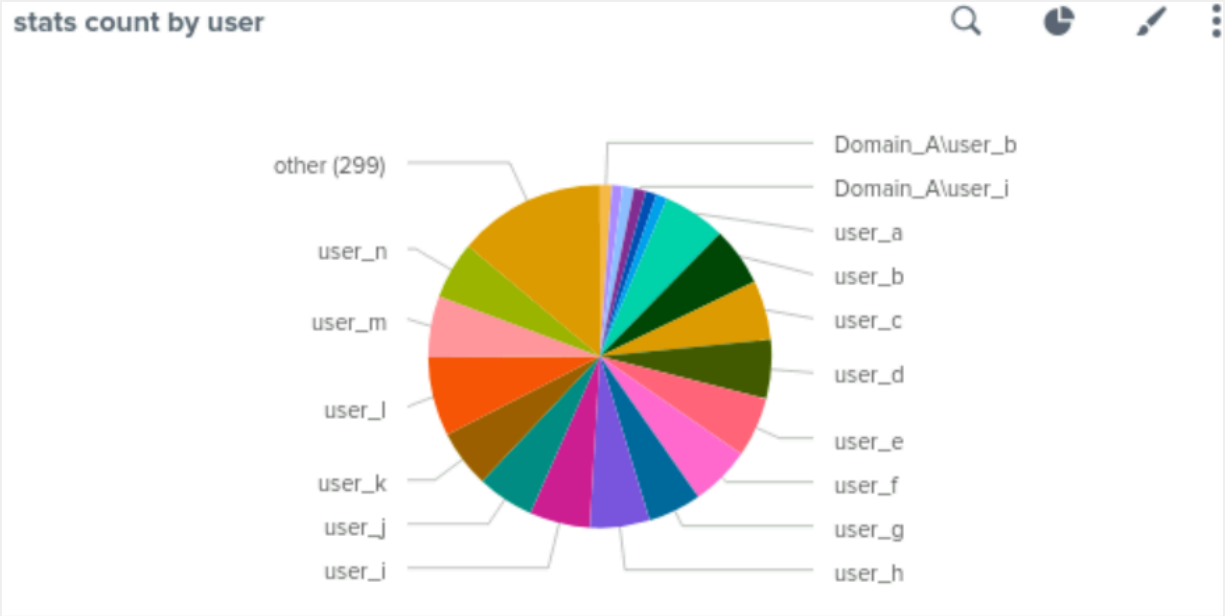
- Do the results match your findings in your time chart for signatures?

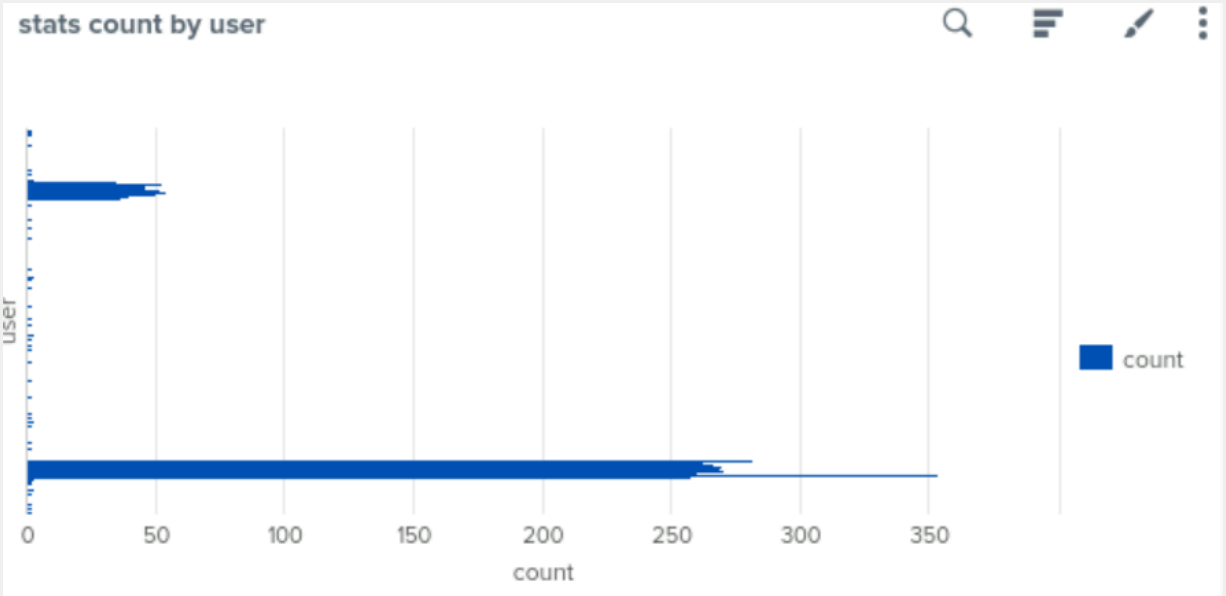
```
yes
```

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

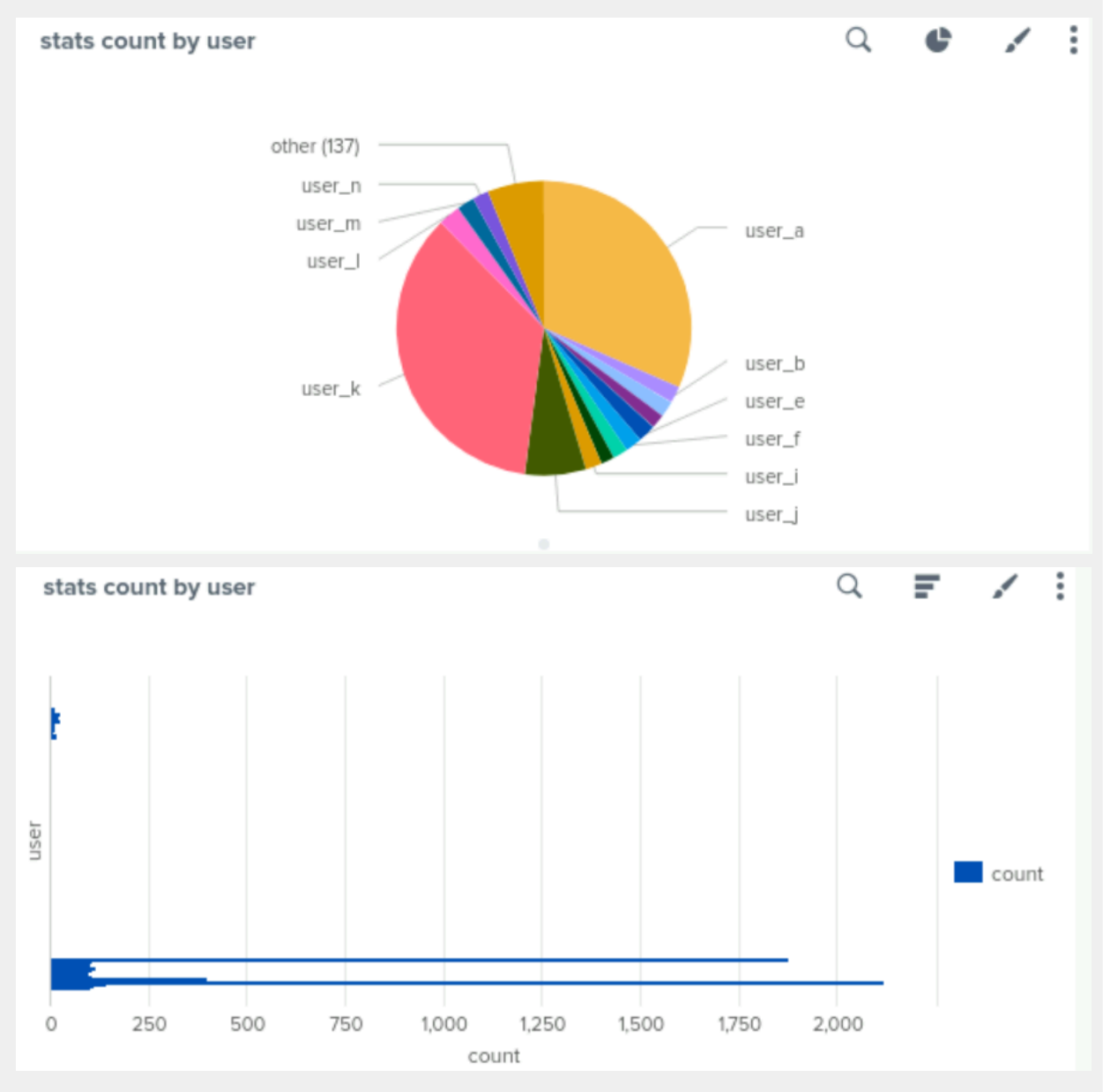
- Does anything stand out as suspicious?

```
Yes, user_a and user_k are the main users with the most activity.
Windows_logs:
```


stats count by user
other (299)
user_n
user_m
user_l
user_k
user_j
user_i
Domain_A\user_b
Domain_A\user_i
user_a
user_b
user_c
user_d
user_e
user_f
user_g
user_h


stats count by user
user
0
50
100
150
200
250
300
350
count
count

Attack_logs:



- 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 advantages of using a statistical time chart for the users is that it show you the time and date of any user and also shows the count when you need it, and the disadvantages of using a pie chart is that it does not specify date and time as an statistical chart, but the pie chart also shows any event of user that has increase.

Apache Web Server Log Questions

Report Analysis for Methods

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

Yes, the POST HTTP method response
Apache_logs:

method	count	percent
GET	9851	98.510000
POST	106	1.060000
HEAD	42	0.420000
OPTIONS	1	0.010000

Attack logs:

20 Per Page ▾ Format Preview ▾

method	count	percent
GET	3157	70.202357
POST	1324	29.441850
HEAD	15	0.333556
OPTIONS	1	0.022237

- What is that method used for?

POST: is a request method to send data and updates supported by HTTP used by the world wide web.

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

Yes there are some changes on the referrer domains on the top 10.

Apache_logs:

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

Attack_logs:

referer_domain	count	percent
http://www.semicomplete.com	764	49.226804
http://semicomplete.com	572	36.855670
http://www.google.com	37	2.384021
https://www.google.com	25	1.610825
http://stackoverflow.com	15	0.966495
https://www.google.com.br	6	0.386598
https://www.google.co.uk	6	0.386598
http://tuxradar.com	6	0.386598
http://logstash.net	6	0.386598
http://www.google.de	5	0.322165

Report Analysis for HTTP Response Codes

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

Yes, specially with code 200 that had a decrease and code 404 had an increase.

Apache_logs:

status	count	percent
200	9126	91.260000
304	445	4.450000
404	213	2.130000
301	164	1.640000
206	45	0.450000
500	3	0.030000
416	2	0.020000
403	2	0.020000

Attack_logs:

status	count	percent
200	3746	83.299978
404	679	15.098955
304	36	0.800534
301	29	0.644874
206	5	0.111185
500	1	0.022237
403	1	0.022237

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

Yes, there was a suspicious volume of international activity.
Apache_logs:

Country	count	percent
United States	3860	38.600000
France	859	8.590000
Germany	567	5.670000
Sweden	440	4.400000
India	430	4.300000
China	376	3.760000
United Kingdom	297	2.970000
Canada	249	2.490000
Netherlands	235	2.350000
Spain	222	2.220000

Attack_logs:

Country	count	percent
United States	2000	44.474094
Ukraine	877	19.501890
Sweden	198	4.402935
France	190	4.225039
Germany	161	3.580165
Spain	108	2.401601
Canada	87	1.934623
Italy	77	1.712253
United Kingdom	73	1.623304
Brazil	65	1.445408

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

- Would your alert be triggered for this activity?

```
Yes, our alert baseline and threshold was set on task.
```

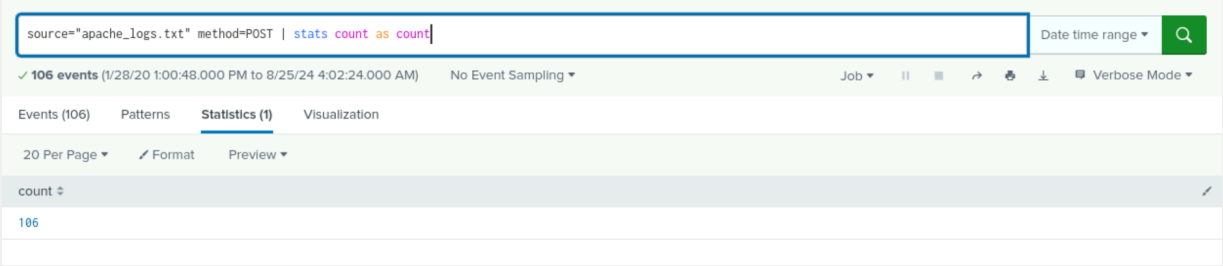
- After reviewing, would you change the threshold that you previously selected?

```
No, it gave us the information we were looking for.
```

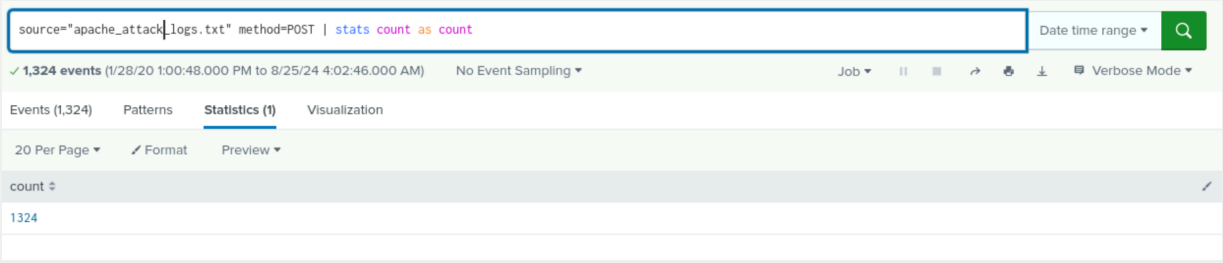
Alert Analysis for HTTP POST Activity

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

```
Yes, it was a volume of 1,218 more POST activity.
Apache_logs:
```




```
Attack_logs:
```



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

```
1296 at 8:00pm
```

- When did it occur?

```
Wednesday March-25-2020
```

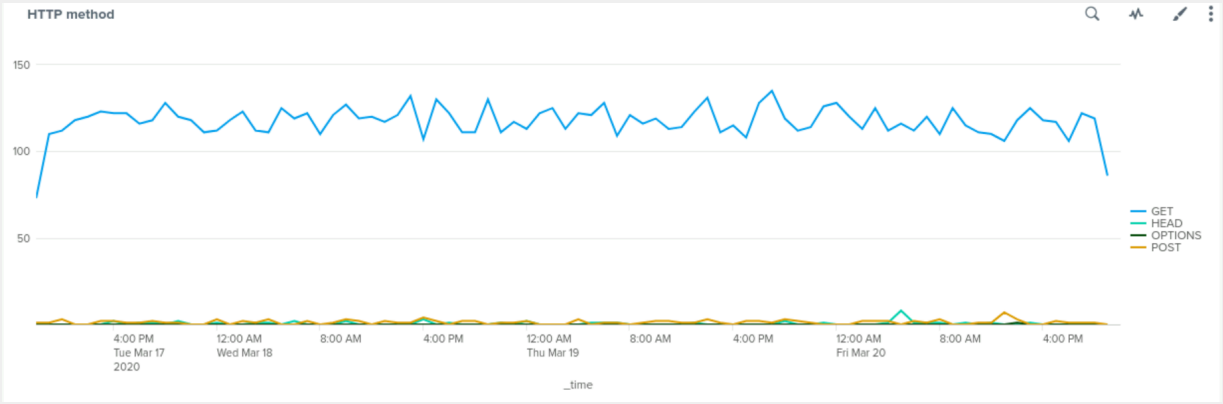
- After reviewing, would you change the threshold that you previously selected?

```
No, I won't change it, it was accurate.
```

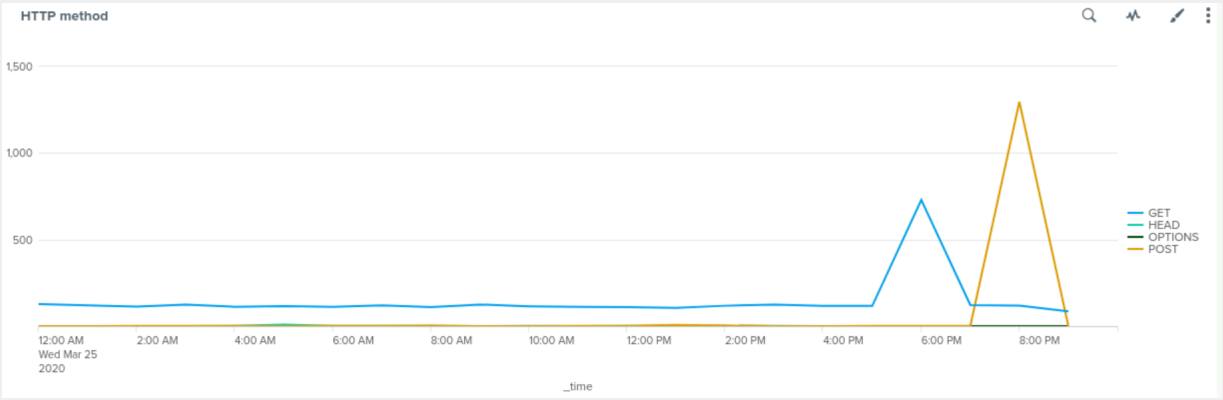
Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
There is an increase in POST activity and the GET activity went down.
Apache_log:
```




```
Attack_logs:
```



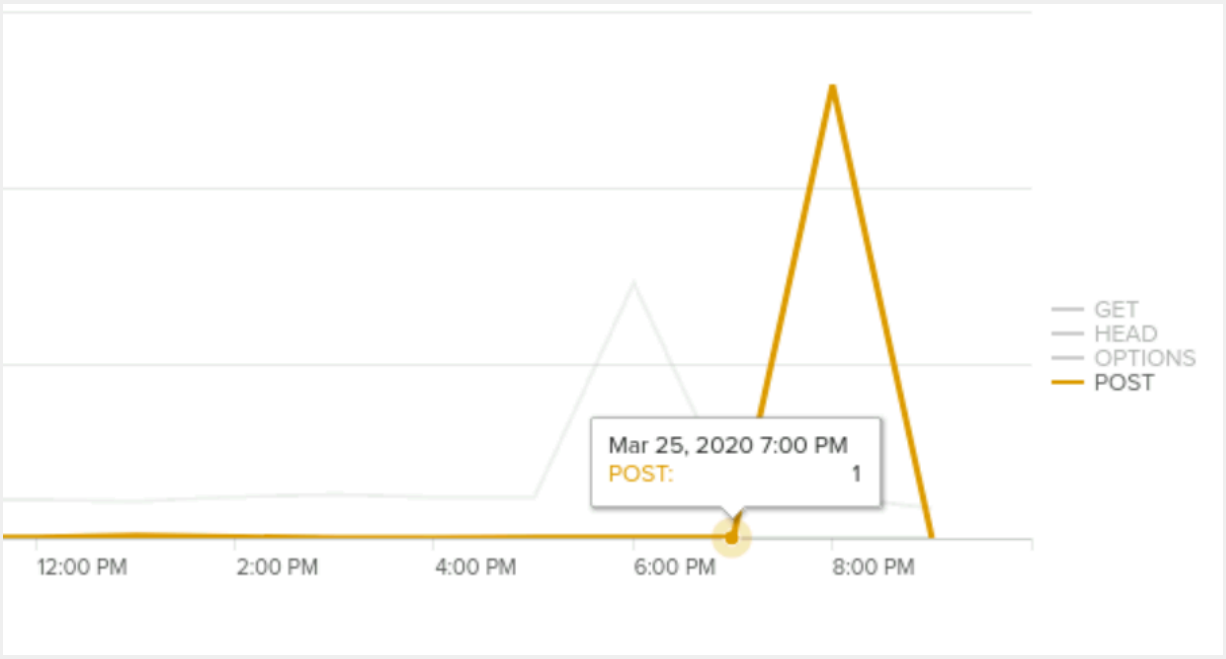
- Which method seems to be used in the attack?

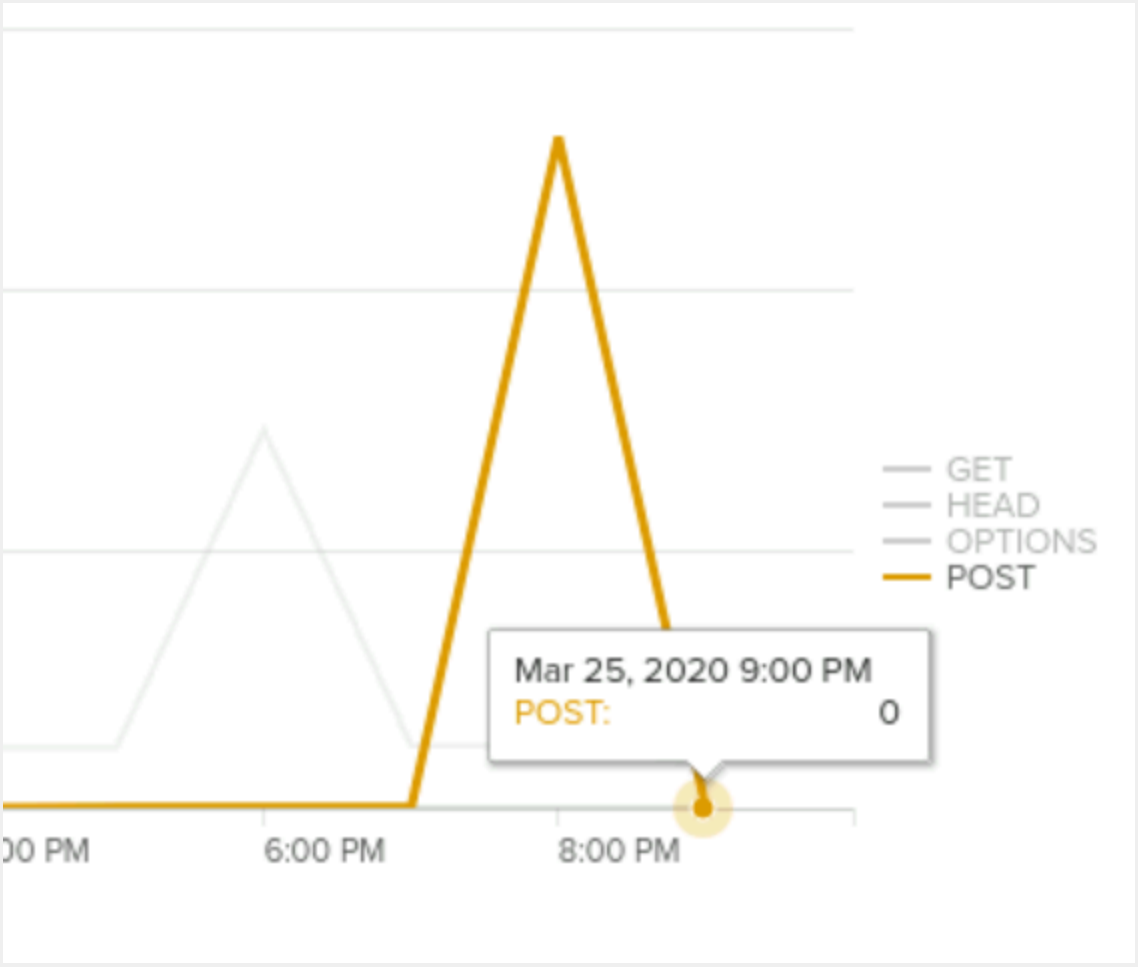
```
POST | GET
```

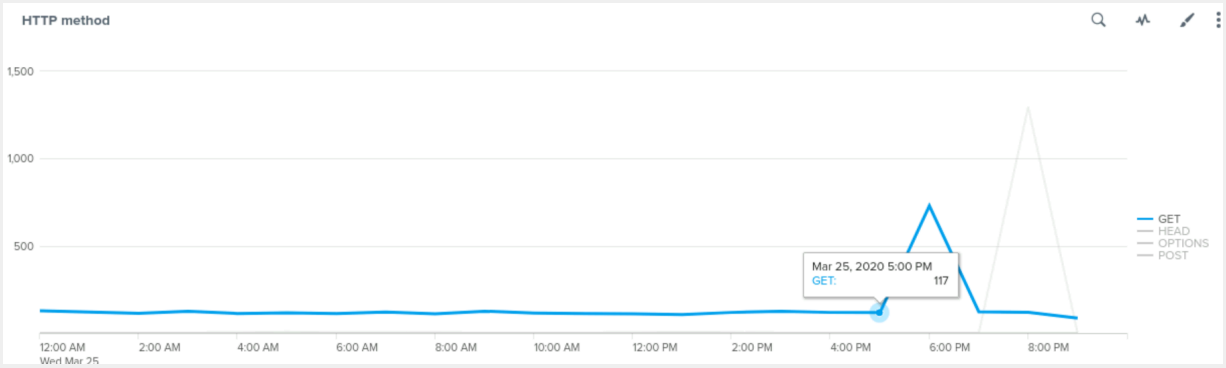
- At what times did the attack start and stop?

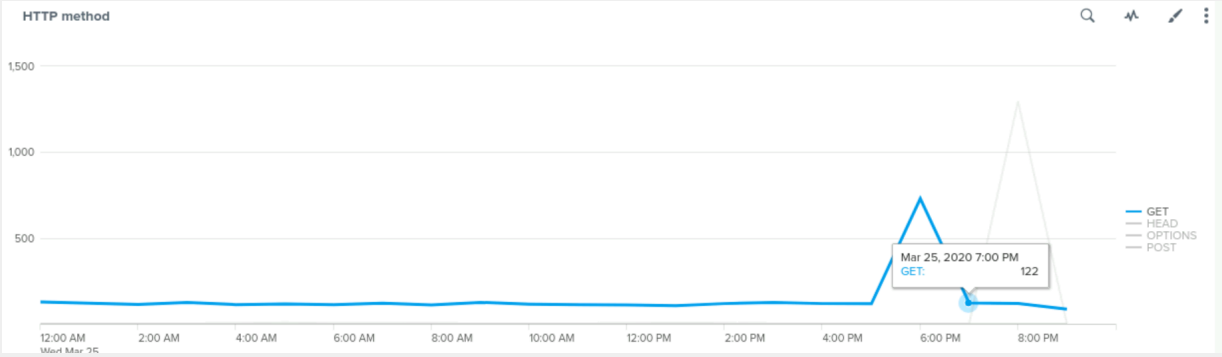
```
POST: started at 7:00pm and stopped at 9:00pm
```

GET: started at 5:00pm and stopped at 7:00pm



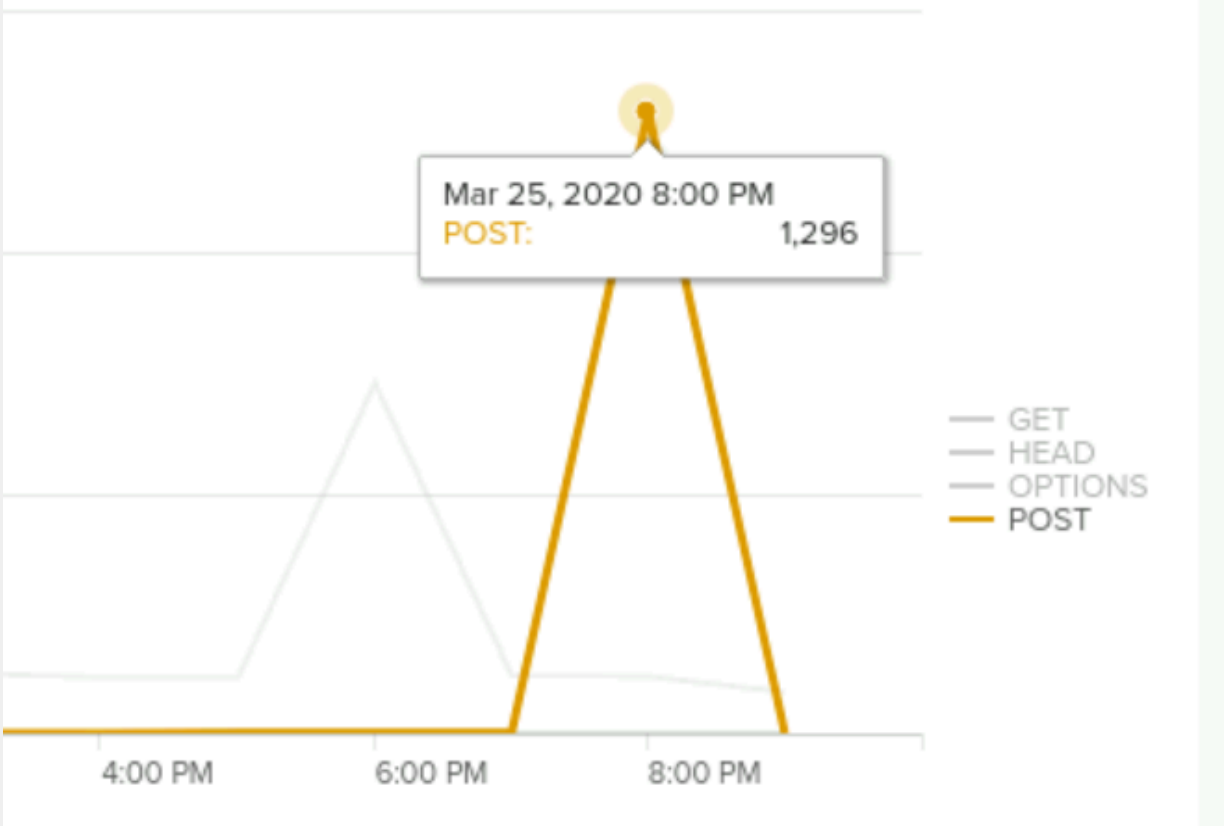

GET
HEAD
OPTIONS
POST
Mar 25, 2020 9:00 PM
POST: 0
00 PM
6:00 PM
8:00 PM

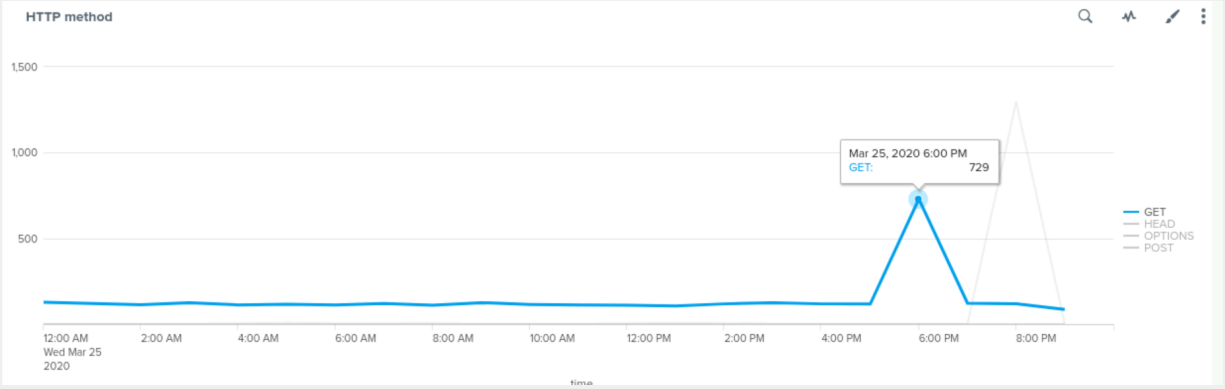

HTTP method
1,500
1,000
500
Mar 25, 2020 5:00 PM
GET: 117
GET
HEAD
OPTIONS
POST
12:00 AM
Wed Mar 25
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM



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

POST:1,296
GET: 729

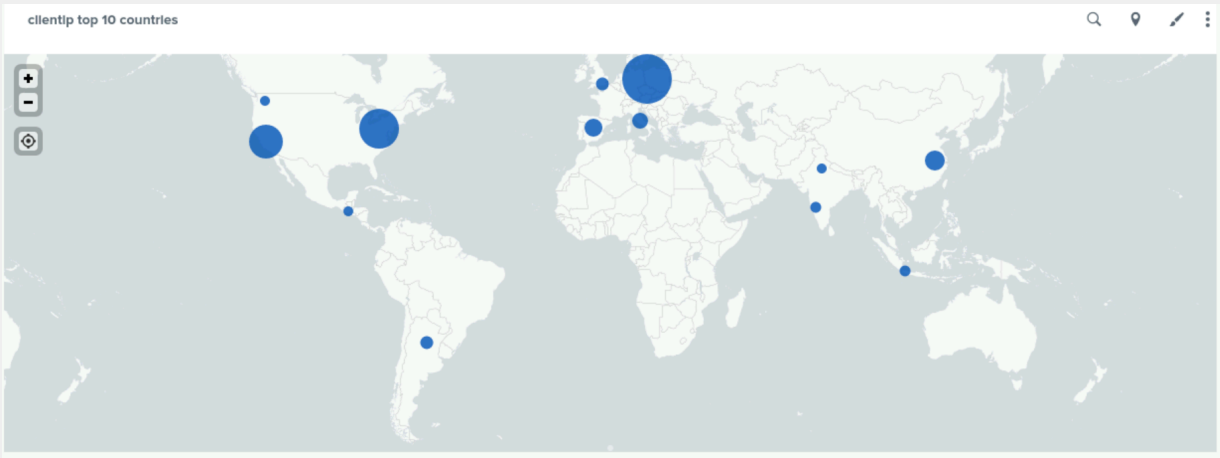




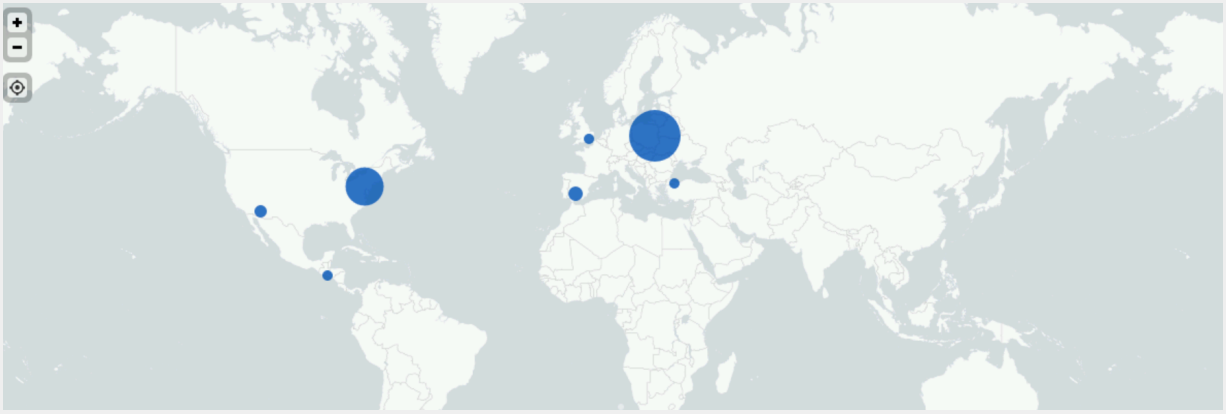
Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

Apache_logs:



Attack_logs:



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

```
Spain= Madrid
Morocco= Rabat
France= Paris, strasbourg
Ukraine= Kiev, Kharkiv
U.K= London
Italy= Millan
Germany= Dresden
Turkey= Istanbul
El salvador= San salvador
Russia= Moscow
Sweden= stockholm, Umea
United States=
   ● Arizona= Phoenix
   ● Kentucky= Frankfort
   ● Virginia= Washington, D.C
   ● New York
   ● Massachusetts= Boston
Canada= toronto
```

- What is the count of that city?

```
Spain: Madrid=2
Morocco: Rabat=1
France: Paris=1, strasbourg=3
Ukraine: Kiev=6, Kharkiv=3
U.K: London=1
Italy: Millan=1
Germany: Dresden=1
Turkey= Istanbul=1
El salvador: San salvador=1
Russia: Moscow=1
Sweden: Stockholm=3, Umea=1
United States:
   ● Arizona: Phoenix=2
   ● Kentucky: Frankfort=1
   ● Virginia: Washington, D.C=4
   ● New York=6
   ● Massachusetts: Boston=1
```

```
Canada: Toronto=1
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes the URI_PATH Data shows suspicious activity.
```

- What URI is hit the most?

```
/VSI_Account_logon.php.
```

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

```
The attacker potentially is doing a brute force attack.
```