Cybersecurity

Project 3 Review Questions

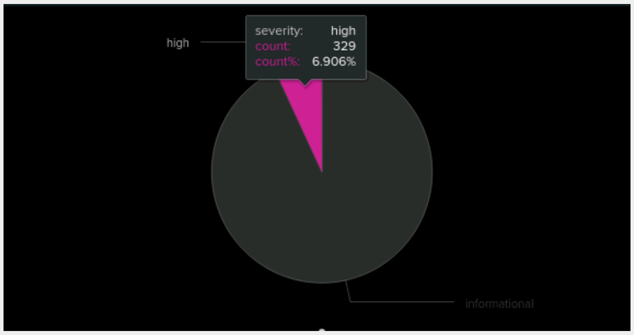
Make a copy of this document before you begin. Place your answers below each question.

Windows Server Log Questions

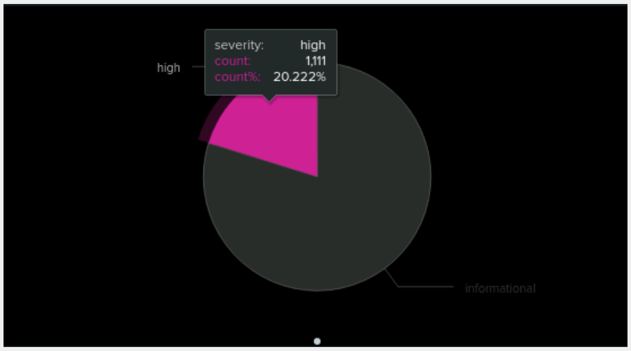
Report Analysis for Severity

- Did you detect any suspicious changes in severity?

Yes we did, “high severity” events jumped from 329 to 1111 on the day of the attack, March 25, 2020.



pre-attack



post-attack

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

The normal rate of Failed activities dropped from 142 to 93 on March 25, 2020.

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

Yes we did. Normal rate of failed activity pre attack was 6/hour with a high of 10 over the course of the day. At 8:00 a.m. on March 25, 2020, we saw a huge spike. It is also noteworthy that after the user “finleyfancy” logged on using explicit credentials at 8:30 a.m., we start to see a spike in failed activities from other users. This could be an indicator of lateral movement.

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

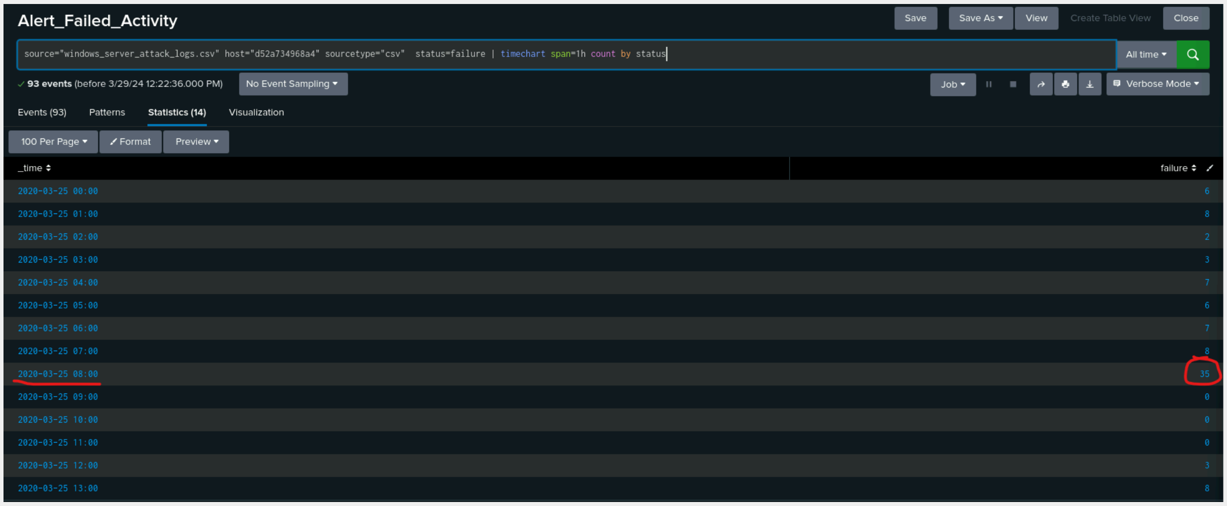
35 events.

- When did it occur?

8:00 a.m.on Wednesday, March 25, 2020.

- Would your alert be triggered for this activity?

Our threshold was set to 15 failed activities/hour to trigger this alert, so yes, it would be triggered as seen in the screenshot below, these events really stood out.



```
source="windows_server_attack_logs.csv" host="d52a734968a4" sourcetype="csv"  status=failure | timechart span=1h count by status
```

✓ **93 events** (before 3/29/24 12:22:36.000 PM)

_time	failure
2020-03-25 00:00	6
2020-03-25 01:00	8
2020-03-25 02:00	2
2020-03-25 03:00	3
2020-03-25 04:00	7
2020-03-25 05:00	6
2020-03-25 06:00	7
2020-03-25 07:00	8
2020-03-25 08:00	35
2020-03-25 09:00	0
2020-03-25 10:00	0
2020-03-25 11:00	0
2020-03-25 12:00	3
2020-03-25 13:00	8

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

```
No, we believe this is a good balance between detecting suspicious activity
and mitigating false positives.
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
Yes we did. The average jumped from 13.45/hour to 30.85/hour
```

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

```
The alert detected 196 events at 11:00 a.m. and 75 events at 12:00 p.m. on
March 25, 2020.
```

- Who is the primary user logging in?

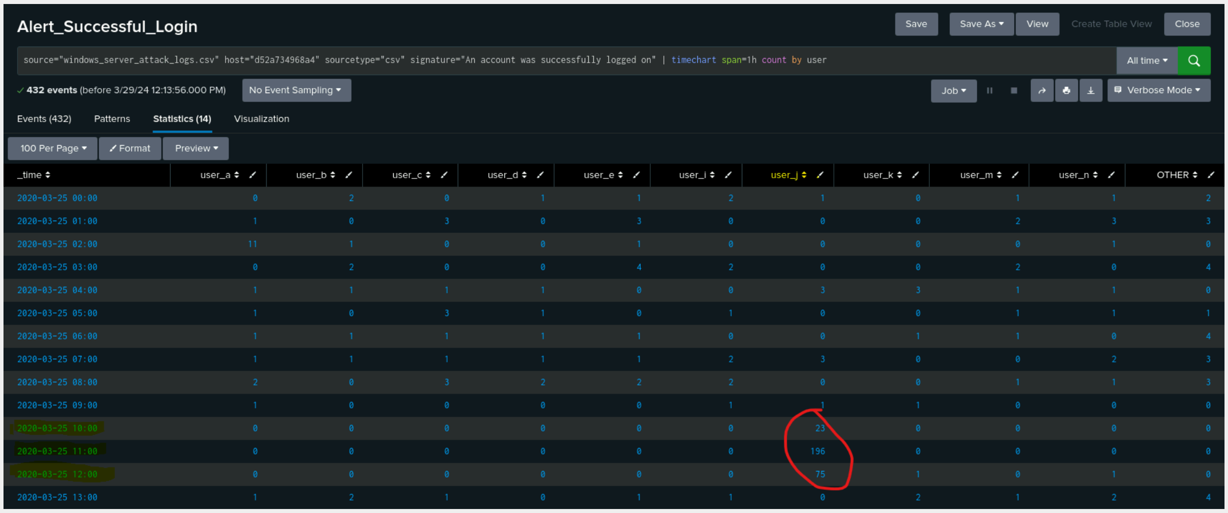
```
The primary user logging on during this time is user_j
```

- When did it occur?

Between 10:00 a.m. and 12:00 p.m., we can see user_j perform 293 successful account logins

- Would your alert be triggered for this activity?

Partially, our threshold for successful logins was set at 25/hour. We would have missed the initial wave of logins at 10:00 a.m. which came in at 23 for user_j. After that, however, our alert would have triggered at 11:00 a.m. and then again at 12:00 p.m. As we can see in the screenshot below of successful hourly logins per user.



```
source="windows_server_attack_logs.csv" host="d52a734968a4" sourcetype="csv" signature="An account was successfully logged on" | timechart span=1h count by user
```

✓ **432 events** (before 3/29/24 12:13:56.000 PM)

_time	user_a	user_b	user_c	user_d	user_e	user_i	user_j	user_k	user_m	user_n	OTHER
2020-03-25 00:00	0	2	0	1	1	2	1	0	1	1	2
2020-03-25 01:00	1	0	3	0	3	0	0	0	2	3	3
2020-03-25 02:00	11	1	0	0	1	0	0	0	0	1	0
2020-03-25 03:00	0	2	0	0	4	2	0	0	2	0	4
2020-03-25 04:00	1	1	1	1	0	0	3	3	1	1	0
2020-03-25 05:00	1	0	3	1	0	1	0	0	1	1	1
2020-03-25 06:00	1	1	1	1	1	0	0	1	1	0	4
2020-03-25 07:00	1	1	1	1	1	2	3	0	0	2	3
2020-03-25 08:00	2	0	3	2	2	2	0	0	1	1	3
2020-03-25 09:00	1	0	0	0	0	1	1	1	0	0	0
2020-03-25 10:00	0	0	0	0	0	0	23	0	0	0	0
2020-03-25 11:00	0	0	0	0	0	0	196	0	0	0	0
2020-03-25 12:00	0	0	0	0	0	0	75	1	0	1	0
2020-03-25 13:00	1	2	1	0	1	1	0	2	1	2	4

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

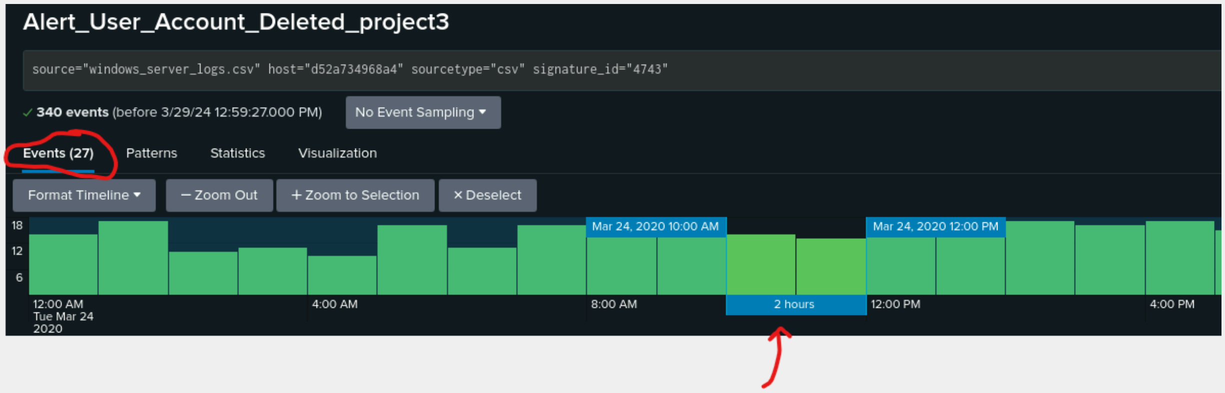
No we would not. This is a nice balance between false positives and suspicious activity.

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

The average number of accounts deleted per hour fell from about 14 to roughly 10 an hour on March 25. What is suspicious is that generally there is a steady flow of accounts being deleted during the course of the day. On

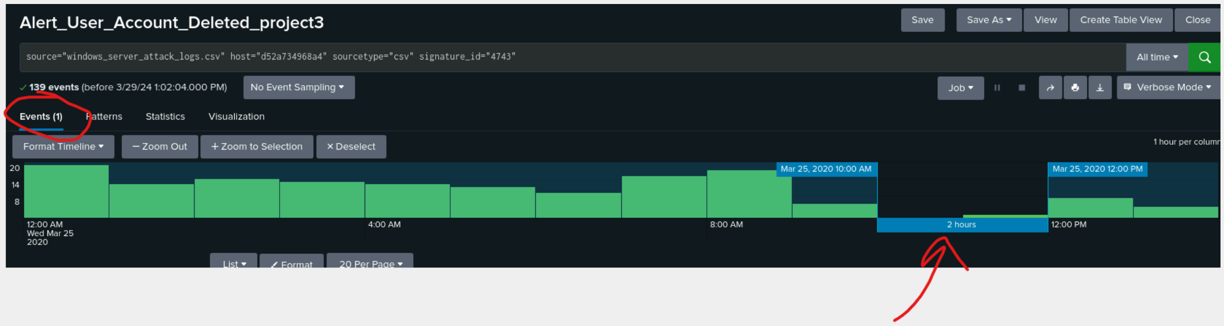
```
March 25, between 10:00 a.m. and 12:00 p.m. we see only one account deletion
occur which is well below normal according to our baseline of 14/hour.
```



Alert_User_Account_Deleted_project3

```
source="windows_server_logs.csv" host="d52a734968a4" sourcetype="csv" signature_id="4743"
```

✓ 340 events (before 3/29/24 12:59:27.000 PM)



Alert_User_Account_Deleted_project3

```
source="windows_server_attack_logs.csv" host="d52a734968a4" sourcetype="csv" signature_id="4743"
```

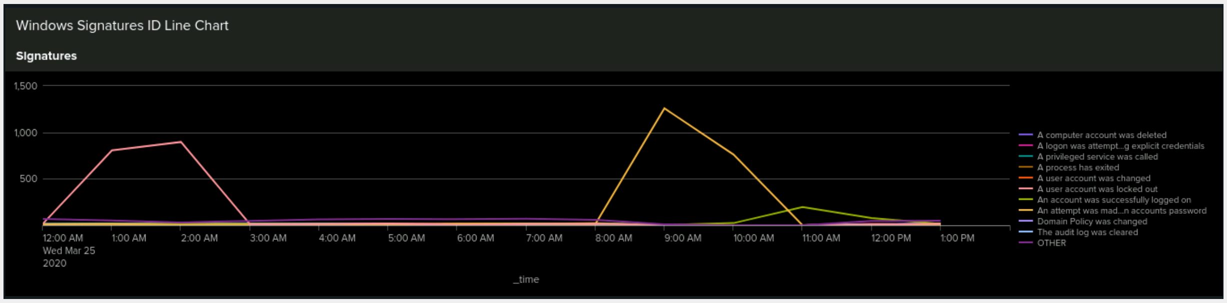
✓ 139 events (before 3/29/24 1:02:04.000 PM)

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
Yes, between the hours of 12:00 a.m. and 1:00 a.m. 805 user accounts were
locked out. Then from 1:00 a.m. to 2:00 a.m., another 896 were locked out.

Then at 9:00 a.m. 1258 attempts were made to reset account passwords.
```



- What signatures stand out?

The “A user account was locked out” and “An attempt was made to reset an accounts password” are the 2 signatures that stand out.

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

Lockout signature started at 1:00 a.m. and ended at 2:00 a.m.

Password reset signature started at 9:00 a.m. and ended at 10:00 a.m.

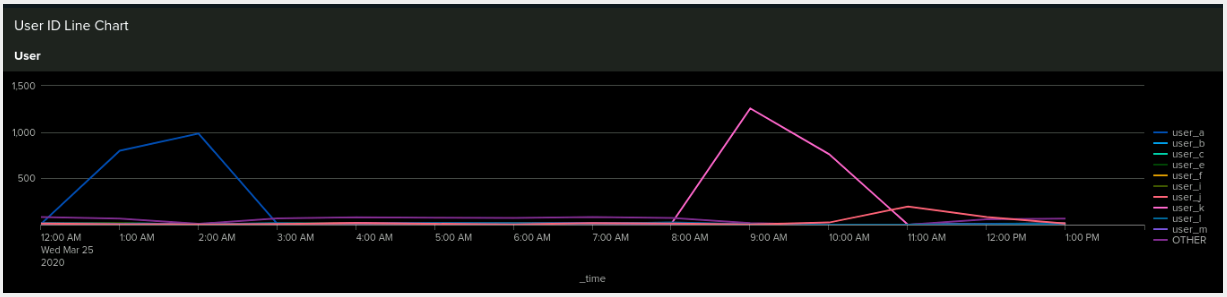
- What is the peak count of the different signatures?

Lockout peak: 896
Reset peak: 1258

Dashboard Analysis for Users

- Does anything stand out as suspicious?

Yes, between 1:00 a.m. and 2:00 a.m., user_a engaged in a large amount of activity and then at 9:00 a.m., user_k was extremely active.



- Which users stand out?

user_a & user_k

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

user_a: 1:00 a.m. - 2:00 a.m.
user_k: 9:00 a.m. - 10:00 a.m.

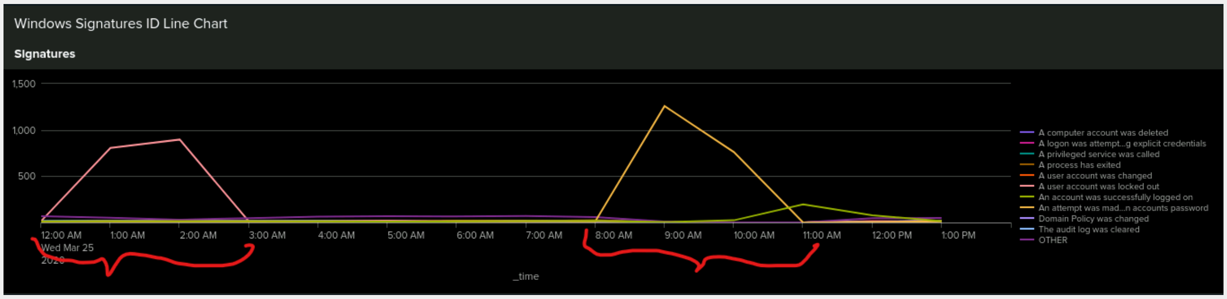
- What is the peak count of the different users?

```
user_a: 984
user_k: 1256
```

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

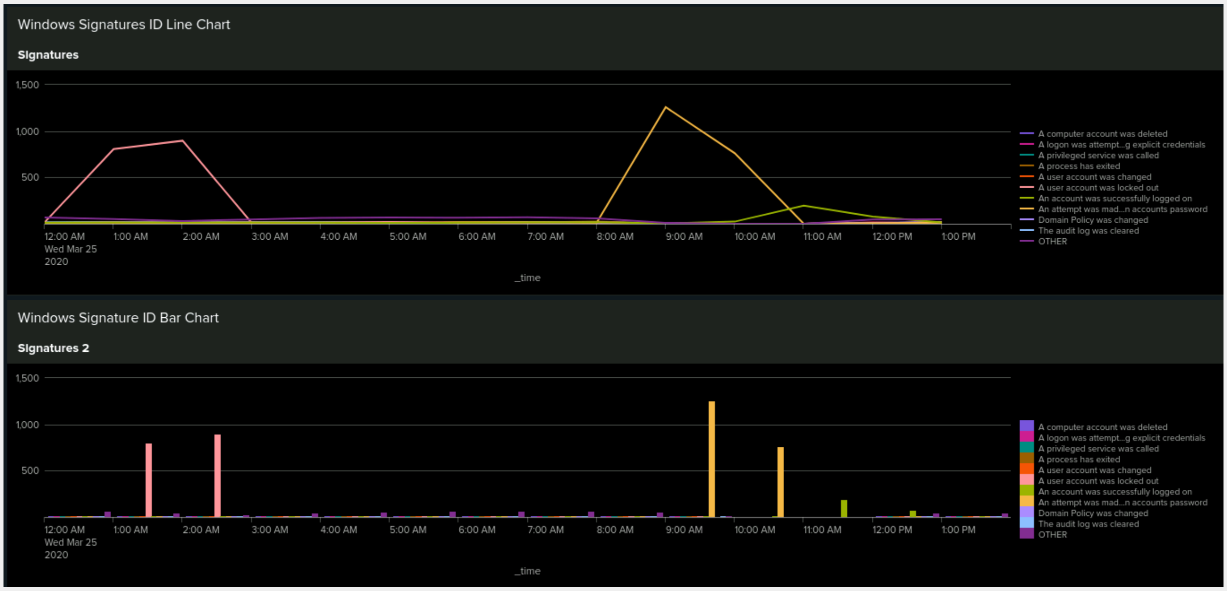
- Does anything stand out as suspicious?

```
Yes. Between 12:00 a.m. and 3:00 a.m. hundreds of accounts were locked out
and then between 8:00 a.m. and 11:00 a.m., someone tried to reset over 1200
account passwords.
```



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

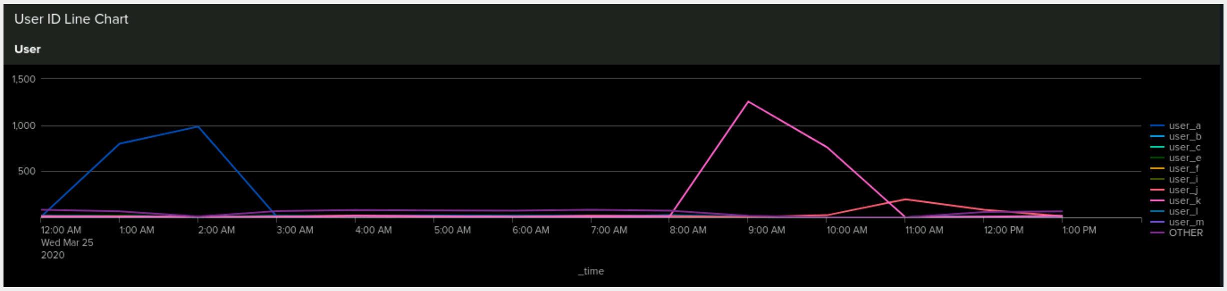
```
The results match up perfectly.
```



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

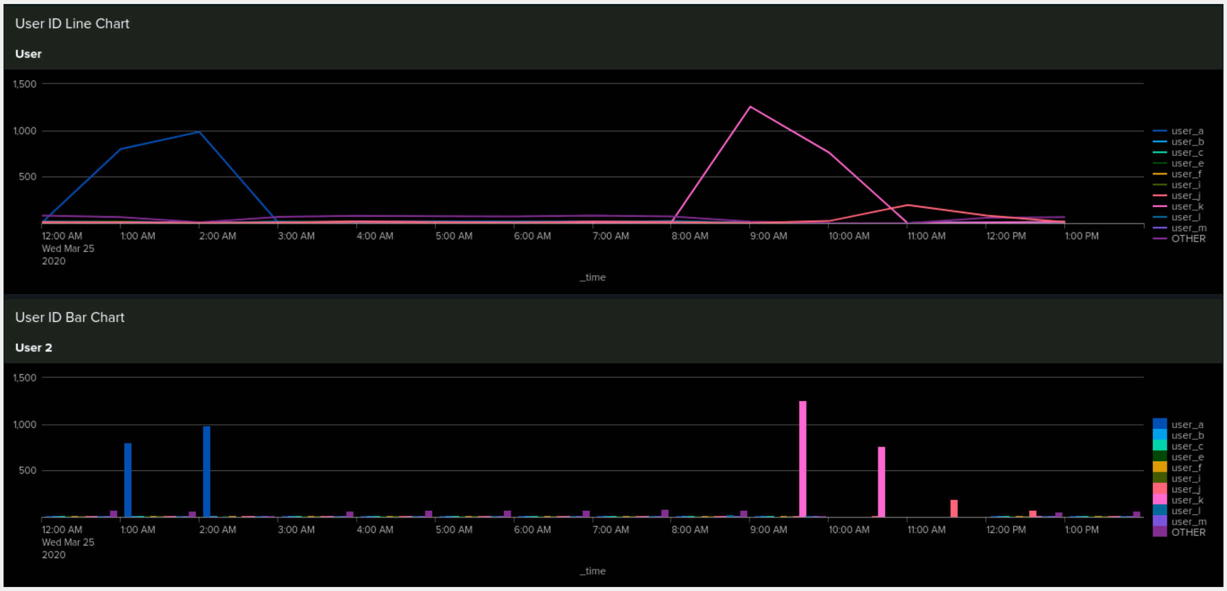
- Does anything stand out as suspicious?

```
user_a was engaged in a high volume of activity during the hours of 12:00
a.m. and 3:00 a.m. and then user_k did the same from 8:00 a.m. to 11:00 a.m.
```



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

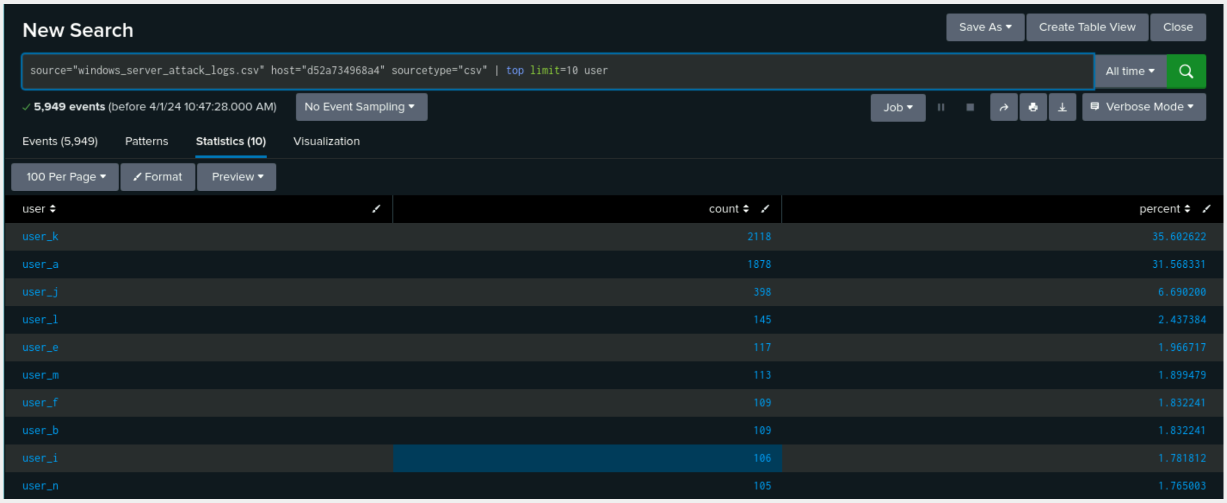
```
The results match up exactly.
```



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?

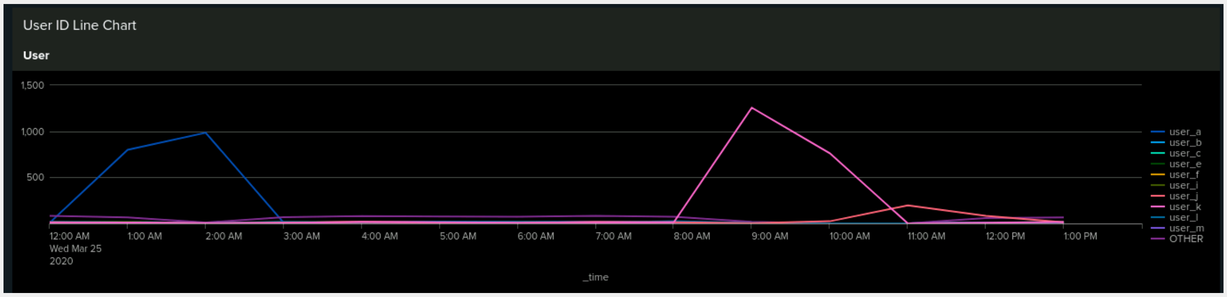
The statistical chart gives us a more detailed chart of user activity but it is much more difficult to quickly identify suspicious activity without the dashboard visualizations.



```
source="windows_server_attack_logs.csv" host="d52a734968a4" sourcetype="csv" | top limit=10 user
```

✓ **5,949 events** (before 4/1/24 10:47:28.000 AM)

user	count	percent
user_k	2118	35.602622
user_a	1878	31.568331
user_j	398	6.690200
user_l	145	2.437384
user_e	117	1.966717
user_m	113	1.899479
user_f	109	1.832241
user_b	109	1.832241
user_i	106	1.781812
user_n	105	1.765003



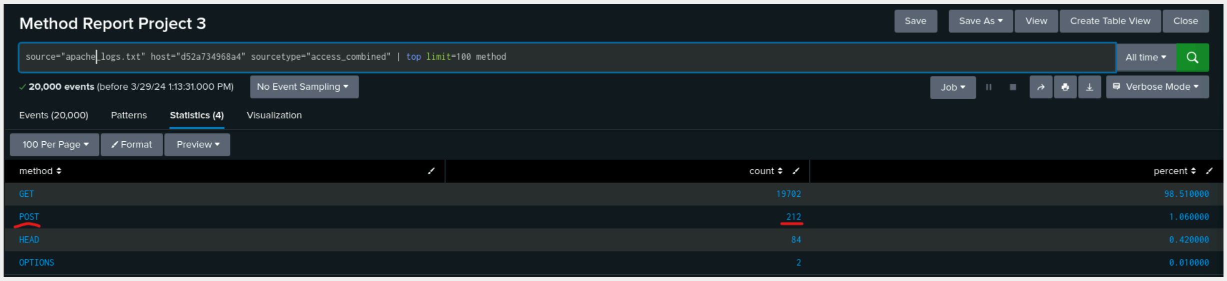
We see the suspicious activity jump right out with the visualization because we have the added advantage of seeing the activity vs time.

Apache Web Server Log Questions

Report Analysis for Methods

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

There was a large jump in the POST request methods. We can see below that POST requests went from just over 1% of HTTP traffic to almost 30% of it on March 25.

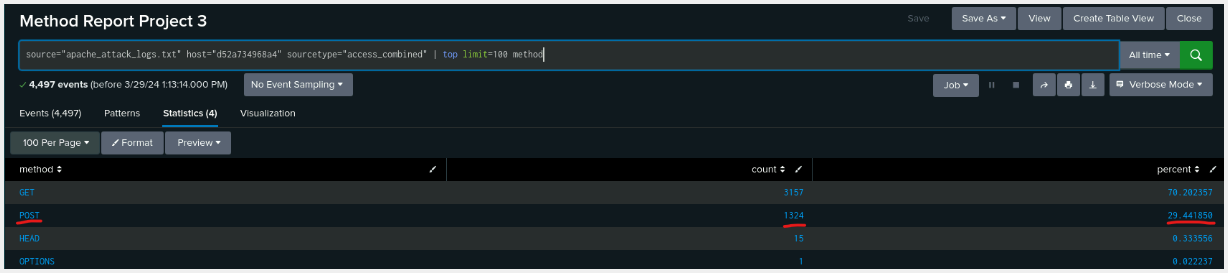


Method Report Project 3

```
source="apache_logs.txt" host="d52a734968a4" sourcetype="access_combined" | top limit=100 method
```

✓ **20,000 events** (before 3/29/24 1:13:31.000 PM)

method	count	percent
GET	19702	98.510000
POST	212	1.060000
HEAD	84	0.420000
OPTIONS	2	0.010000



Method Report Project 3

```
source="apache_attack_logs.txt" host="d52a734968a4" sourcetype="access_combined" | top limit=100 method
```

✓ **4,497 events** (before 3/29/24 1:13:14.000 PM)

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?

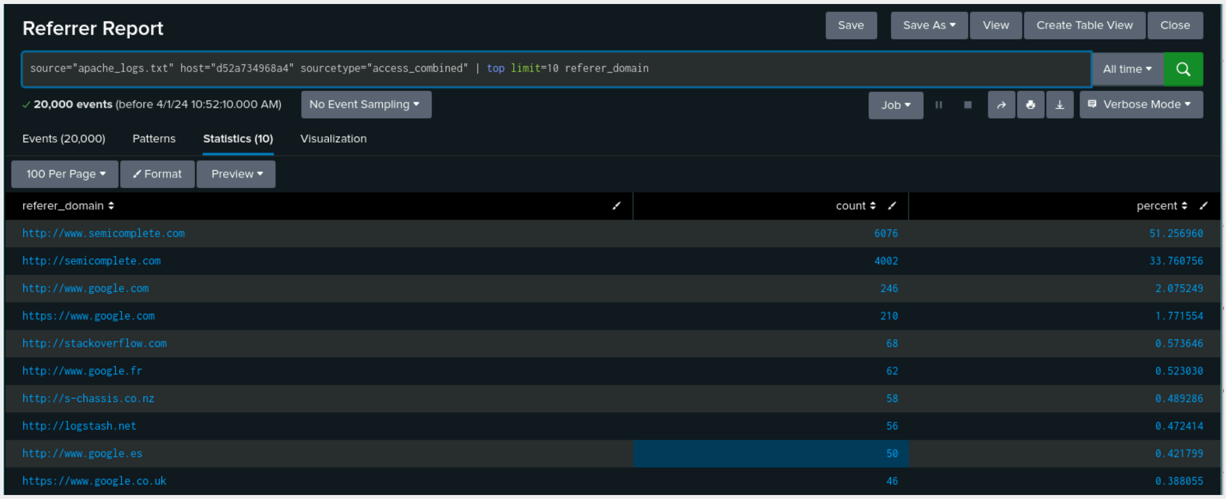
```
POST is used to send data to a server to update a resource.
```

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

```
The amount of referrer domains to VSI’s website decreased by 90%

Pre-attack
```



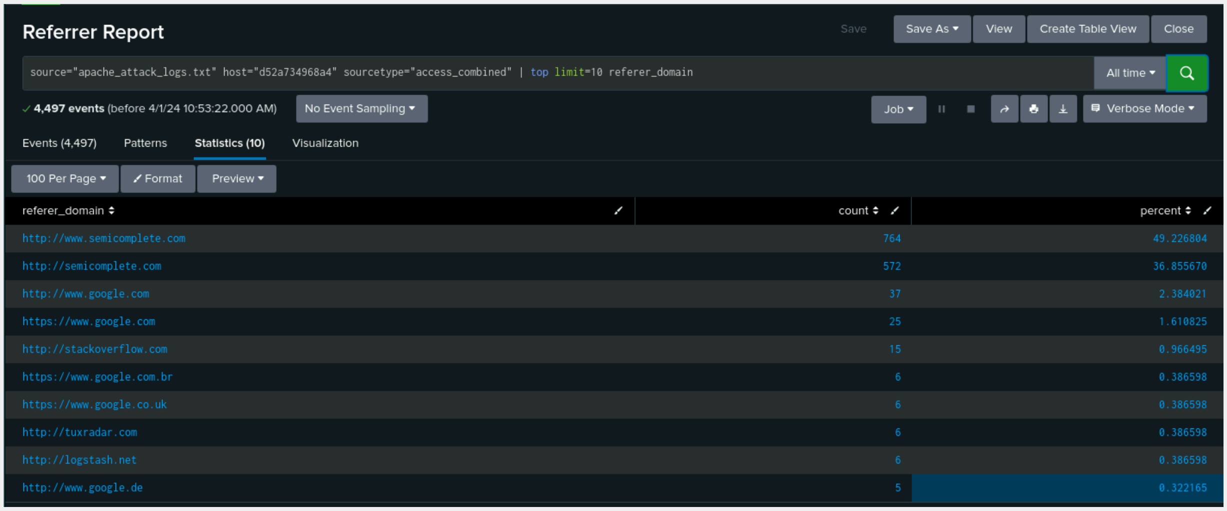
Referrer Report

```
source="apache_logs.txt" host="d52a734968a4" sourcetype="access_combined" | top limit=10 referer_domain
```

✓ **20,000 events** (before 4/1/24 10:52:10.000 AM)

referer_domain	count	percent
http://www.semicomplete.com	6076	51.256960
http://semicomplete.com	4002	33.760756
http://www.google.com	246	2.075249
https://www.google.com	210	1.771554
http://stackoverflow.com	68	0.573646
http://www.google.fr	62	0.523030
http://s-chassis.co.nz	58	0.489286
http://logstash.net	56	0.472414
http://www.google.es	50	0.421799
https://www.google.co.uk	46	0.388055

Post-attack



Referrer Report

```
source="apache_attack_logs.txt" host="d52a734968a4" sourcetype="access_combined" | top limit=10 referer_domain
```

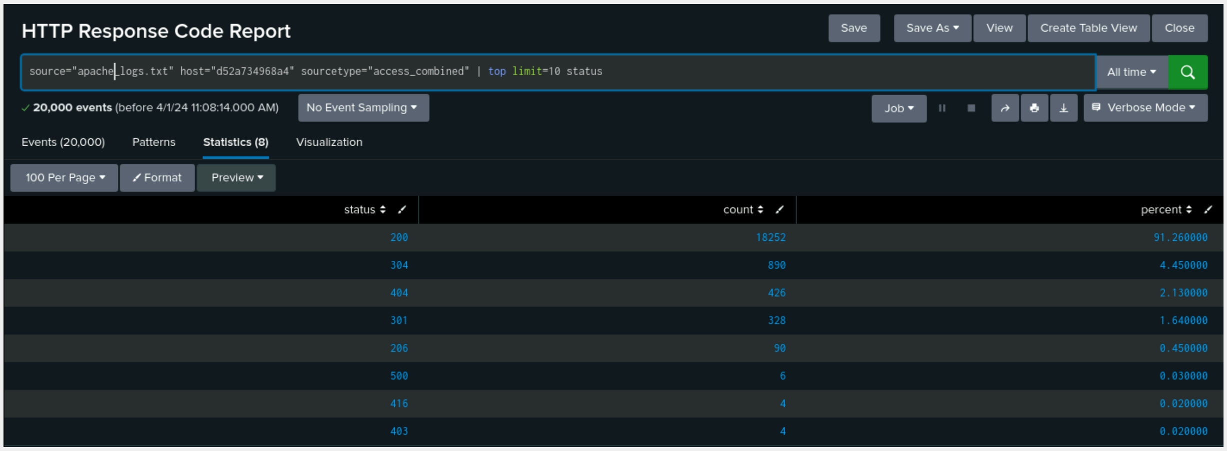
✓ **4,497 events** (before 4/1/24 10:53:22.000 AM)

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?

The overall number of codes fell, however, there was an increase in 404 error codes. From 426 to 679.

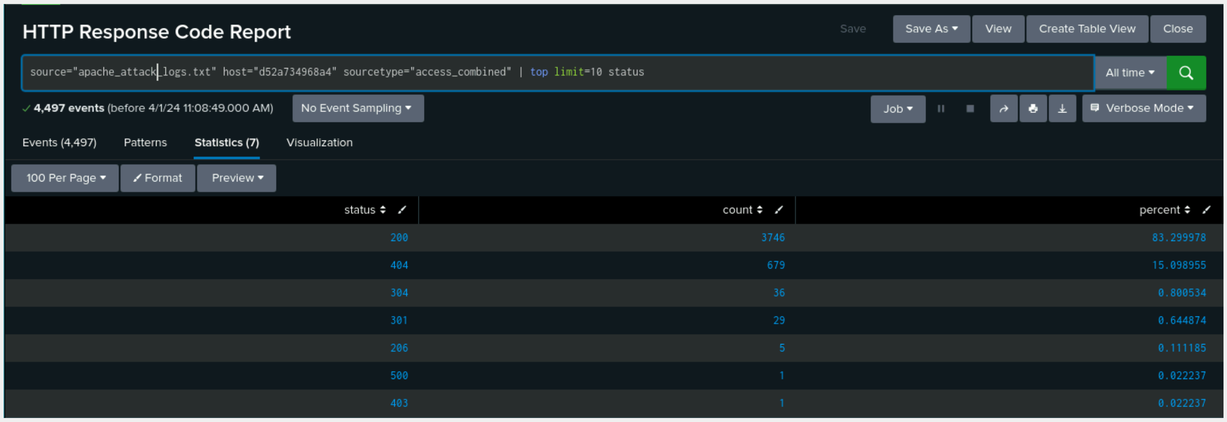


HTTP Response Code Report

```
source="apache_logs.txt" host="d52a734968a4" sourcetype="access_combined" | top limit=10 status
```

✓ **20,000 events** (before 4/1/24 11:08:14.000 AM)

status	count	percent
200	18252	91.260000
304	890	4.450000
404	426	2.130000
301	328	1.640000
206	90	0.450000
500	6	0.030000
416	4	0.020000
403	4	0.020000



HTTP Response Code Report

```
source="apache_attack_logs.txt" host="d52a734968a4" sourcetype="access_combined" | top limit=10 status
```

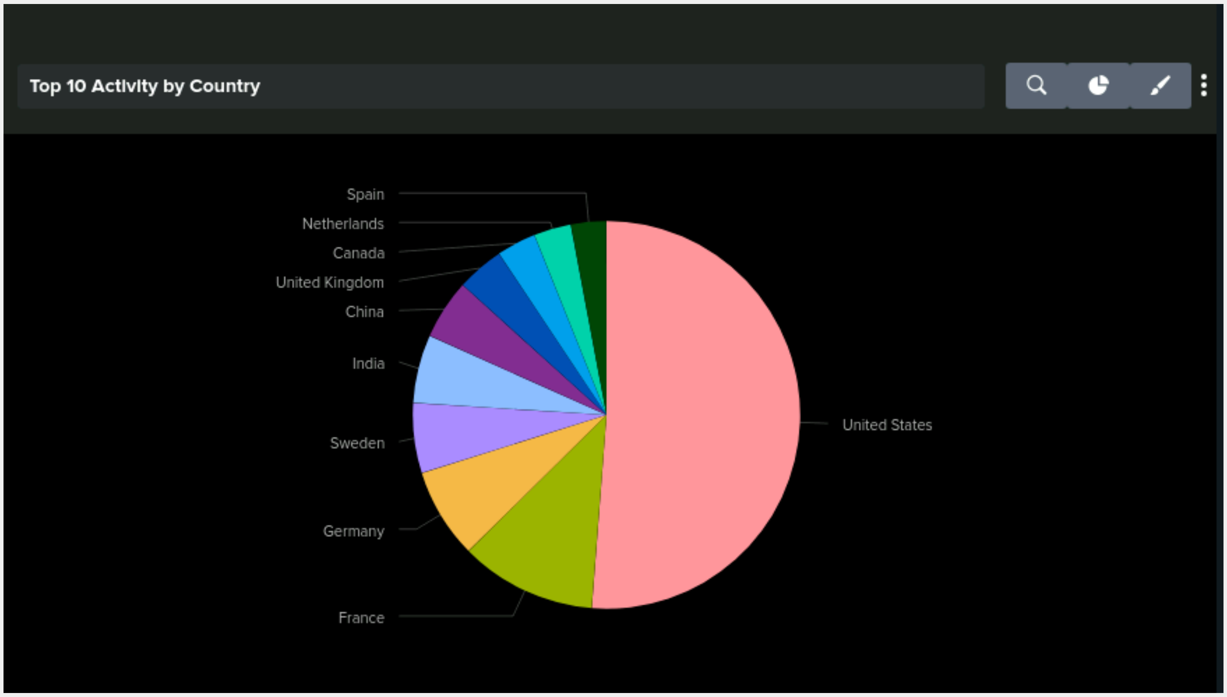
✓ **4,497 events** (before 4/1/24 11:08:49.000 AM)

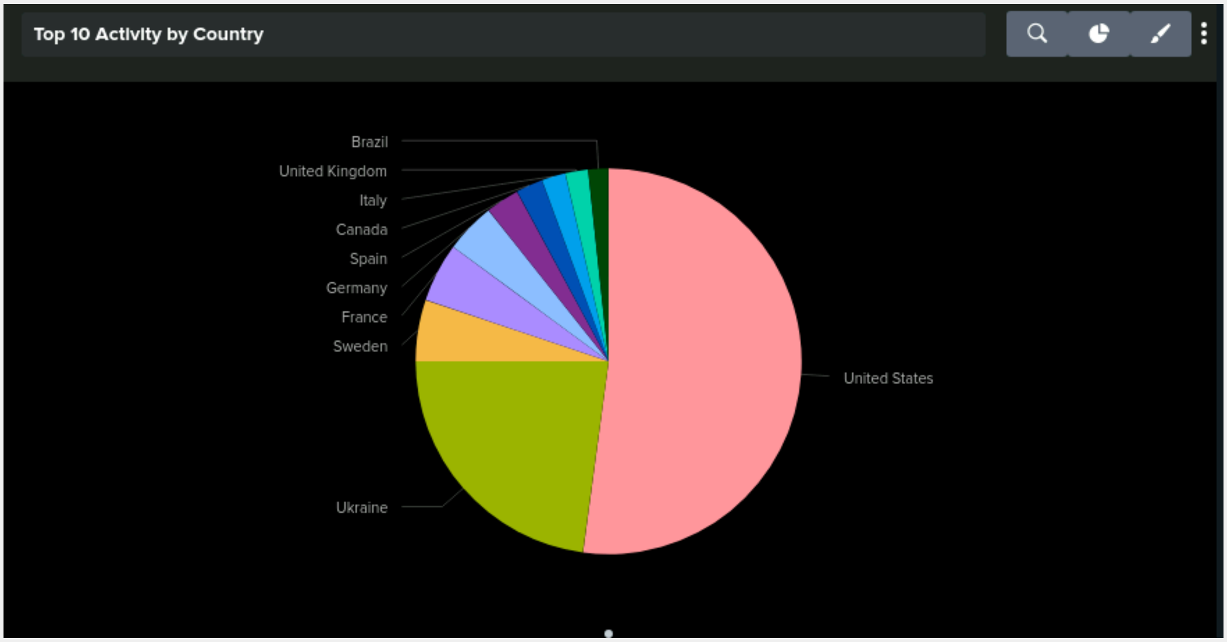
status	count	percent
200	3746	83.299978
404	679	15.098955
304	36	0.800534
301	29	0.644874
206	5	0.111185
500	1	0.022237
403	1	0.022237

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

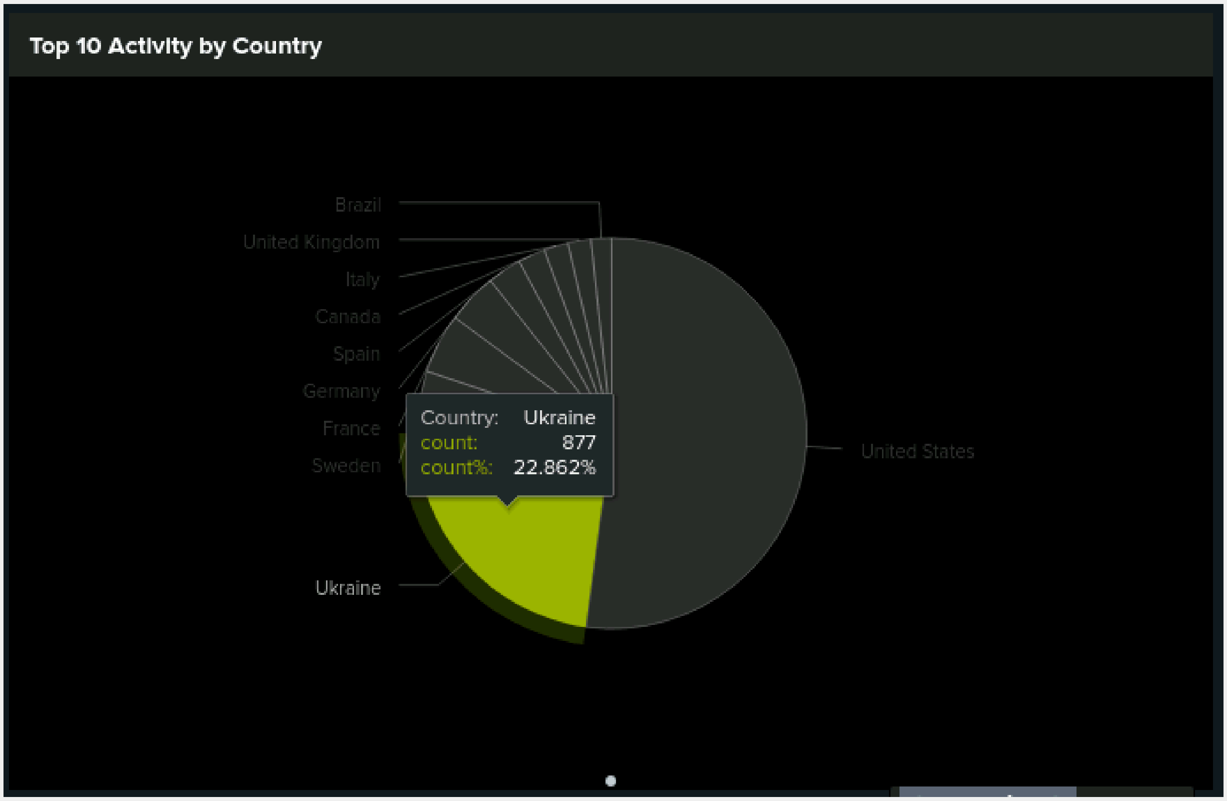
Yes we did. Before March 25, there was no significant activity from Ukraine directed at the Apache web server. However, on March 25, we can see that Ukraine made up almost 23% of activity on the web server. This is a huge jump.





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

```
877 events.
```



Country: Ukraine
count: 877
count%: 22.862%

- Would your alert be triggered for this activity?

Yes, we set our threshold to 230 events/hour for activity outside of the US so the alert should trigger.

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

No we would not. This threshold seems to be a good balance to avoid alert fatigue.

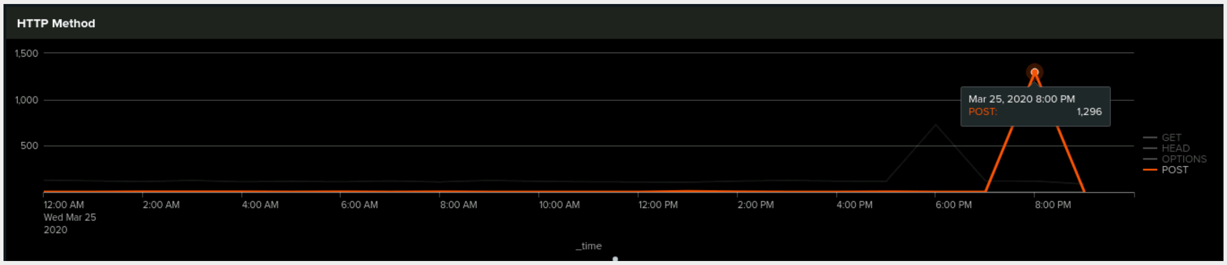
Alert Analysis for HTTP POST Activity

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

Yes we did. We saw the normal baseline of 2.55 POST requests/hour jump to 69.68/hour on March 25, 2020.

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

1296 events.



- When did it occur?

8:00 p.m. on March 25, 2020.

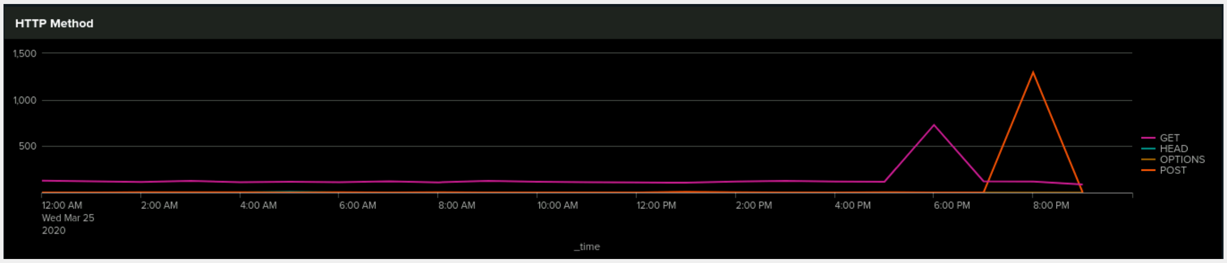
- After reviewing, would you change the threshold that you previously selected?

We set the threshold to 12 and no we would not change it. The spike in activity is extremely aggressive.

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

There was a large spike in GET and POST requests.



- Which method seems to be used in the attack?

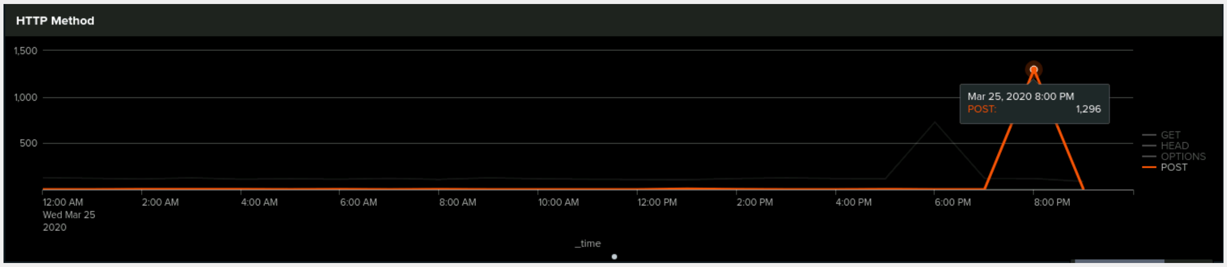
Both GET and POST were used according to our report. The GET requests targeted the logstash uri and the POST requests targeted the logon.php URI.

- At what times did the attack start and stop?

The attack started at 5:00 p.m.and ended at 9:00 p.m. on March 25, 2020.

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

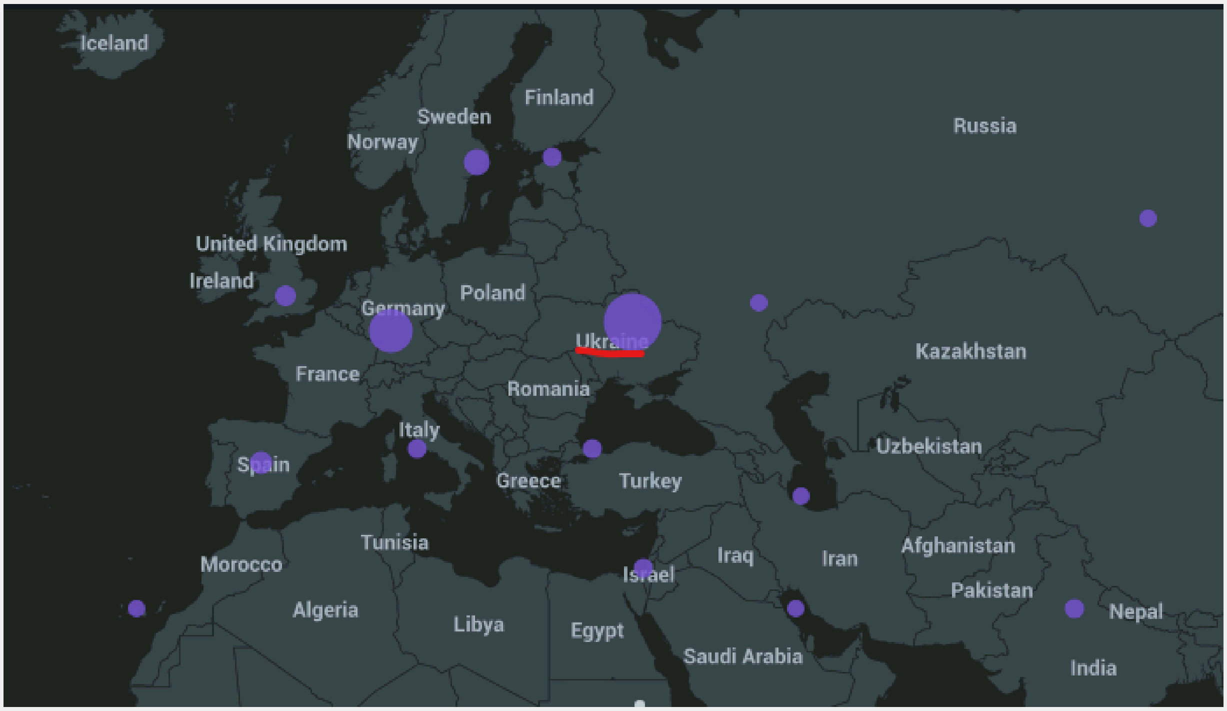
1296 POST methods



Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
There was a large spike in activity from Ukraine.
```



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

```
Kharkiv/Kiev, Ukraine
```

- What is the count of that city?

```
Kiev(440) + Kharkiv(432) = 872(combined)
```

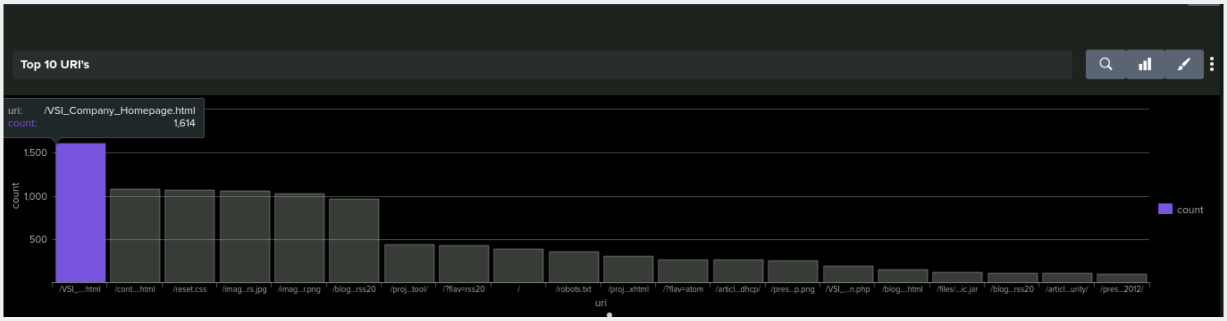
Chernobyl
Sumy
Belgorod
Kiev
myr
Kharkiv
Ukraine

Dashboard Analysis for URI Data

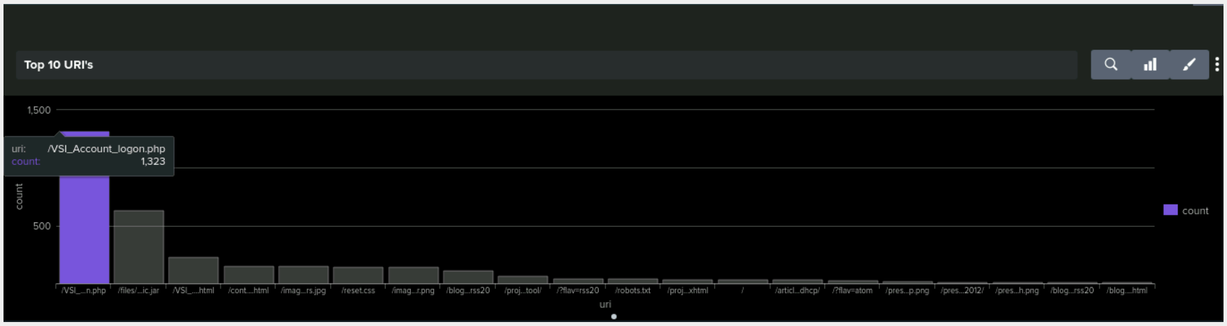
- Does anything stand out as suspicious?

Yes. Before March 25, the most commonly accessed URI was the /VSI_Company_Homepage.html with a count of 1614. On March 25, that count fell to 235 and we see the /VSI_Account_logon.php URI hit with 1323 events up from 202.

Pre-attack:



Post-attack:



- What URI is hit the most?

/VSI_Account_logon.php is hit the most, however, the logstash URI was also targeted by GET requests, just not as much as the POST/logon URI attack.

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

Brute Force Attack/Credential Stuffing or even DDoS since we also saw a drop in HTTP 200 response codes.