Cybersecurity

Project 3 Review Questions

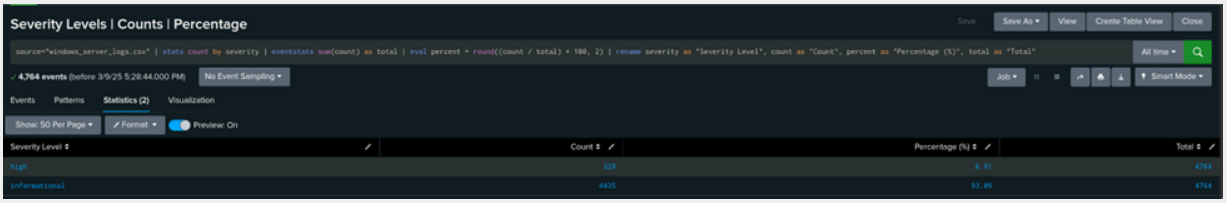
Make a copy of this document before you begin. Place your answers below each question.

Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

```
Yes, were able to find the change in severity level count, High count
increased from 6.91% to 20.22%
Before:
```



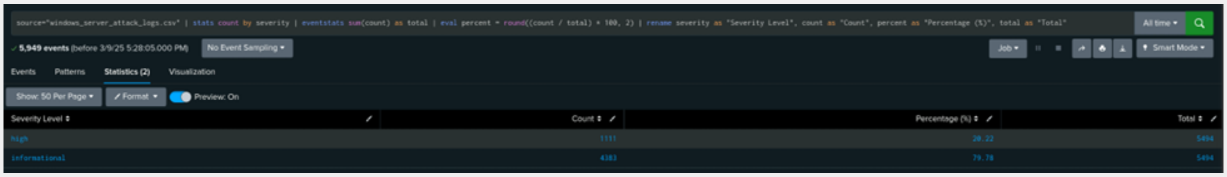
Severity Levels | Counts | Percentage

```
source="windows_server_logs.csv" | stats count by severity | eventstats sum(count) as total | eval percent = round((count / total) * 100, 2) | rename severity as "Severity Level", count as "Count", percent as "Percentage (%)", total as "Total"
```

✓ 4,764 events (before 3/9/25 5:28:44.000 PM)

Severity Level	Count	Percentage (%)	Total
high	329	6.91	4764
informational	4435	93.09	4764

```
After attack:
```



```
source="windows_server_attack_logs.csv" | stats count by severity | eventstats sum(count) as total | eval percent = round((count / total) * 100, 2) | rename severity as "Severity Level", count as "Count", percent as "Percentage (%)", total as "Total"
```

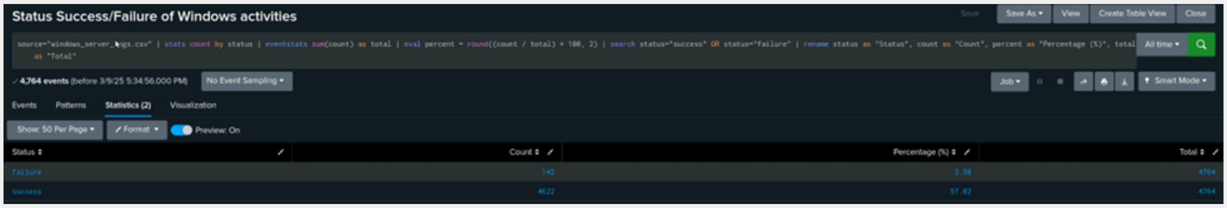
✓ 5,949 events (before 3/9/25 5:28:05.000 PM)

Severity Level	Count	Percentage (%)	Total
high	1111	20.22	5494
informational	4383	79.78	5494

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

```
Yes, The failed activities count decreased from 142 to 93
Before:
```



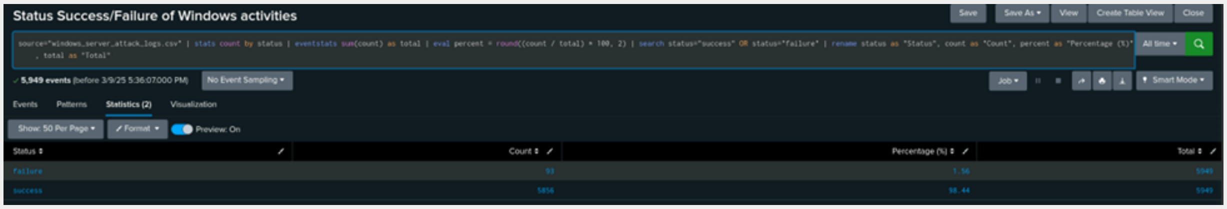
Status Success/Failure of Windows activities

```
source="windows_server_logs.csv" | stats count by status | eventstats sum(count) as total | eval percent = round((count / total) * 100, 2) | search status="success" OR status="failure" | rename status as "Status", count as "Count", percent as "Percentage (%)", total
    as "Total"
```

✓ 4,764 events (before 3/9/25 5:34:56.000 PM)

Status	Count	Percentage (%)	Total
failure	142	2.98	4764
success	4622	97.02	4764

After:



Status Success/Failure of Windows activities

```
source="windows_server_attack_logs.csv" | stats count by status | eventstats sum(count) as total | eval percent = round((count / total) * 100, 2) | search status="success" OR status="failure" | rename status as "Status", count as "Count", percent as "Percentage (%)"
    , total as "Total"
```

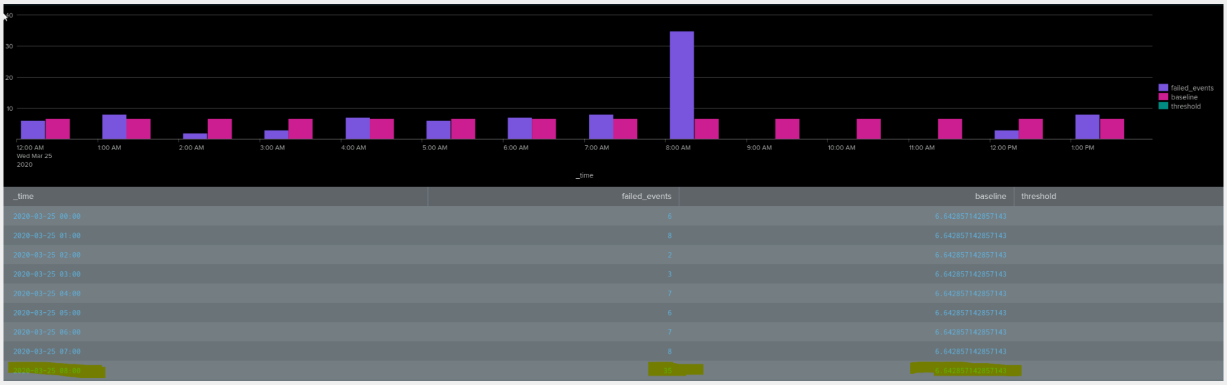
✓ 5,949 events (before 3/9/25 5:36:07.000 PM)

Status	Count	Percentage (%)	Total
failure	93	1.56	5949
success	5856	98.44	5949

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

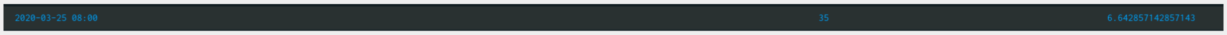
Yes, I can see there is a spike in failed activity at 8AM.



_time	failed_events	baseline	threshold
2020-03-25 00:00	6	6.642857142857143	
2020-03-25 01:00	8	6.642857142857143	
2020-03-25 02:00	2	6.642857142857143	
2020-03-25 03:00	3	6.642857142857143	
2020-03-25 04:00	7	6.642857142857143	
2020-03-25 05:00	6	6.642857142857143	
2020-03-25 06:00	7	6.642857142857143	
2020-03-25 07:00	8	6.642857142857143	
2020-03-25 08:00	35	6.642857142857143	

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

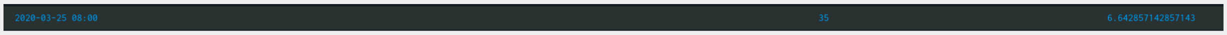
35 count of the events.



2020-03-25 08:00	35	6.642857142857143

- When did it occur?

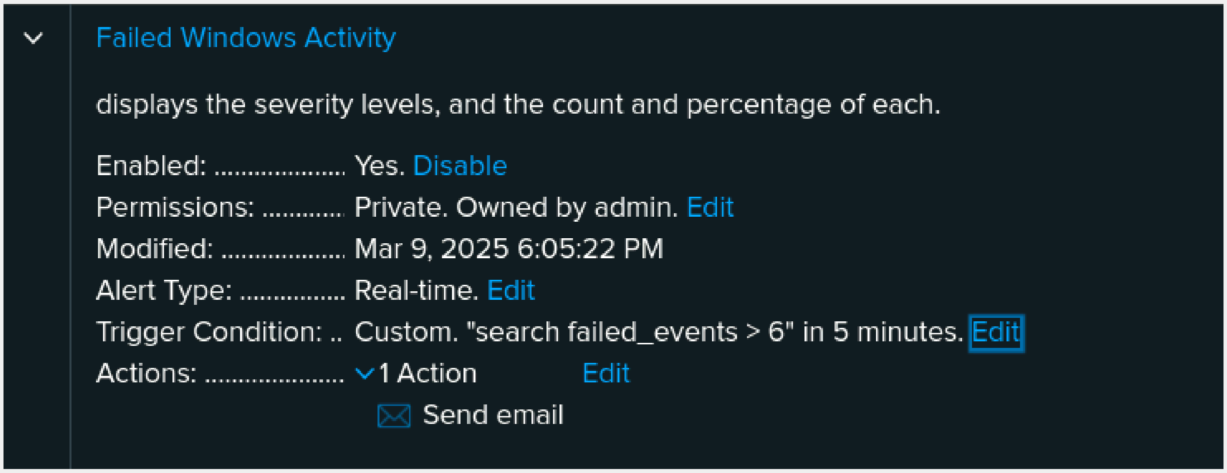
2020-03-25 08:00 AM



2020-03-25 08:00	35	6.642857142857143

- Would your alert be triggered for this activity?

```
Yes, I set up the real time failed events alert based on the baseline
threshold, which was “6”. Now that the count is 35, it will trigger.
```



Failed Windows Activity

displays the severity levels, and the count and percentage of each.

Enabled: .... Yes. Disable
Permissions: .... Private. Owned by admin. Edit
Modified: .... Mar 9, 2025 6:05:22 PM
Alert Type: .... Real-time. Edit
Trigger Condition: .. Custom. "search failed_events > 6" in 5 minutes. Edit
Actions: .... 1 Action Edit
Send email

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

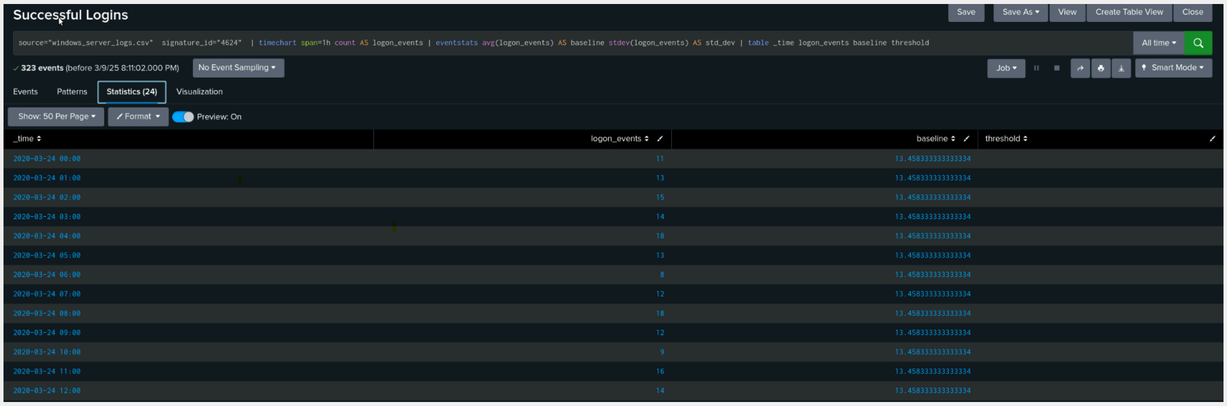
```
I believe I should change it to 10, because 6 is too low and it may increase
the chances of false positives.
```

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

```
Yes, After reviewing the logs, there is a suspicious activity where a
slightly increased successful login attempt happened and then suddenly
dropped to 4.

Log activity:
```



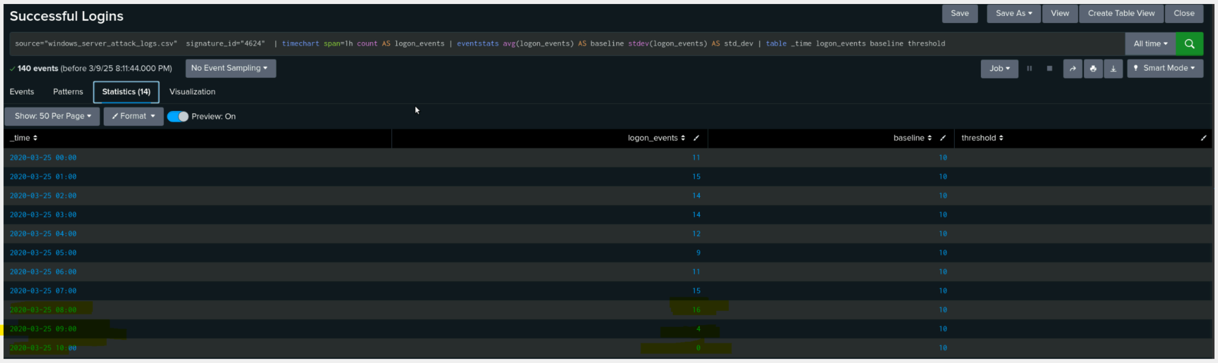
Successful Logins

```
source="windows_server_logs.csv"  signature_id="4624"  | timechart span=1h count AS logon_events | eventstats avg(logon_events) AS baseline stdev(logon_events) AS std_dev | table _time logon_events baseline threshold
```

✓ **323 events** (before 3/9/25 8:11:02.000 PM)

_time	logon_events	baseline	threshold
2020-03-24 00:00	11	13.458333333333334	
2020-03-24 01:00	13	13.458333333333334	
2020-03-24 02:00	15	13.458333333333334	
2020-03-24 03:00	14	13.458333333333334	
2020-03-24 04:00	18	13.458333333333334	
2020-03-24 05:00	13	13.458333333333334	
2020-03-24 06:00	8	13.458333333333334	
2020-03-24 07:00	12	13.458333333333334	
2020-03-24 08:00	18	13.458333333333334	
2020-03-24 09:00	12	13.458333333333334	
2020-03-24 10:00	9	13.458333333333334	
2020-03-24 11:00	16	13.458333333333334	
2020-03-24 12:00	14	13.458333333333334	

After attack:



Successful Logins

```
source="windows_server_attack_logs.csv"  signature_id="4624"  | timechart span=1h count AS logon_events | eventstats avg(logon_events) AS baseline stdev(logon_events) AS std_dev | table _time logon_events baseline threshold
```

✓ **140 events** (before 3/9/25 8:11:44.000 PM)

_time	logon_events	baseline	threshold
2020-03-25 00:00	11	10	
2020-03-25 01:00	15	10	
2020-03-25 02:00	14	10	
2020-03-25 03:00	14	10	
2020-03-25 04:00	12	10	
2020-03-25 05:00	9	10	
2020-03-25 06:00	11	10	
2020-03-25 07:00	15	10	
2020-03-25 08:00	16	10	
2020-03-25 09:00	4	10	
2020-03-25 10:00	0	10	

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

At 08:00 AM there were a total of 16 successful logins occurred and then the number significantly drops to 4 at 09:00 AM AM and is at 0 logins from 10:00 AM to 11:00 AM and goes up to 4 logins at 12:00 PM.

- Who is the primary user logging in?

Upon further analysis, we saw that user_a had a spike of total 10 login attempts.

- When did it occur?

It occurred at 2020-03-25 2.30AM

- Would your alert be triggered for this activity?

No, We have set the trigger to 15 or more successful logins per hour.

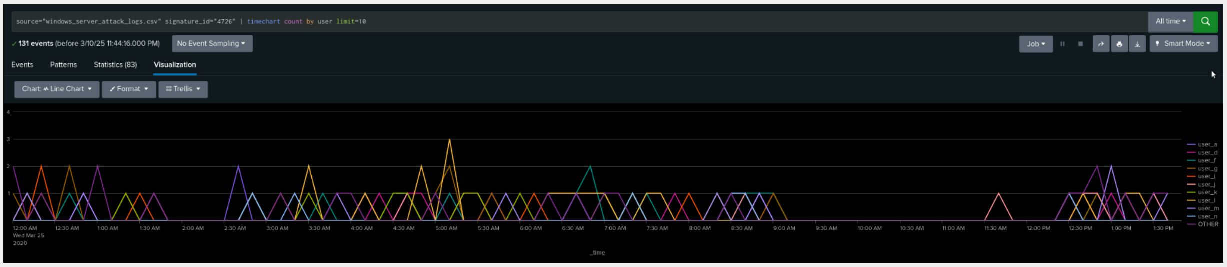
- After reviewing, would you change your threshold from what you previously selected?

I would not change it, because it can create alert fatigue for the SOC team.

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

Yes, we see a significant amount of deletion events, which happened between 9AM to 11.30 AM. The count dropped to 0.



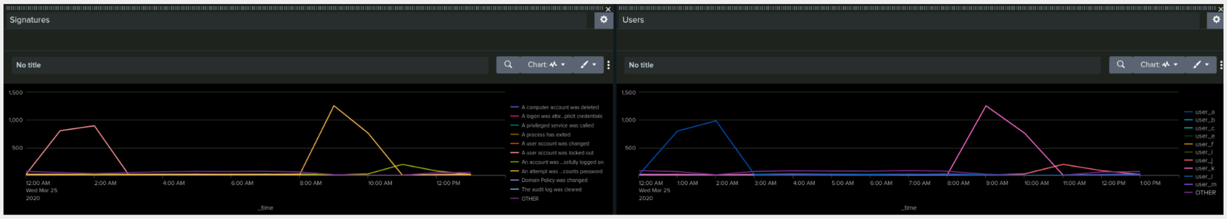
```
source="windows_server_attack_logs.csv" signature_id="4726" | timechart count by user limit=10
```

✓ 131 events (before 3/10/25 11:44:16.000 PM)

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

Yes, in the timechart we can see attempts to change passwords for certain users.



- What signatures stand out?

There are 2 signatures that stand out in the chart.

1. The user account was locked out.
2. An attempt was made to reset the password.

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

```
 1. The user account was locked out at 1 am to 2:30AM
 2. An attempt was made to reset the password at 9AM to 10AM
```

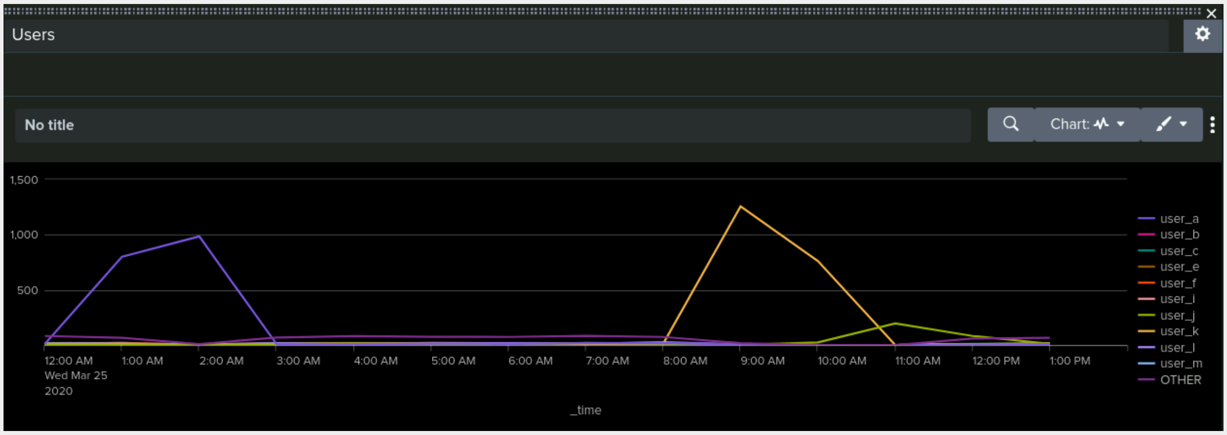
- What is the peak count of the different signatures?

```
 1. The user account was locked out peaked at 896
 2. An attempt was made to reset the password peaked at 1258
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
There is a significant increase in user activity for 2 users.
```



- Which users stand out?

```
User_a
user_k
```

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

```
User_a had increased activity occur between 01:00 AM and 02:30 AM
User_k had increased activity occur between 09:00 AM and 10:00 AM
```

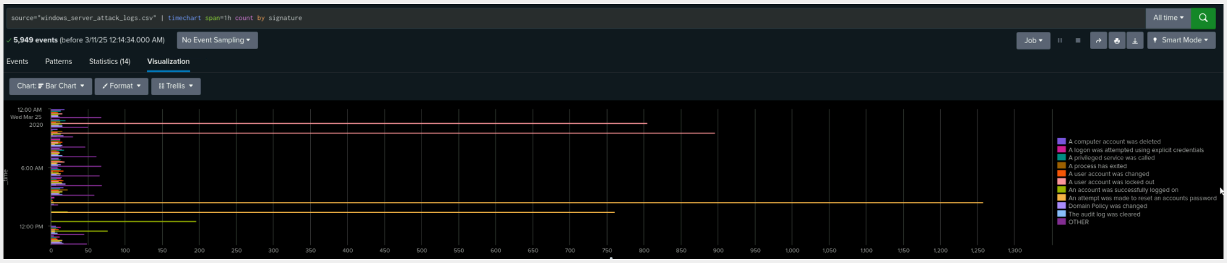
- What is the peak count of the different users?

```
User_a peaked at 984
User_k peaked at 1256
```

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

- Does anything stand out as suspicious?

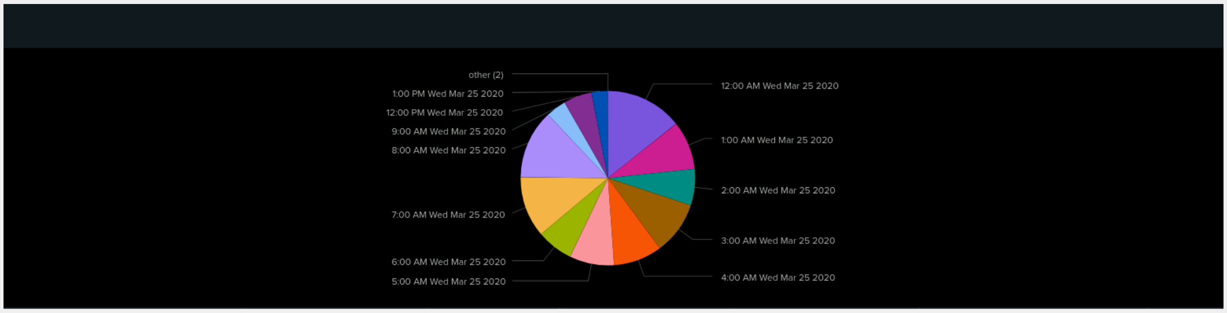
```
Yes 2 signatures are standing out in these charts:
The user account was locked out.
An attempt was made to reset the password.
```



```
source="windows_server_attack_logs.csv" | timechart span=1h count by signature
```

✓ 5,949 events (before 3/11/25 12:14:34.000 AM)

All time ▾
No Event Sampling ▾
Job ▾
Smart Mode ▾
Events
Patterns
Statistics (14)
Visualization
Chart: Bar Chart ▾
Format ▾
Trellis ▾
12:00 AM Wed Mar 25 2020
6:00 AM
12:00 PM
_time
0
50
100
150
200
250
300
350
400
450
500
550
600
650
700
750
800
850
900
950
1,000
1,050
1,100
1,150
1,200
1,250
1,300
A computer account was deleted
A logon was attempted using explicit credentials
A privileged service was called
A process has exited
A user account was changed
A user account was locked out
An account was successfully logged on
An attempt was made to reset an accounts password
Domain Policy was changed
The audit log was cleared
OTHER



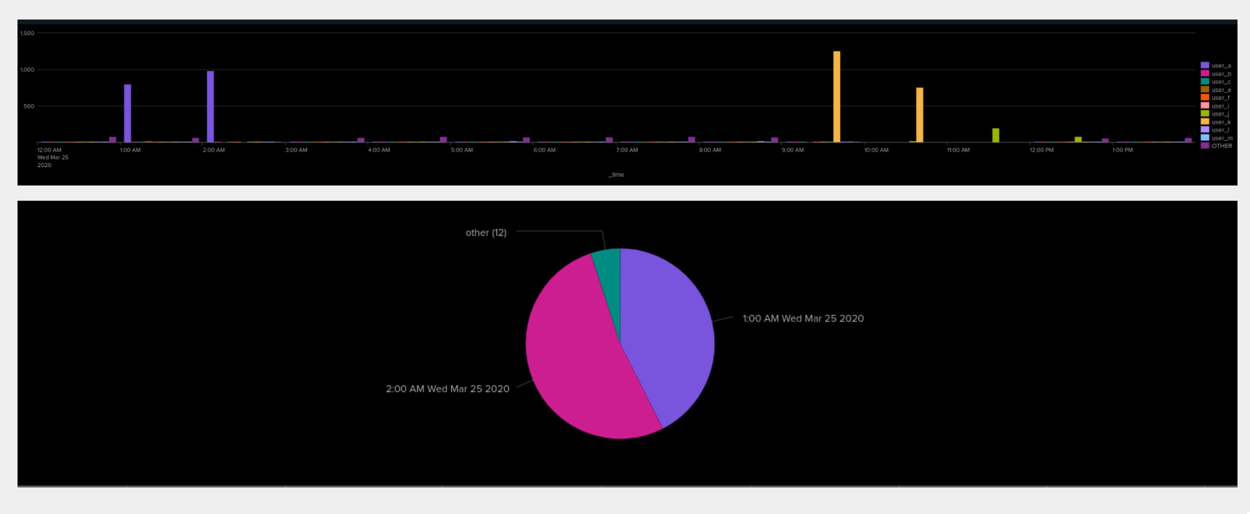
- Do the results match your findings in your time chart for signatures?

```
Yes they do match.
```

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

- Does anything stand out as suspicious?

```
Yes, there is increased activity from user_a and user_k
Attack
```



- 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?

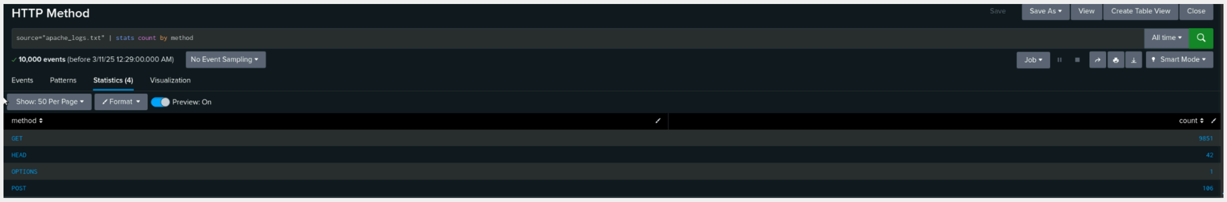
```
One benefit of using statistical time charts for tracking events and user
activity is that they make it easy to see how often something happens each
hour. However, compared to bar graphs and pie charts, they don’t clearly
highlight changes in activity. Bar graphs and pie charts are better for
spotting sudden spikes or drops in activity at a glance. A pie chart, in
particular, makes it easy to see which event or user had the most activity.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

```
Yes, we detect some suspicious changes in HTTP methods.
Normal Logs:
```



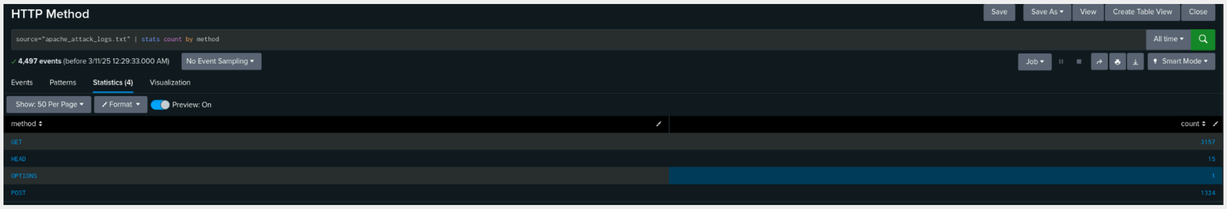
HTTP Method

```
source="apache_logs.txt" | stats count by method
```

✓ **10,000 events** (before 3/11/25 12:29:00.000 AM) No Event Sampling

method	count
GET	9851
HEAD	42
OPTIONS	1
POST	106

After attack:



HTTP Method

```
source="apache_attack_logs.txt" | stats count by method
```

✓ **4,497 events** (before 3/11/25 12:29:33.000 AM) No Event Sampling

method	count
GET	3157
HEAD	15
OPTIONS	1
POST	1324

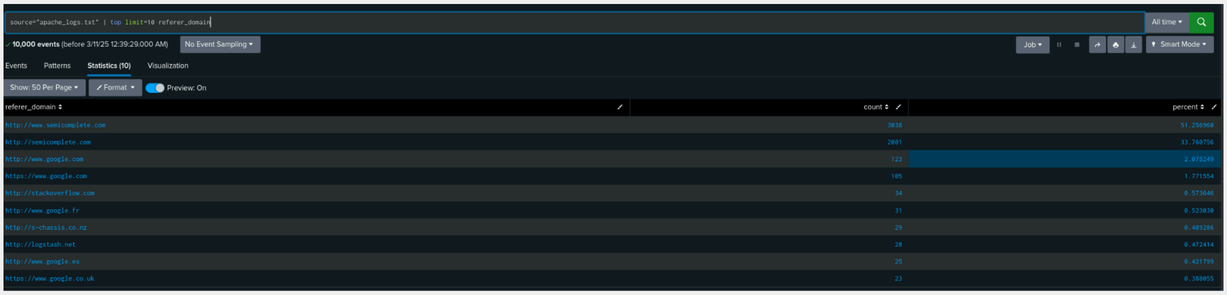
- What is that method used for?

```
POST: 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?

```
We did see some changes in referer_domain, the count decreased
significantly.
Before:
```

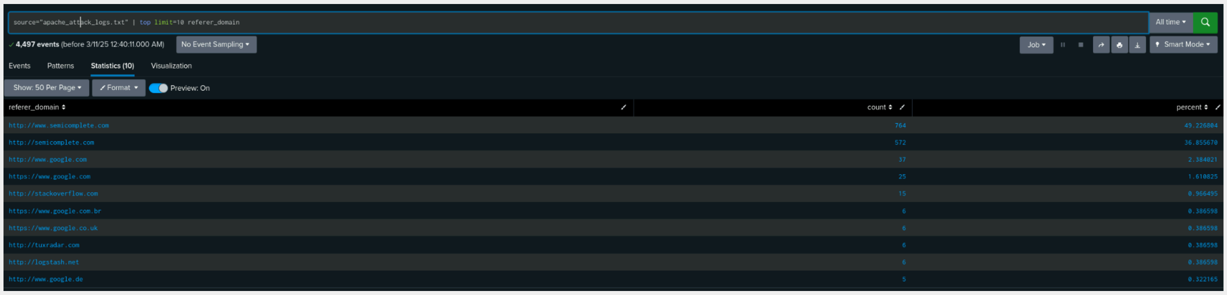


```
source="apache_logs.txt" | top limit=10 referer_domain
```

✓ **10,000 events** (before 3/11/25 12:39:29.000 AM) No Event Sampling

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

```
After:
```



```
source="apache_attack_logs.txt" | top limit=10 referer_domain
```

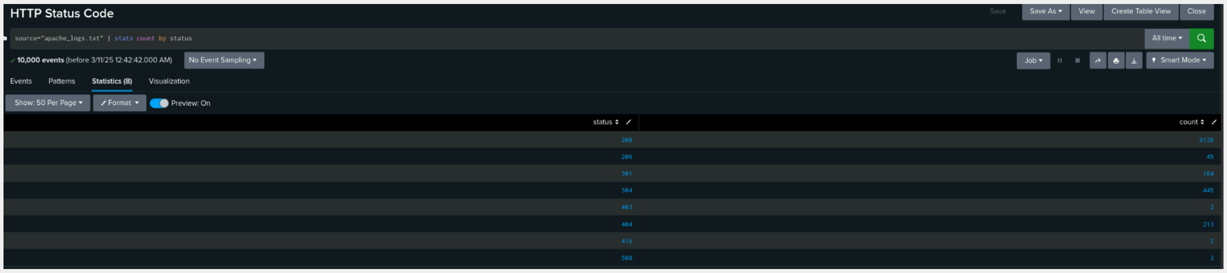
✓ **4,497 events** (before 3/11/25 12:40:11.000 AM) No Event Sampling

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?

We did detect a suspicious change in HTTP response codes, specifically with response code 200 and 404. Response code 200 saw a decrease in amount and 404 saw an increase.
Normal Apache Logs:



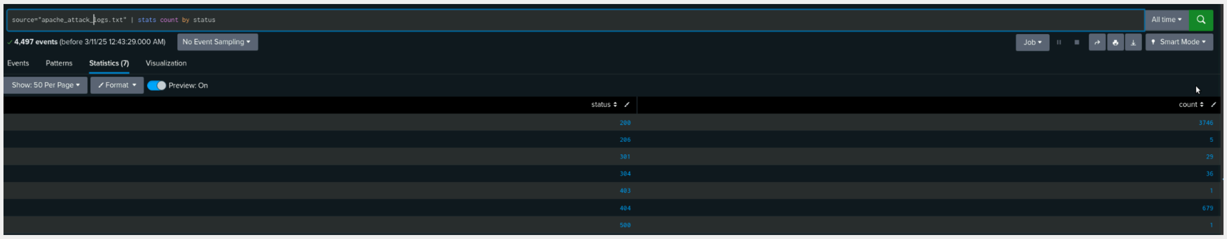
HTTP Status Code

```
source="apache_logs.txt" | stats count by status
```

✓ 10,000 events (before 3/11/25 12:42:42.000 AM)

status	count
200	9126
206	45
301	164
304	445
403	2
404	213
416	2
500	3

After attack:



```
source="apache_attack_logs.txt" | stats count by status
```

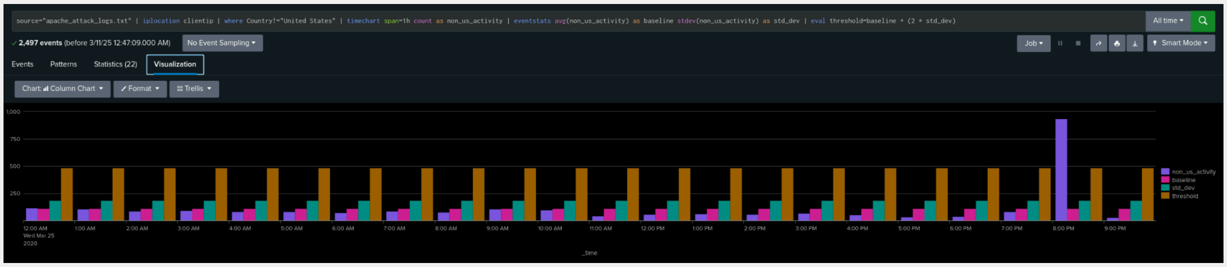
✓ 4,497 events (before 3/11/25 12:43:29.000 AM)

status	count
200	3746
206	5
301	29
304	36
403	1
404	679
500	1

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

Yes we did detect a suspicious volume of international activity



```
source="apache_attack_logs.txt" | iplocation clientip | where Country!="United States" | timechart span=1h count as non_us_activity | eventstats avg(non_us_activity) as baseline stdev(non_us_activity) as std_dev | eval threshold=baseline + (2 * std_dev)
```

✓ 2,497 events (before 3/11/25 12:47:09.000 AM)

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

The count was 937 at 08:00 PM

- Would your alert be triggered for this activity?

```
Yes our alert would have been triggered as we set the threshold to more than
118 in an hour to send an alert and this was well above that.
```

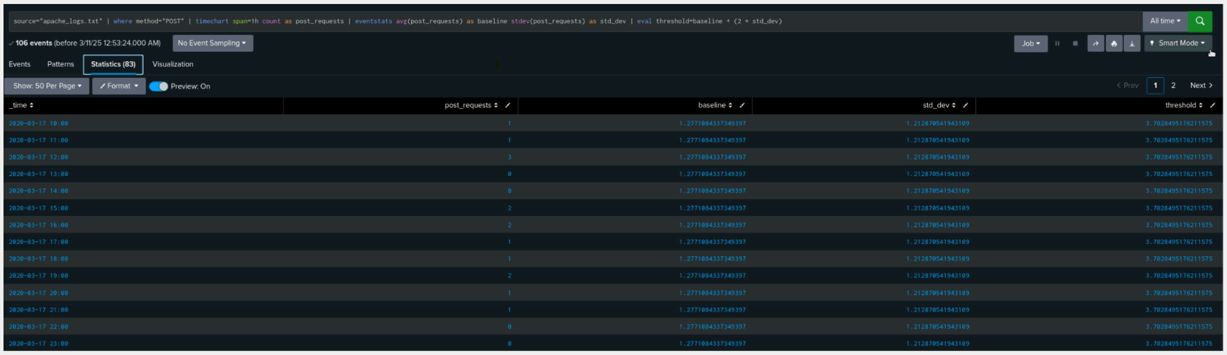
- After reviewing, would you change the threshold that you previously selected?

```
I would keep it as it is, and keep monitoring Apache logs and see if there
is any requirement to increase it.
```

Alert Analysis for HTTP POST Activity

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

```
Yes we did detect a spike of HTTP POST activity.
Normal Apache Logs:
```

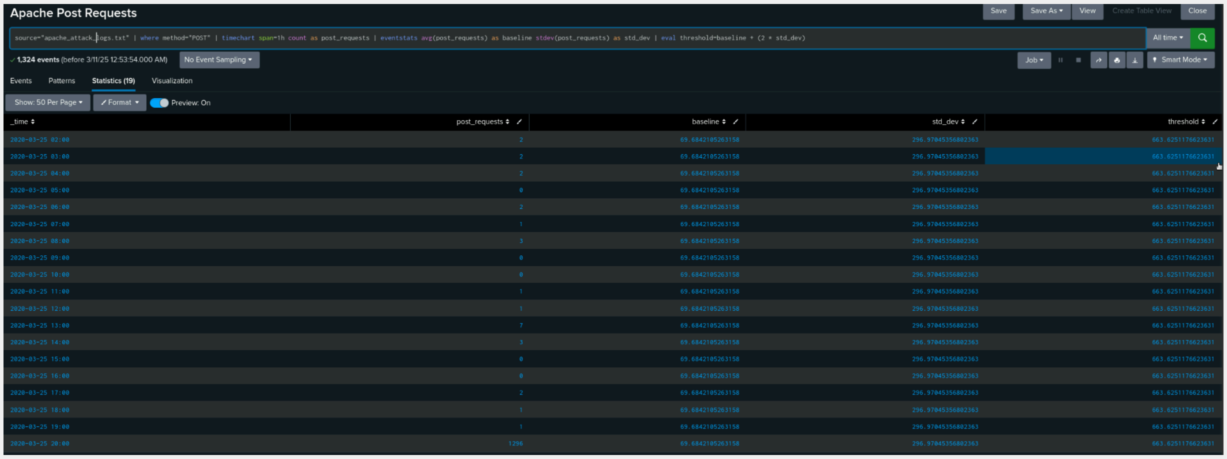


```
source="apache_logs.txt" | where method="POST" | timechart span=1h count as post_requests | eventstats avg(post_requests) as baseline stdev(post_requests) as std_dev | eval threshold=baseline + (2 * std_dev)
```

✓ **106 events** (before 3/11/25 12:53:24.000 AM)

_time	post_requests	baseline	std_dev	threshold
2020-03-17 10:00	1	1.2771084337349397	1.212870541943109	3.7028495176211575
2020-03-17 11:00	1	1.2771084337349397	1.212870541943109	3.7028495176211575
2020-03-17 12:00	3	1.2771084337349397	1.212870541943109	3.7028495176211575
2020-03-17 13:00	0	1.2771084337349397	1.212870541943109	3.7028495176211575
2020-03-17 14:00	0	1.2771084337349397	1.212870541943109	3.7028495176211575
2020-03-17 15:00	2	1.2771084337349397	1.212870541943109	3.7028495176211575
2020-03-17 16:00	2	1.2771084337349397	1.212870541943109	3.7028495176211575
2020-03-17 17:00	1	1.2771084337349397	1.212870541943109	3.7028495176211575
2020-03-17 18:00	1	1.2771084337349397	1.212870541943109	3.7028495176211575
2020-03-17 19:00	2	1.2771084337349397	1.212870541943109	3.7028495176211575
2020-03-17 20:00	1	1.2771084337349397	1.212870541943109	3.7028495176211575
2020-03-17 21:00	1	1.2771084337349397	1.212870541943109	3.7028495176211575
2020-03-17 22:00	0	1.2771084337349397	1.212870541943109	3.7028495176211575
2020-03-17 23:00	0	1.2771084337349397	1.212870541943109	3.7028495176211575

```
After:
```



Apache Post Requests

```
source="apache_attack_logs.txt" | where method="POST" | timechart span=1h count as post_requests | eventstats avg(post_requests) as baseline stdev(post_requests) as std_dev | eval threshold=baseline + (2 * std_dev)
```

✓ **1,324 events** (before 3/11/25 12:53:54.000 AM)

_time	post_requests	baseline	std_dev	threshold
2020-03-25 02:00	2	69.6842105263158	296.97045356802363	663.6251176623631
2020-03-25 03:00	2	69.6842105263158	296.97045356802363	663.6251176623631
2020-03-25 04:00	2	69.6842105263158	296.97045356802363	663.6251176623631
2020-03-25 05:00	0	69.6842105263158	296.97045356802363	663.6251176623631
2020-03-25 06:00	2	69.6842105263158	296.97045356802363	663.6251176623631
2020-03-25 07:00	1	69.6842105263158	296.97045356802363	663.6251176623631
2020-03-25 08:00	3	69.6842105263158	296.97045356802363	663.6251176623631
2020-03-25 09:00	0	69.6842105263158	296.97045356802363	663.6251176623631
2020-03-25 10:00	0	69.6842105263158	296.97045356802363	663.6251176623631
2020-03-25 11:00	1	69.6842105263158	296.97045356802363	663.6251176623631
2020-03-25 12:00	1	69.6842105263158	296.97045356802363	663.6251176623631
2020-03-25 13:00	7	69.6842105263158	296.97045356802363	663.6251176623631
2020-03-25 14:00	3	69.6842105263158	296.97045356802363	663.6251176623631
2020-03-25 15:00	0	69.6842105263158	296.97045356802363	663.6251176623631
2020-03-25 16:00	0	69.6842105263158	296.97045356802363	663.6251176623631
2020-03-25 17:00	2	69.6842105263158	296.97045356802363	663.6251176623631
2020-03-25 18:00	1	69.6842105263158	296.97045356802363	663.6251176623631
2020-03-25 19:00	1	69.6842105263158	296.97045356802363	663.6251176623631
2020-03-25 20:00	1296	69.6842105263158	296.97045356802363	663.6251176623631

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

```
The count was 1296 at 08:00 PM
```

- When did it occur?

```
8 pm Wednesday March 25, 2020
```

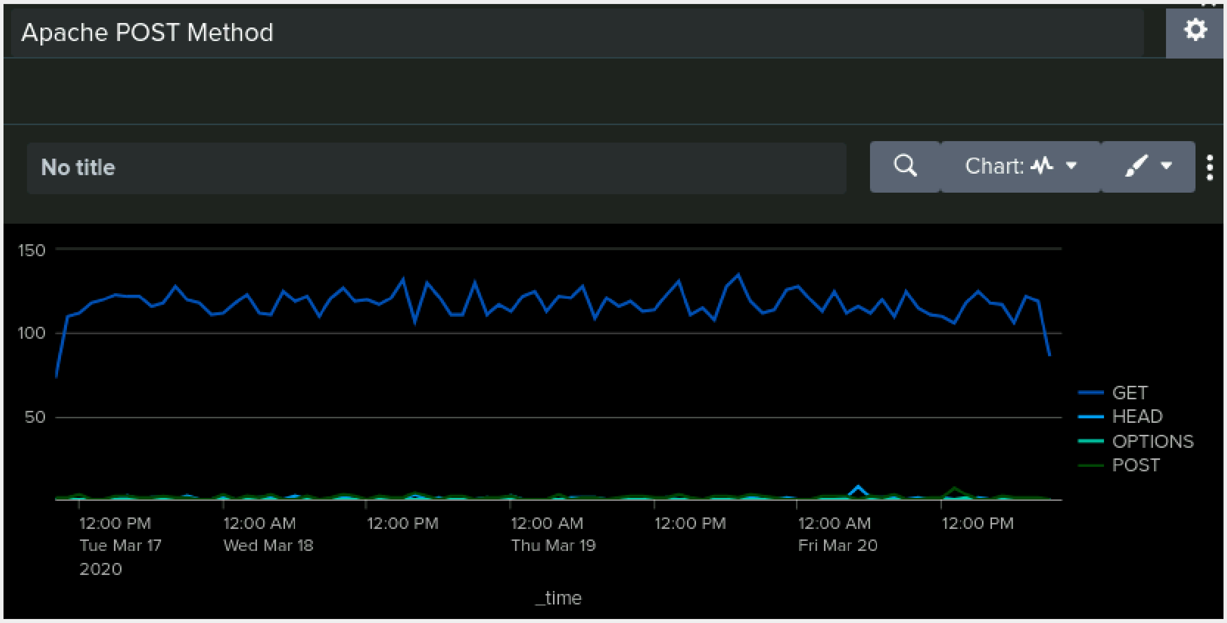
- After reviewing, would you change the threshold that you previously selected?

```
Yes, I would change it. I initially set it to 3, but considering the amount of requests, I have increased it to 15, and keep monitoring Apache logs.
```

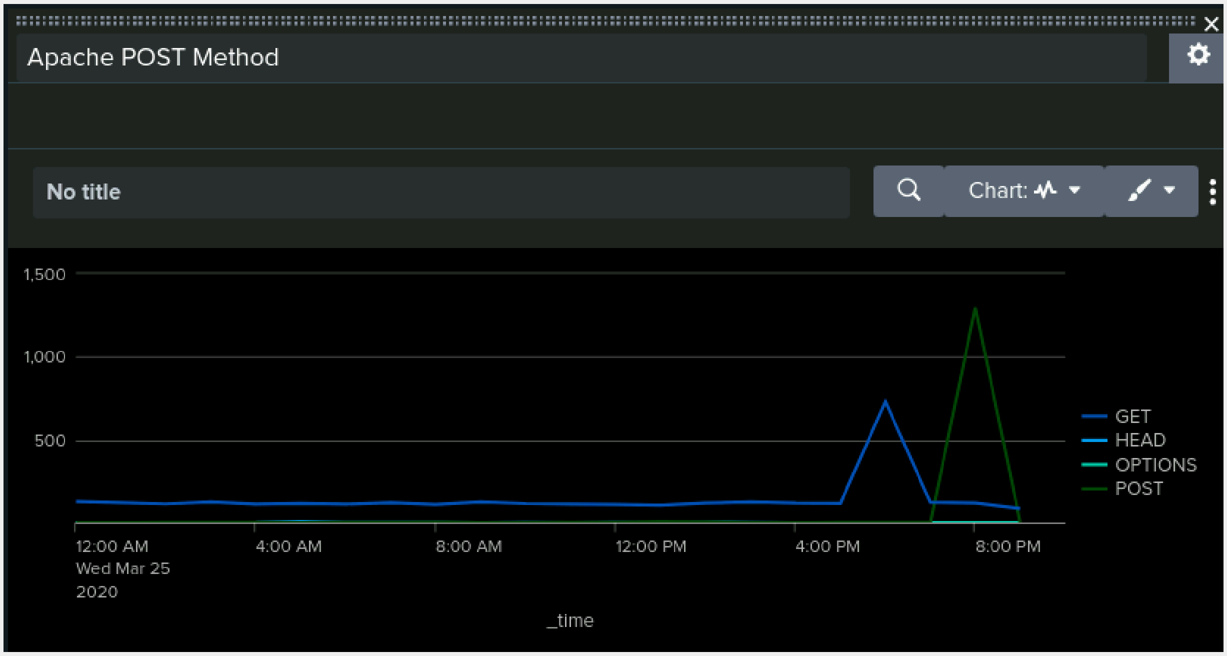
Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
Yes, there is a significant spike in HTTP methods: GET & POST
Before Attack:
```



```
After:
```



- Which method seems to be used in the attack?

```
POST
```

- At what times did the attack start and stop?

```
Attack starts between 7PM to 9PM
```

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

```
1296
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Yes, activities significantly increased in 2 cities from Ukraine
```

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

```
Kiev and Kharkiv in Ukraine both had an increase in activity
```

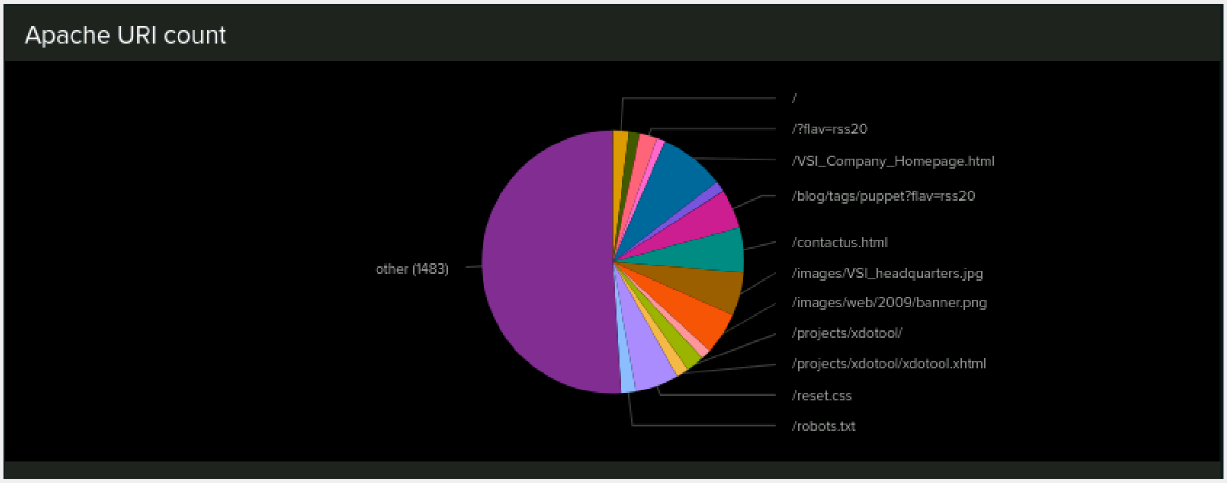
- What is the count of that city?

```
Kiev = 439
Kharkiv = 433
```

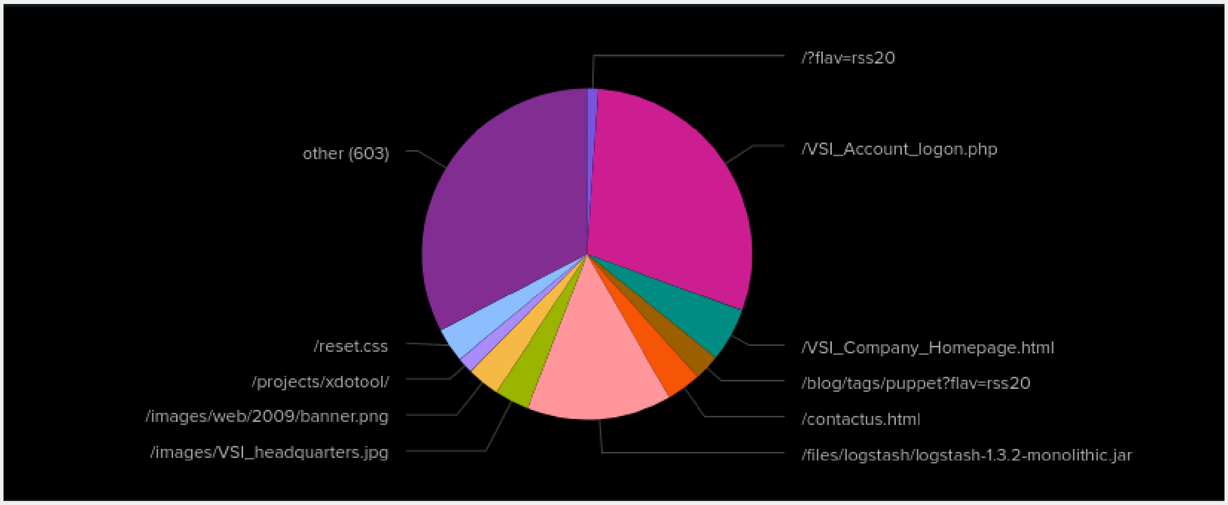
Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes the chart shows suspicious activity.
Before attack:
```



```
After:
```



- What URI is hit the most?

```
Apart from ‘other’ section, /VSI_Account_logon.php hit the most
```

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

```
Based on the URI being accessed the attacker could potentially be trying a
brute force attack or an SQL injection.
```