Cybersecurity

Project 3 Review Questions

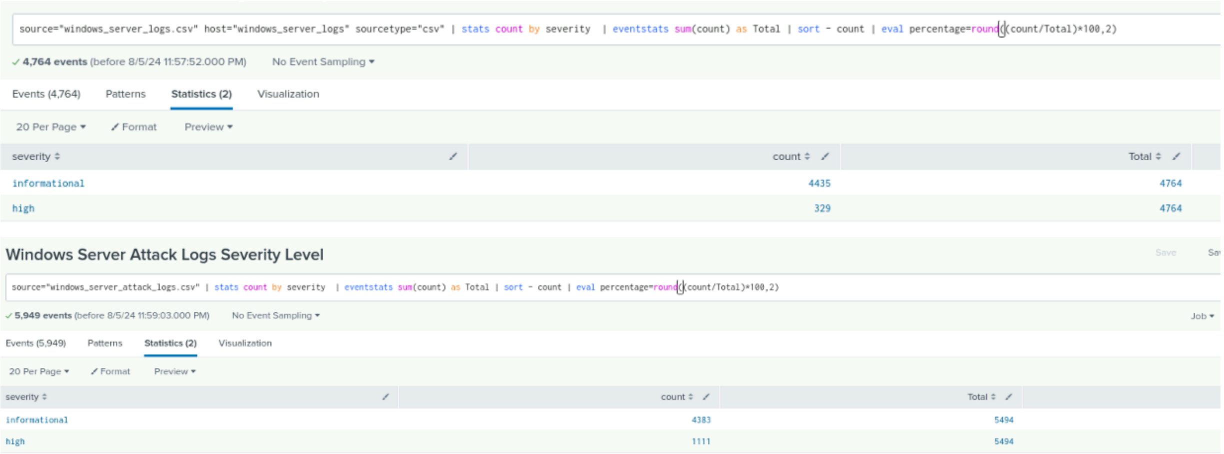
Make a copy of this document before you begin. Place your answers below each question.

Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

Yes, there was a significant increase in high-severity level events during the attacks,(nearly tripled) indicating the potential serious issues or threats that require further investigation.



```
source="windows_server_logs.csv" host="windows_server_logs" sourcetype="csv" | stats count by severity  | eventstats sum(count) as Total | sort - count | eval percentage=round((count/Total)*100,2)
```

✓ 4,764 events (before 8/5/24 11:57:52.000 PM)   No Event Sampling ▾

severity	count	Total
informational	4435	4764
high	329	4764

Windows Server Attack Logs Severity Level

```
source="windows_server_attack_logs.csv" | stats count by severity  | eventstats sum(count) as Total | sort - count | eval percentage=round((count/Total)*100,2)
```

✓ 5,949 events (before 8/5/24 11:59:03.000 PM)   No Event Sampling ▾

severity	count	Total
informational	4383	5494
high	1111	5494

Report Analysis for Failed Activities

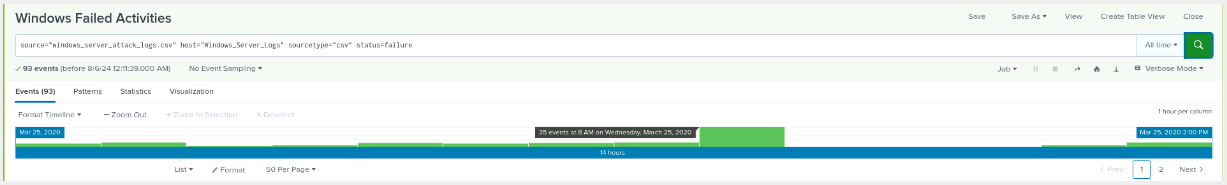
- Did you detect any suspicious changes in failed activities?

The percentage of successful activities slightly increased, while the percentage of failed activities slightly decreased. This could suggest a possible breach where an unauthorized user gained access and performed activities that would usually fail. It would warrant further investigation.
Success went from 97% to 98%
Failure went 3% to 2%
No big changes to failed activities.

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

Yes, a significant spike in failed activities was noted, which is considered suspicious -



Windows Failed Activities

```
source="windows_server_attack_logs.csv" host="Windows_Server_Logs" sourcetype="csv" status=failure
```

✓ 93 events (before 8/6/24 12:11:39.000 AM)

35 events at 8 AM on Wednesday, March 25, 2020

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

a spike exceeded the alert threshold of 20 events with 35 recorded between 8 am and 9 am on march 25, 2020

- When did it occur?

a spike exceeded the alert threshold of 20 events with 35 recorded between 8 am and 9 am on march 25, 2020

- Would your alert be triggered for this activity?

Yes, the alert threshold was set at 20 events, so it was triggered

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

After reviewing, I would keep the threshold the same at 20 because it was able to work correctly in capturing suspicious activity without generating too many false positives. If there are more false positives in the future, I may need to re-evaluate and adjust, but for now I would keep it as-is.

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

Yes, a spike was detected that exceeded the threshold - 70 successful logins occurring between 1:50 and 2:30 am on march 25, 2020

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

70 successful logins occurring between 1:50 and 2:30 am on march 25, 2020

- Who is the primary user logging in?

ACME-002 pckomono

- When did it occur?

between 1:50 and 2:30 am on march 25, 2020

- Would your alert be triggered for this activity?

Yes - the alert threshold was set at 20 successful logins, so it was triggered

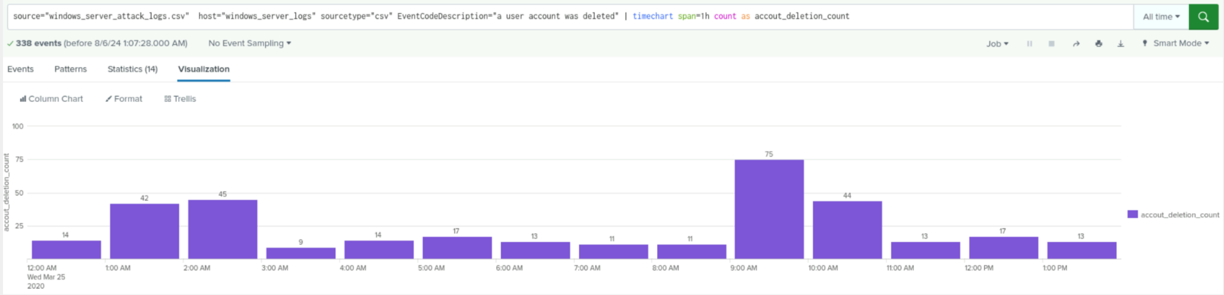
- After reviewing, would you change your threshold from what you previously selected?

After reviewing, I would consider increasing the threshold slightly, perhaps to 23 or 25.

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
Yes, there were multiple spikes in deleted accounts. There were 42 and 45
account deleted between 1 and 2 am, and 75 and 44 accounts deleted between
10-11 am on march 25, 2020.
```



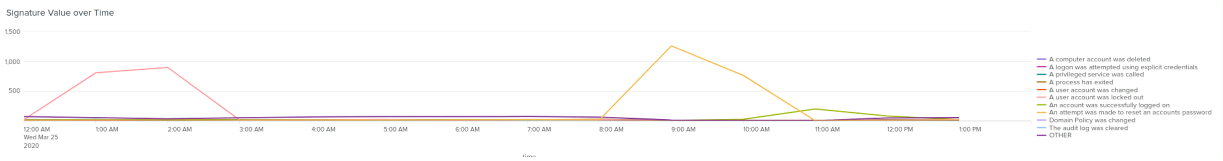
```
source="windows_server_attack_logs.csv"  host="windows_server_logs" sourcetype="csv" EventCodeDescription="a user account was deleted" | timechart span=1h count as accout_deletion_count
```

✓ 338 events (before 8/6/24 1:07:28.000 AM) No Event Sampling ▾

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
Yes, early in the morning, approx 6-8 hours before the attack, a large
number of user account lockouts occurred, then there was a high number of
password reset attempts during the attack
```



- What signatures stand out?

```
‘A user account was locked out’ and ‘an attempt was made to reset an
account’s password’
```

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

```
A user account was locked out began at 12 am and stopped at 3 am on
3/25/2020.
An attempt was made to reset an accounts password began at 8 am and stopped
at 11 am on 3/25/2020
```

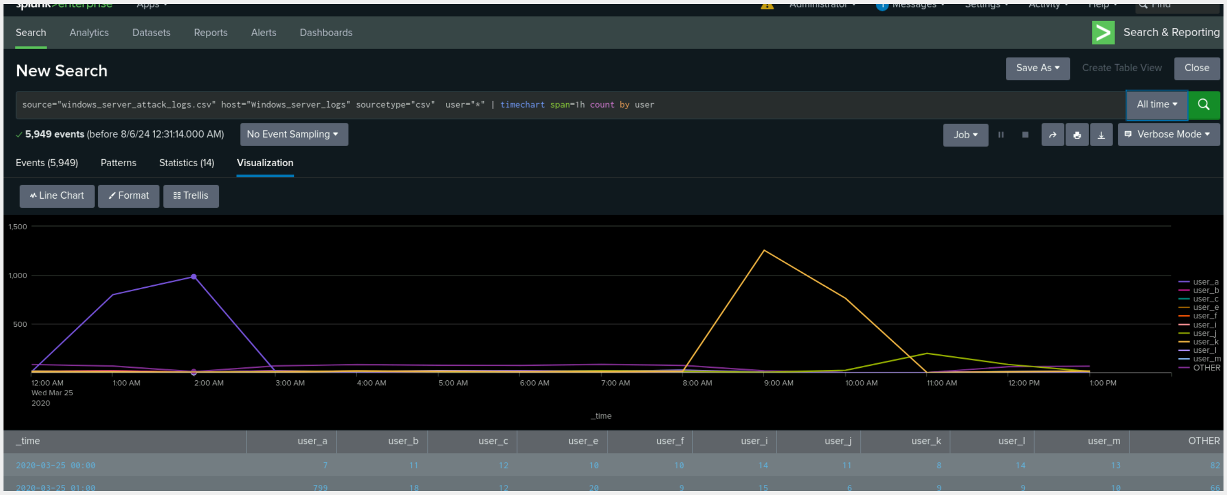
- What is the peak count of the different signatures?

```
A user account was locked out had peak count of 896, and an attempt was made
to reset an account’s password had a peak count of 1258
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes, suspicious activity was detected with user_a and user_k at different
times on march 25, 2020
```



New Search

```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv"  user="*" | timechart span=1h count by user
```

✓ 5,949 events (before 8/6/24 12:31:14.000 AM)

_time	user_a	user_b	user_c	user_e	user_f	user_i	user_j	user_k	user_l	user_m	OTHER
2020-03-25 00:00	7	11	12	10	10	14	11	8	14	13	82
2020-03-25 01:00	799	18	12	20	9	15	6	9	9	10	66

- Which users stand out?

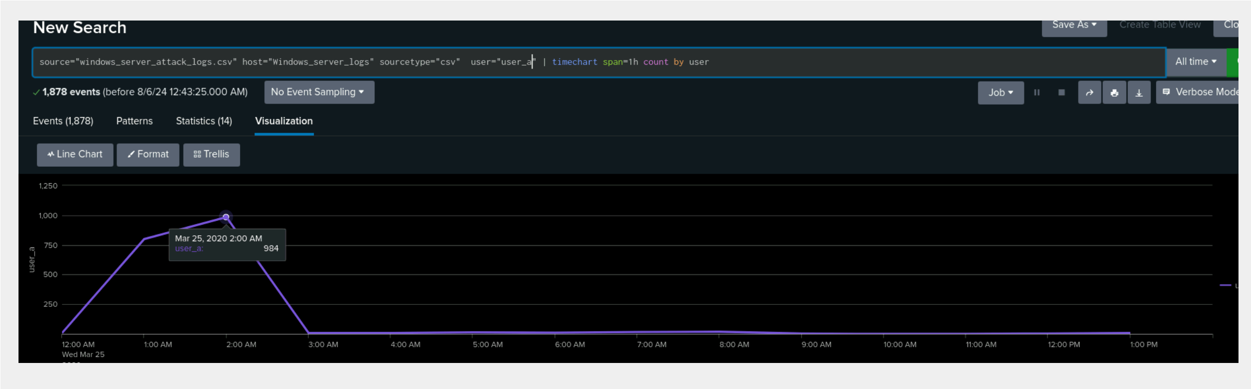
```
user_a and user_k
```

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

```
User_a on March 25, 2020, from 12 AM to 3 AM and User_k on March 25, 2020,
from 8 AM to 11 AM.
```

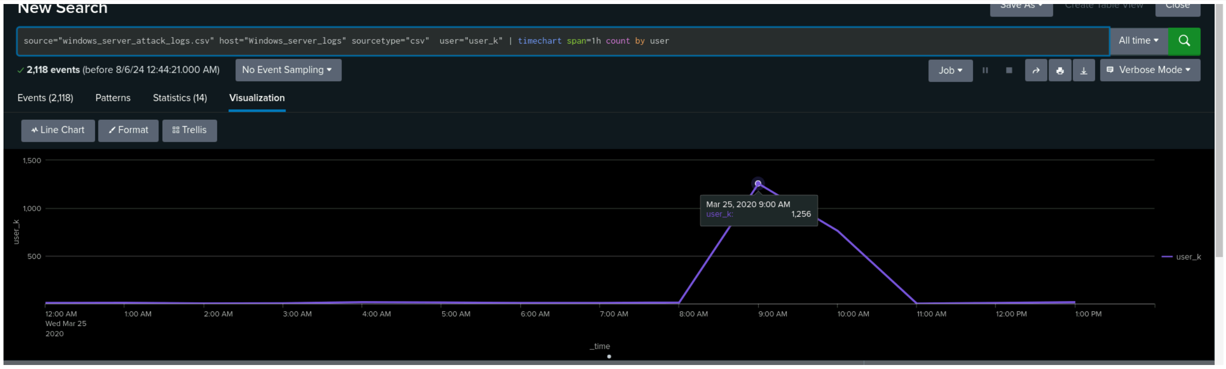
- What is the peak count of the different users?

```
User_a had a peak count of 984 and User_k had a peak count of 1,256
```



```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv"  user="user_a" | timechart span=1h count by user
```

✓ 1,878 events (before 8/6/24 12:43:25.000 AM)



```
source="windows_server_attack_logs.csv" host="Windows_server_logs" sourcetype="csv"  user="user_k" | timechart span=1h count by user
```

✓ 2,118 events (before 8/6/24 12:44:21.000 AM)

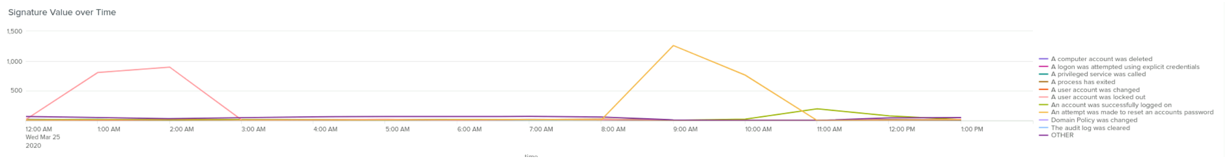
Dashboard Analysis for Signatures with Bar, Graph, and Pie Charts

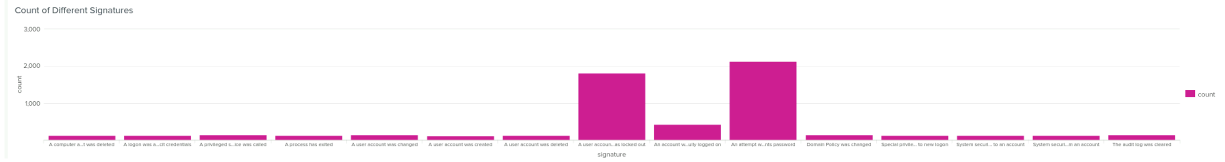
- Does anything stand out as suspicious?

```
Yes, the values for the signatures “A user account was locked out” and “An
attempt was made to reset an account’s password” both increased
significantly in occurrence compared to the other signatures
```

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

```
Yes, they match the same trends in terms of increased signature activity of
the same types as the time chart
```

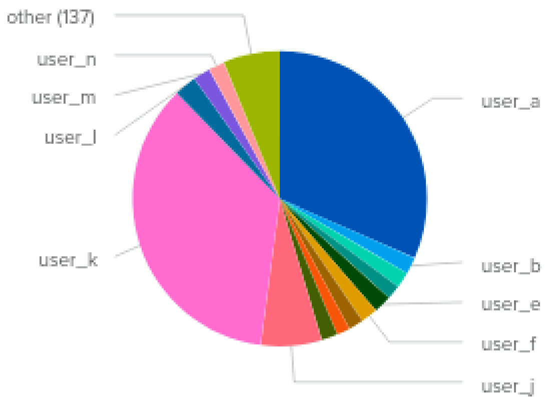




Dashboard Analysis for Users with Bar, Graph, and Pie Charts

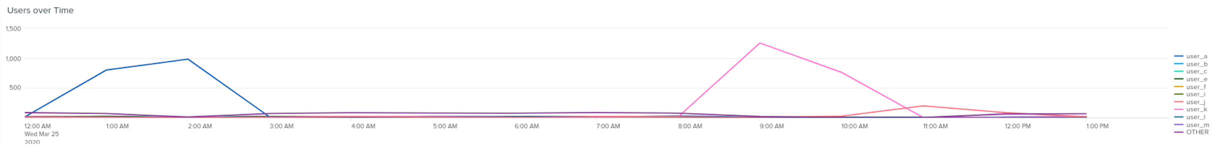
- Does anything stand out as suspicious?

```
Yes, activity from user_a & user_k increased significantly during the high signature activity periods. Each user coincided with a particular type of signature.
```



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

```
yes, they match and show the same trends.
```



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?

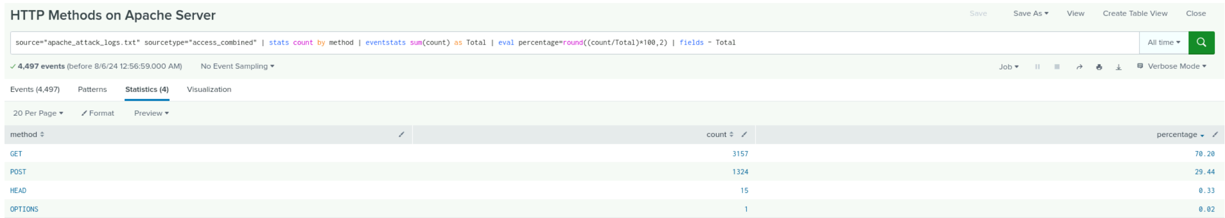
```
The advantage of using statistical charts is that they make it easy to differentiate users and determine which users are more active. The disadvantage is that as the number of users increases, the charts become busy and harder to read.It helps with me being a visual learner as well.
```

Apache Web Server Log Questions

Report Analysis for Methods

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

Yes, there was a significant increase in POST method events, going from 106 to 1,324 logged events



HTTP Methods on Apache Server

```
source="apache_attack_logs.txt" sourcetype="access_combined" | stats count by method | eventstats sum(count) as Total | eval percentage=round((count/Total)*100,2) | fields - Total
```

✓ 4,497 events (before 8/6/24 12:56:59.000 AM) No Event Sampling ▾

method	count	percentage
GET	3157	70.20
POST	1324	29.44
HEAD	15	0.33
OPTIONS	1	0.02

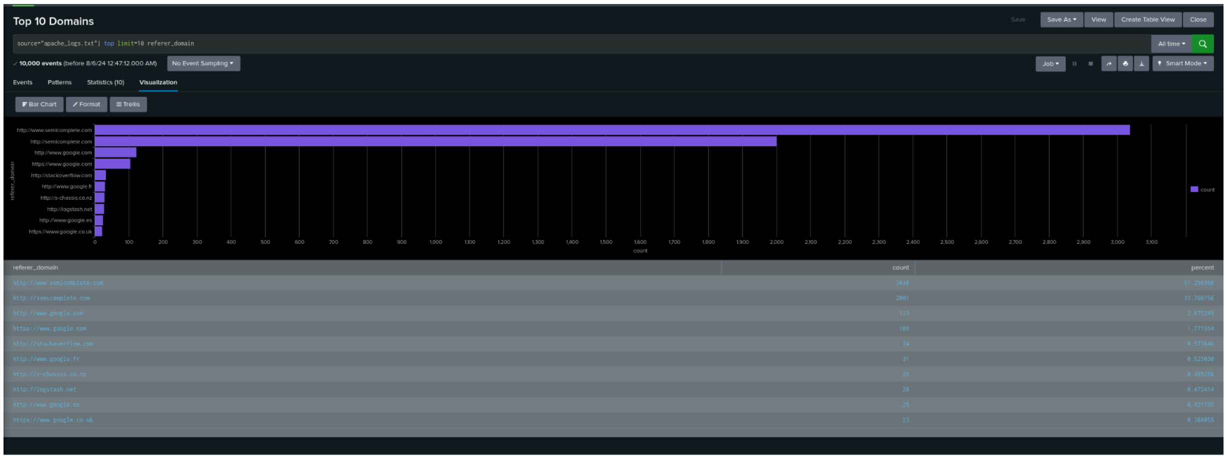
- What is that method used for?

POST method is used to send data to a server to create or modify a resource

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

No suspicious activity or changes were detected. The top 5 domains remained the same with high counts

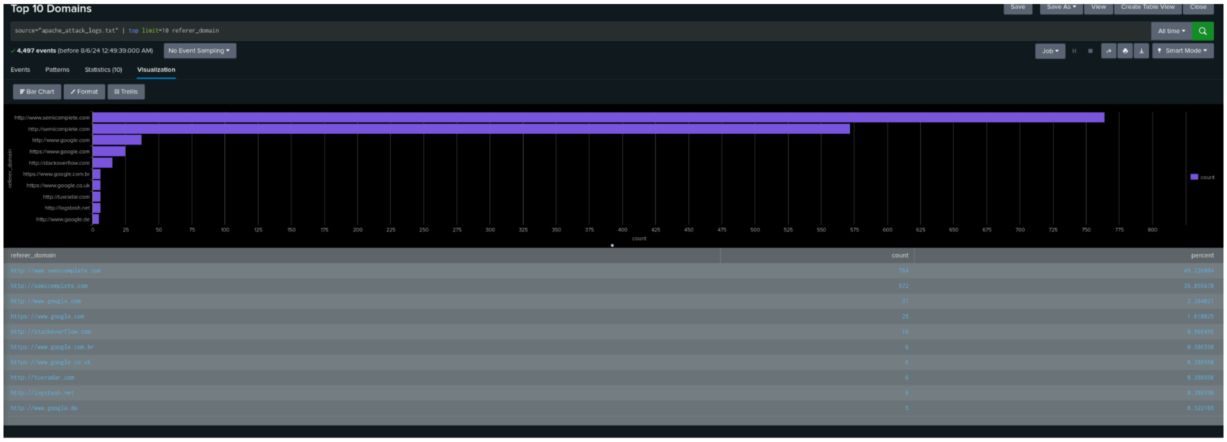


Top 10 Domains

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

✓ 10,000 events (before 8/6/24 12:47:12.000 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



Top 10 Domains

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

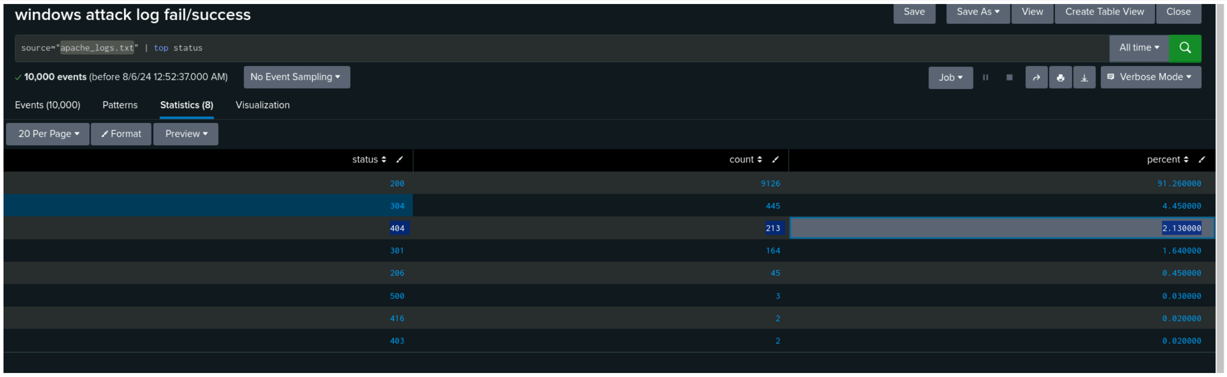
✓ 4,497 events (before 8/6/24 12:49:39.000 AM) No Event Sampling ▾

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?

```
Yes, the 404 response code increased from 2% to 15%, indicating potential
issues
```

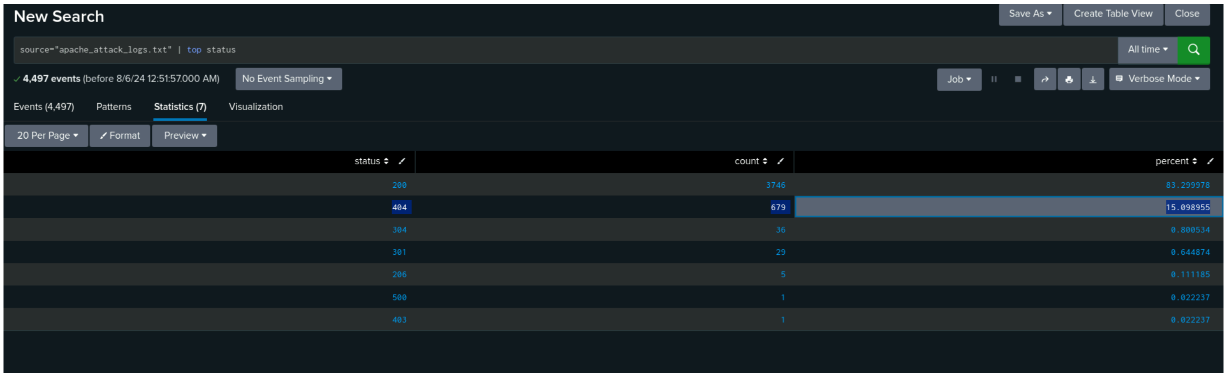


windows attack log fail/success

```
source="apache_logs.txt" | top status
```

✓ 10,000 events (before 8/6/24 12:52:37.000 AM) No Event Sampling ▾

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



New Search

```
source="apache_attack_logs.txt" | top status
```

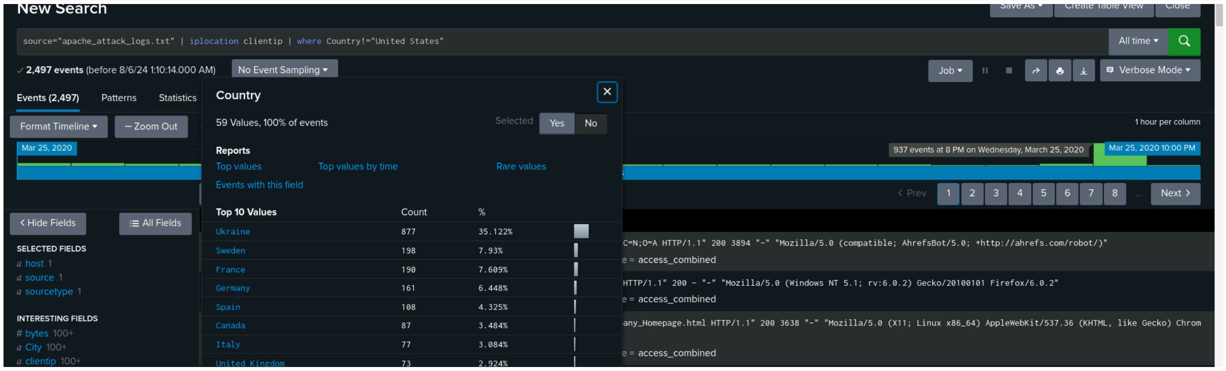
✓ 4,497 events (before 8/6/24 12:51:57.000 AM) No Event Sampling ▾

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 from Ukraine on 3/25/2020, at 8 PM, with
937 attacks
```



```
source="apache_attack_logs.txt" | iplocation clientip | where Country!="United States"
```

✓ 2,497 events (before 8/6/24 1:10:14.000 AM)

937 events at 8 PM on Wednesday, March 25, 2020

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- # bytes 100+
- a City 100+
- a clientip 100+

Country

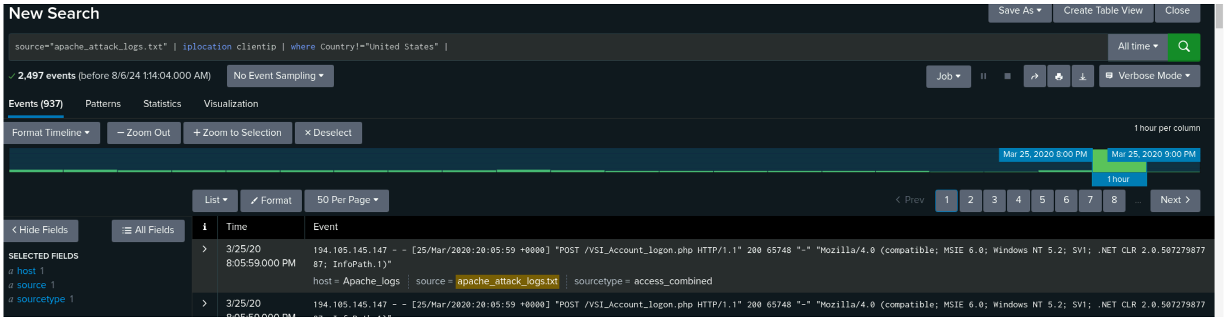
59 Values, 100% of events

Top 10 Values	Count	%
Ukraine	877	35.122%
Sweden	198	7.93%
France	190	7.609%
Germany	161	6.448%
Spain	108	4.325%
Canada	87	3.484%
Italy	77	3.084%
United Kingdom	73	2.924%

```
C=N;O=A HTTP/1.1" 200 3894 "-" "Mozilla/5.0 (compatible; AhrefsBot/5.0; +http://ahrefs.com/robot/)"
e = access_combined
HTTP/1.1" 200 - "-" "Mozilla/5.0 (Windows NT 5.1; rv:6.0.2) Gecko/20100101 Firefox/6.0.2"
e = access_combined
any_Homepage.html HTTP/1.1" 200 3638 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
e = access_combined
```

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

```
937 attacks were recorded at 8 PM on 3/25/2020.
```



```
source="apache_attack_logs.txt" | iplocation clientip | where Country!="United States" |
```

✓ 2,497 events (before 8/6/24 1:14:04.000 AM)

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

i	Time	Event
>	3/25/20 8:05:59.000 PM	194.105.145.147 - - [25/Mar/2020:20:05:59 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.507279877 87; InfoPath.1)" host = Apache_logs source = apache_attack_logs.txt sourcetype = access_combined
>	3/25/20	194.105.145.147 - - [25/Mar/2020:20:05:59 +0000] "POST /VSI_Account_logon.php HTTP/1.1" 200 65748 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.507279877

- Would your alert be triggered for this activity?

```
Yes, the alert threshold was set at 150 events, so this would trigger it
```

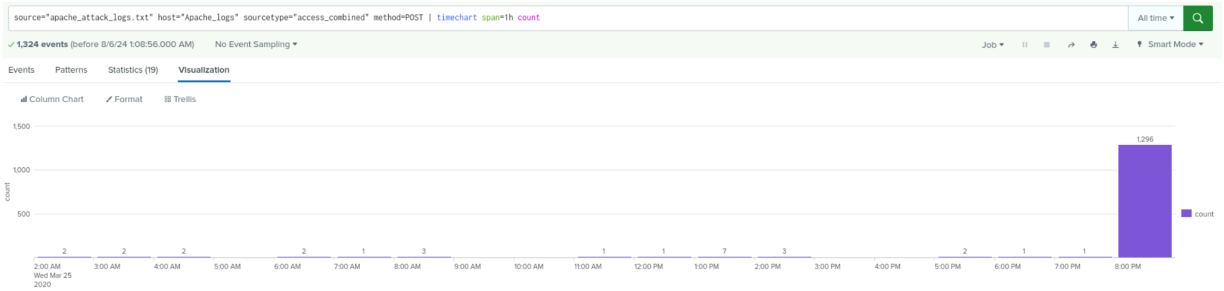
- After reviewing, would you change the threshold that you previously selected?

```
After reviewing, I determined no changes were needed, the current threshold
will stay the same
```

Alert Analysis for HTTP POST Activity

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

```
Yes, there were 1,296 POST requests during the peak hour at 8PM on 3/25/2020
```



```
source="apache_attack_logs.txt" host="Apache_logs" sourcetype="access_combined" method=POST | timechart span=1h count
```

✓ 1,324 events (before 8/6/24 1:08:56.000 AM)

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

Peak count was 1,296 at 8PM on 3/25/2020

- When did it occur?

8PM on 3/25/2020

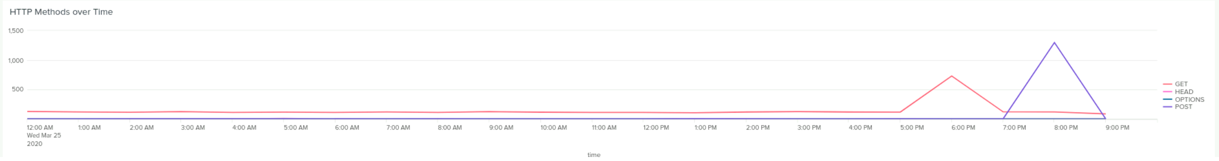
- After reviewing, would you change the threshold that you previously selected?

The previous threshold was 4, so after reviewing, I would change that to 10 to reduce the likelihood of false positives while still capturing significant activity. Not an enormous increase, but would increase to 10.

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

Yes, there was a significant spike in GET and POST methods atypical of standard HTTP request traffic. The POST methods were primarily used in the attack, but there was also an atypical spike in GET requests just before the POST cluster



- Which method seems to be used in the attack?

POST methods were primarily used in the attack.

- At what times did the attack start and stop?

The attack started at 5 PM and ended at 9 PM on March 25, 2020.

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

The peak count of POST methods was 1,296 at 8 PM.

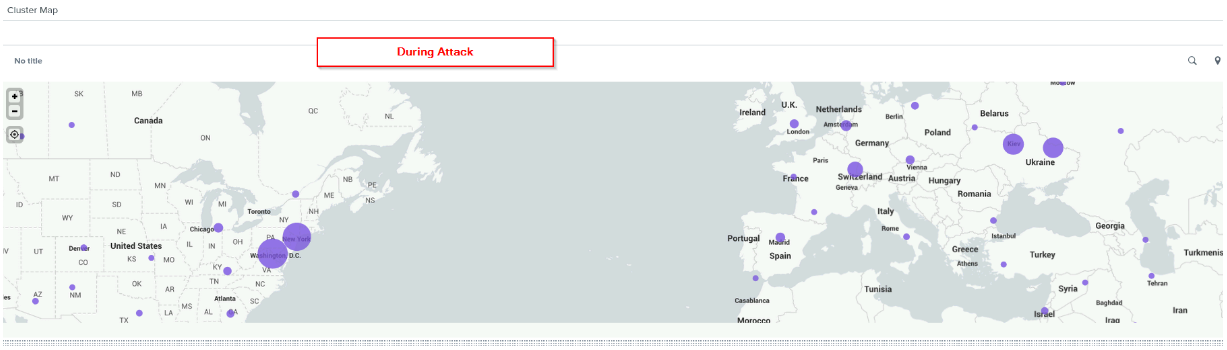
Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

Yes, there was a large amount of user activity logged in Ukraine. Ukraine and the surrounding regions are typically not a significant portion of the standard network traffic. Ukraine is considered a high-risk country, and this could indicate a threat actor and would warrant attention.

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

Ukraine, particularly the cities of Kiev and Kharkiv, had an unusually large amount of traffic for the region, which is not seen during normal operations



- What is the count of that city?

Kiev had 439 events & Kharkiv had 432 events during the attack

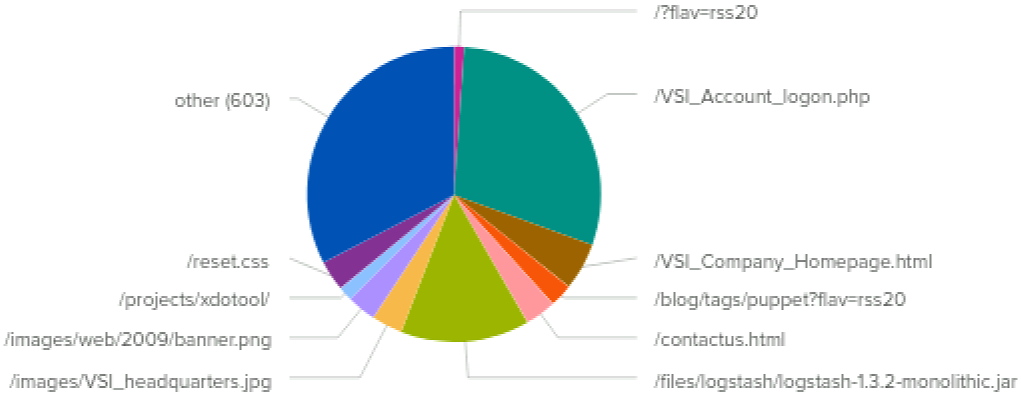
Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes, there was a large uptick in visits to the following URIs:
/VSI_Account_logon.php AND /files/logstash/logstash-1.3.2-monolithic.jar
```

- What URI is hit the most?

```
/VSI_Account_logon.php AND /files/logstash/logstash-1.3.2-monolithic.jar
```



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

```
The logon.php screen activity could indicate a brute force attack is being
attempted in a login field or another kind of attack related to .php. The
.jar URI could indicate a vulnerable .jar file, which are known to be
exploitable and are often considered insecure file types.
```