Cybersecurity

Project 3 Review Questions

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

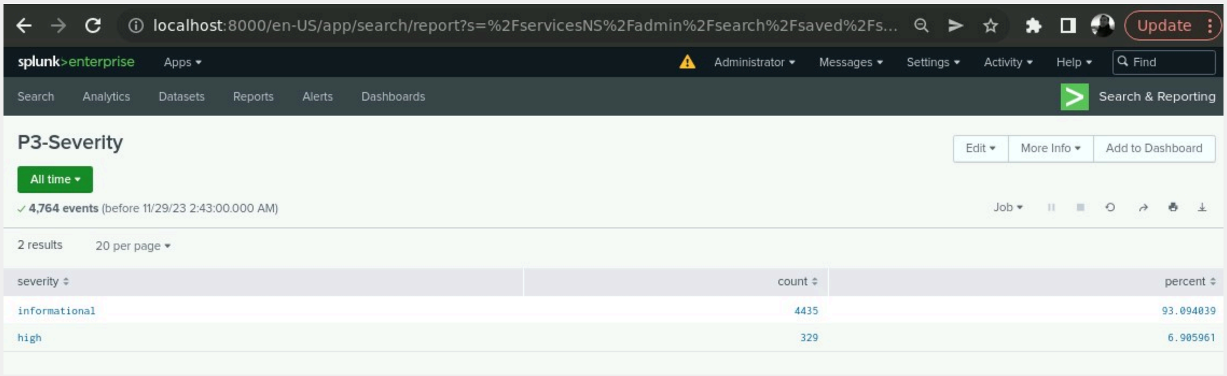
Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

A sharp rise in high severity events, jumping from 6.9% to 20.2% between 03/24/2020 and 03/25/2020, indicates potential tampering with "**Password Policy**" and "**Domain Policy**" during an ongoing attack. Urgent investigation is crucial to understand these events and the reasons behind their increase, mitigating risks associated with this security breach.

Screenshot of severity levels during the Windows server log monitoring session (03/24/2020):

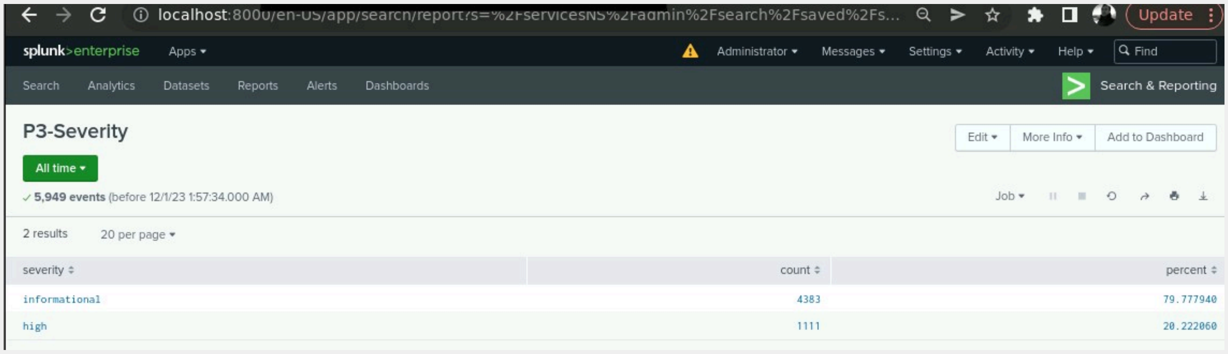


P3-Severity

✓ 4,764 events (before 11/29/23 2:43:00.000 AM)

2 results

severity	count	percent
informational	4435	93.094039
high	329	6.905961



P3-Severity

✓ 5,949 events (before 12/1/23 1:57:34.000 AM)

2 results

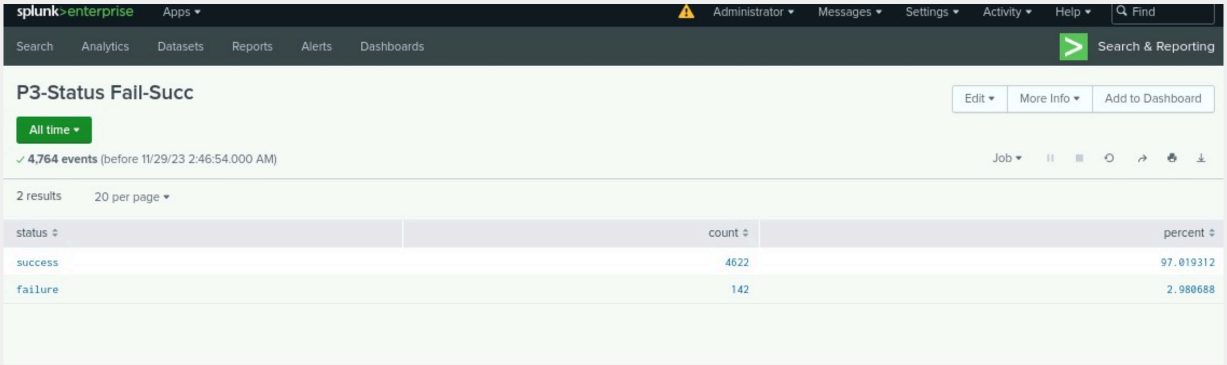
severity	count	percent
informational	4383	79.777940
high	1111	20.222060

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

Fewer failures occurred on 03/25/2020 compared to the first day (03/24/2020), with the failure rate dropping from 2.98% to 1.56%. This decline in failed activities suggests a potential security breach where attackers may have gained access to the system. Further investigation is necessary to confirm and address the implications of this decrease in failed activities.

Screenshot of failed activity for windows server log monitoring session:

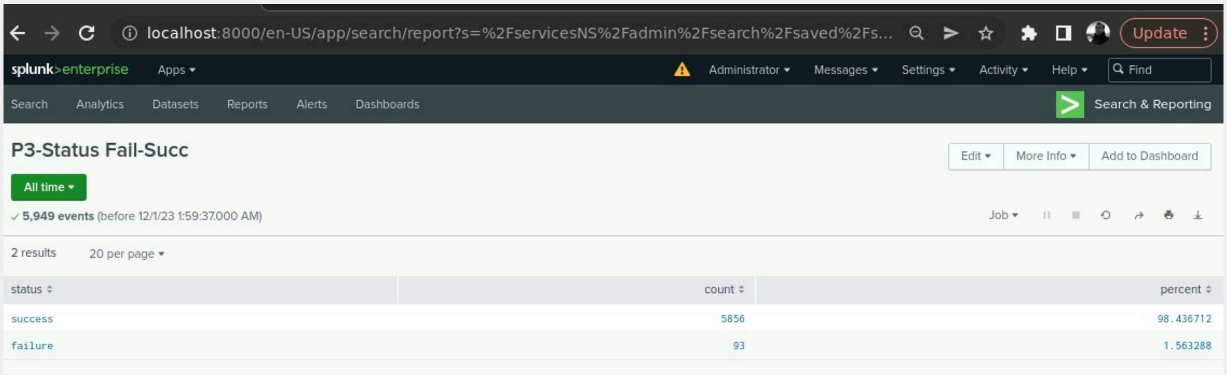


P3-Status Fail-Succ

✓ 4,764 events (before 11/29/23 2:46:54.000 AM)

2 results

status	count	percent
success	4622	97.019312
failure	142	2.980688



P3-Status Fail-Succ

✓ 5,949 events (before 12/1/23 1:59:37.000 AM)

2 results

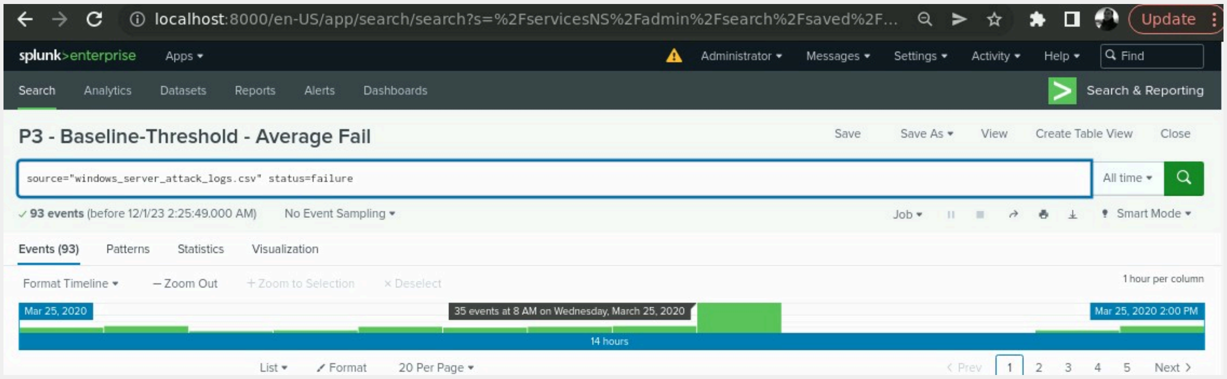
status	count	percent
success	5856	98.436712
failure	93	1.563288

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

A single suspicious surge in failed activity was detected on 03/25/2020, with 35 events concentrated between 8:00:42 am and 8:40:38 am. The percentage decreased from 2.98% to 1.56% could be indicative of a security breach. This timeframe exhibited a notably higher volume compared to any other hour in both normal and attack log files.

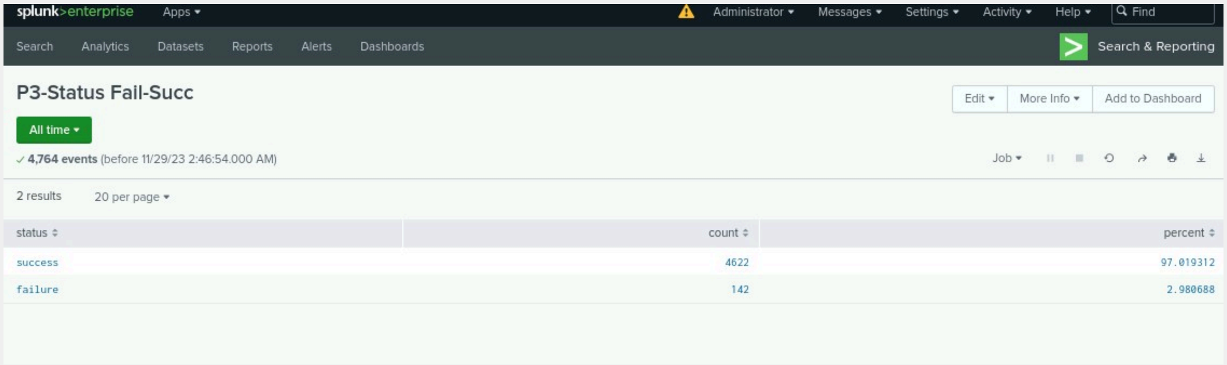
Screenshots of failed activity:



P3 - Baseline-Threshold - Average Fail

```
source="windows_server_attack_logs.csv" status=failure
```

✓ 93 events (before 12/1/23 2:25:49.000 AM)



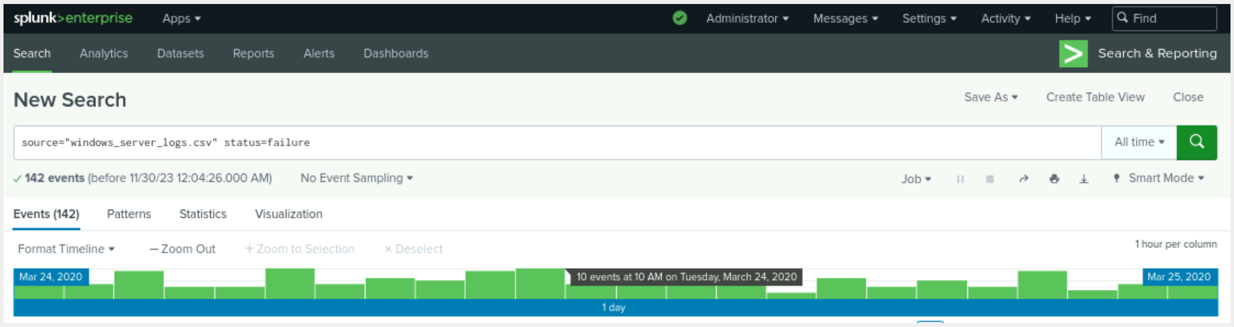
P3-Status Fail-Succ

All time

✓ 4,764 events (before 11/29/23 2:46:54.000 AM)

2 results 20 per page

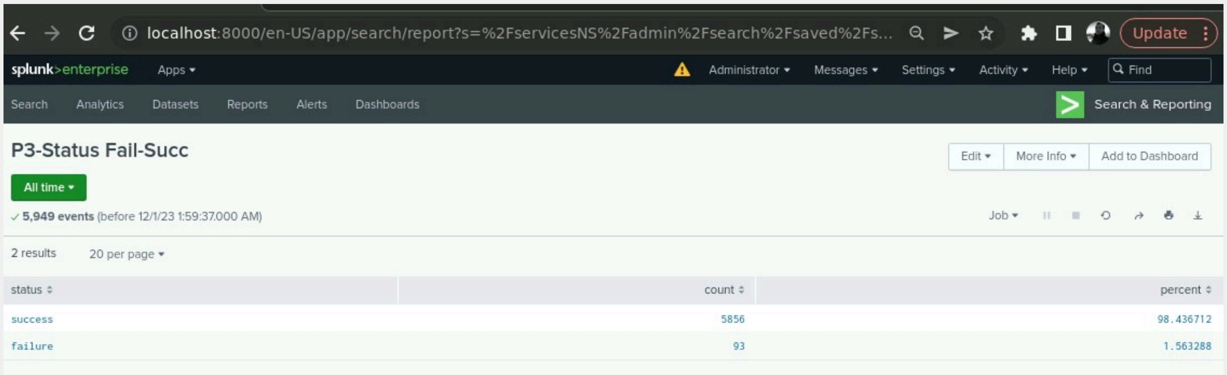
status	count	percent
success	4622	97.019312
failure	142	2.980688



New Search

```
source="windows_server_logs.csv" status=failure
```

✓ 142 events (before 11/30/23 12:04:26.000 AM) No Event Sampling



P3-Status Fail-Succ

All time

✓ 5,949 events (before 12/1/23 1:59:37.000 AM)

2 results 20 per page

status	count	percent
success	5856	98.436712
failure	93	1.563288

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

```
On March 25, 2020, 35 events occurred at 8:00:42 am, which is way more than
other hours.
```

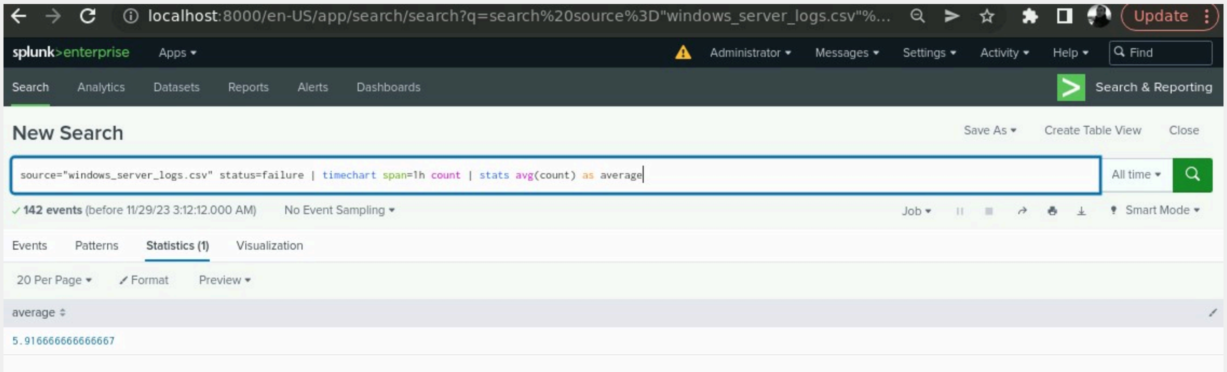
- When did it occur?

```
Suspicious activity failed a bunch at 8:00:42 am, and 8:40:38 am on March
25, 2020. The highest event count is 35 occurred at 8:00:42 am.
```

- Would your alert be triggered for this activity?

The alert would activate due to the activity, as the count of 35 exceeds the threshold of 15. The baseline threshold for such events was established at 7 occurrences. In Windows server log monitoring on 03/24/2020, the baseline, set at an average of 5.91 attempts plus 10%, equates to around 7 attempts per hour.

Screenshot:



```
source="windows_server_logs.csv" status=failure | timechart span=1h count | stats avg(count) as average
```

✓ 142 events (before 11/29/23 3:12:12.000 AM)

average
5.916666666666667

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

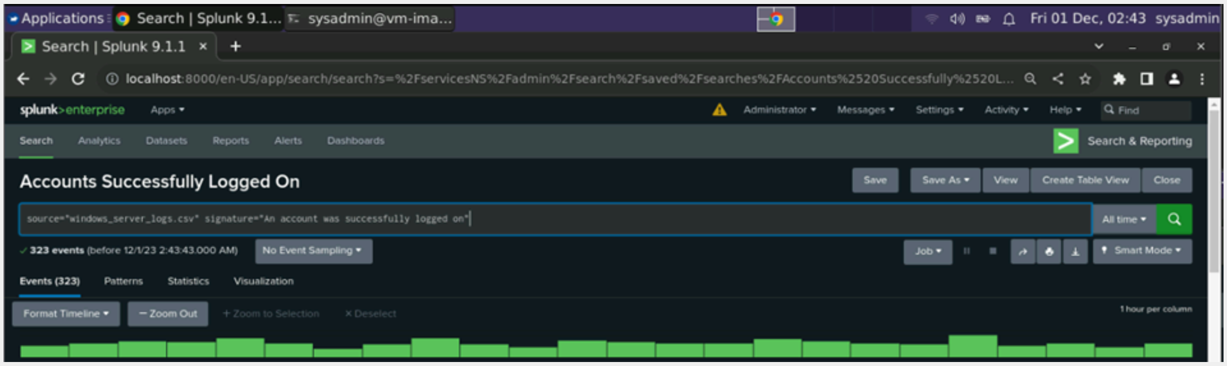
We'll raise the threshold from 7 to 11 events since on 03/25/2020, we noted 8 minor events. Adjusting the threshold prevents triggering the alert for non-threatening incidents.

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

Possible suspicious logins occurred at 11:00:49 am and 12:50:51 pm on March 25, 2020, totaling 273 events.

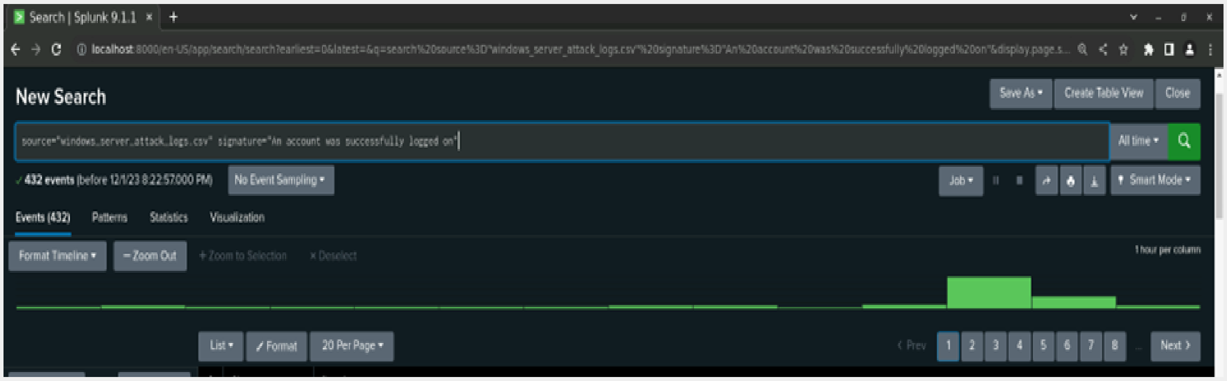
Successful login in the Windows Server Log Monitoring:



Accounts Successfully Logged On

```
source="windows_server_logs.csv" signature="An account was successfully logged on"
```

✓ 323 events (before 12/1/23 2:43:43.000 AM)



New Search

```
source="windows_server_attack_logs.csv" signature="An account was successfully logged on"
```

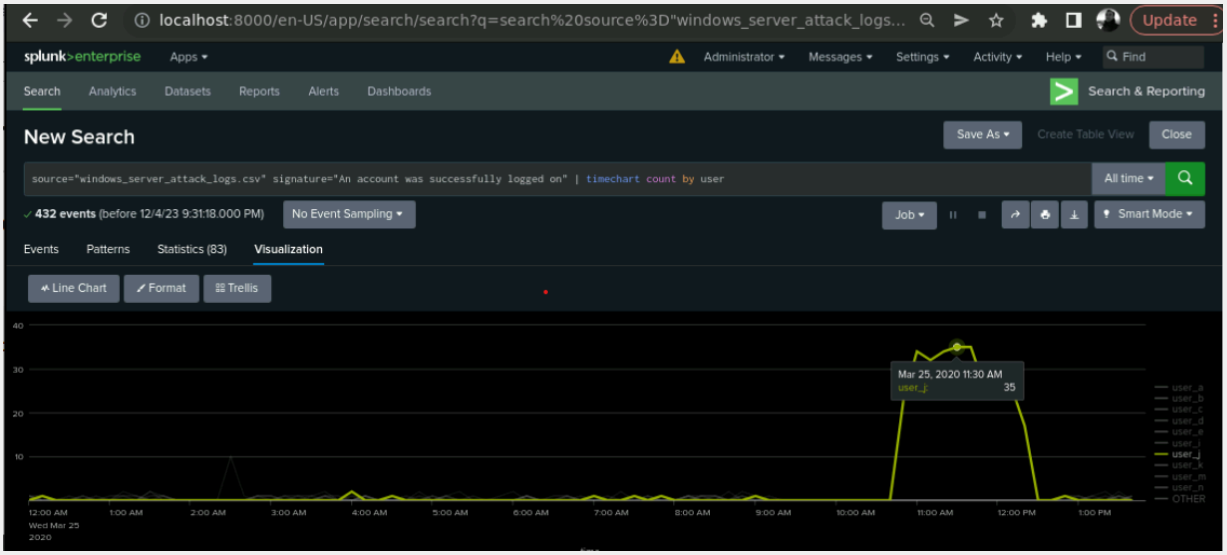
✓ 432 events (before 12/1/23 8:22:57.000 PM)

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

```
➢ 196 events at 11:00am.
➢ 77 events at 12:00pm.
```

- Who is the primary user logging in?

The primary user logging in is "**user_j**".
Screenshot of user activity for windows attack logs:



New Search

```
source="windows_server_attack_logs.csv" signature="An account was successfully logged on" | timechart count by user
```

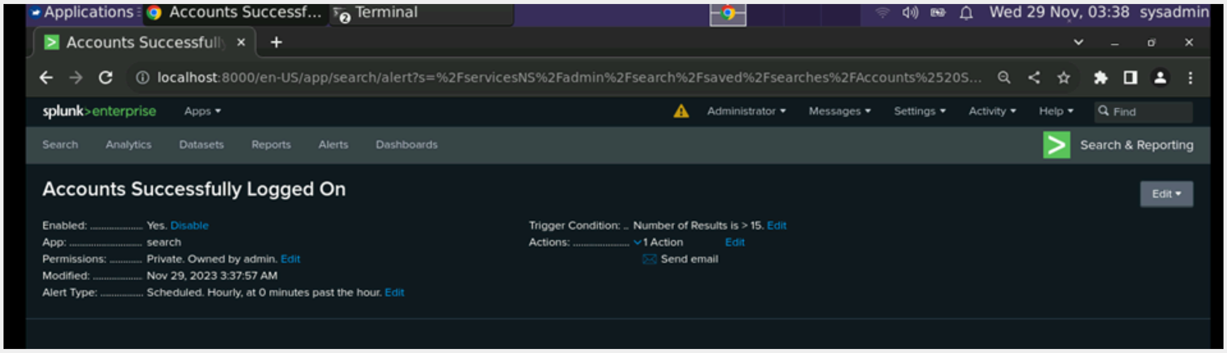
✓ 432 events (before 12/4/23 9:31:18.000 PM)

- When did it occur?

```
It occurred on 25th March 2020 in the hours of 11:00:49 am and 12:50:51 pm.
```

- Would your alert be triggered for this activity?

```
Obviously, the events are greater than the hourly threshold of 15 events.
```



Accounts Successfully Logged On

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Nov 29, 2023 3:37:57 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 15. Edit
Actions: .... 1 Action Edit
Send email

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

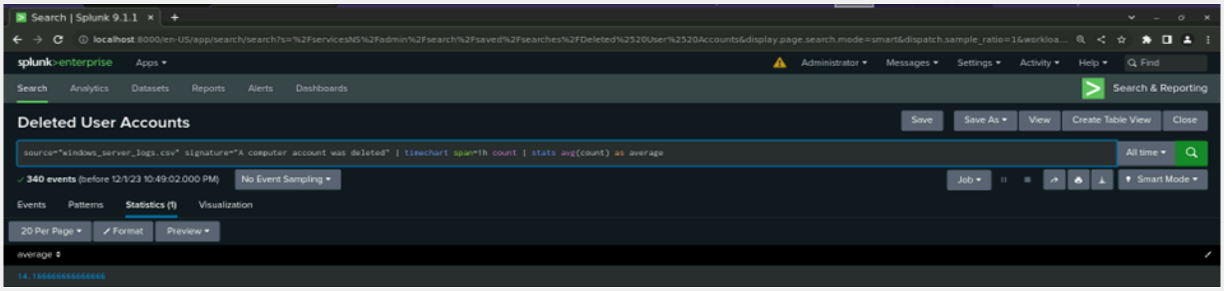
No changes seem necessary to the threshold when considering the provided data. The maximum count of successful logins by the primary user within an hour is less than the current threshold, indicating the threshold is appropriate.

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

No unusual surge in deleted accounts is evident. The average count of events in server logs - 14 exceeds that in attack logs - 10. Notably, from 10:00 am to 12:00 pm, there was zero - 0 deleted account activity, coinciding with a spike in successful log-ons.

Screenshot of deleted account activity for windows server logs:

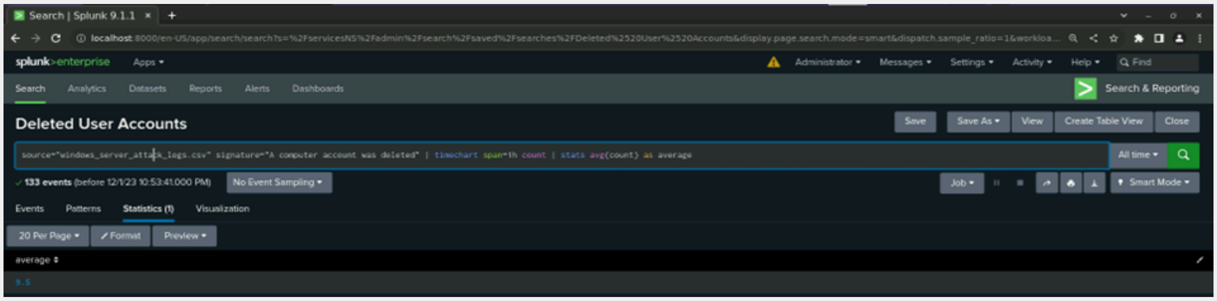


Deleted User Accounts

```
source="windows_server_logs.csv" signature="A computer account was deleted" | timechart span=1h count | stats avg(count) as average
```

✓ 340 events (before 12/1/23 10:49:02.000 PM)

average
14.166666666666666



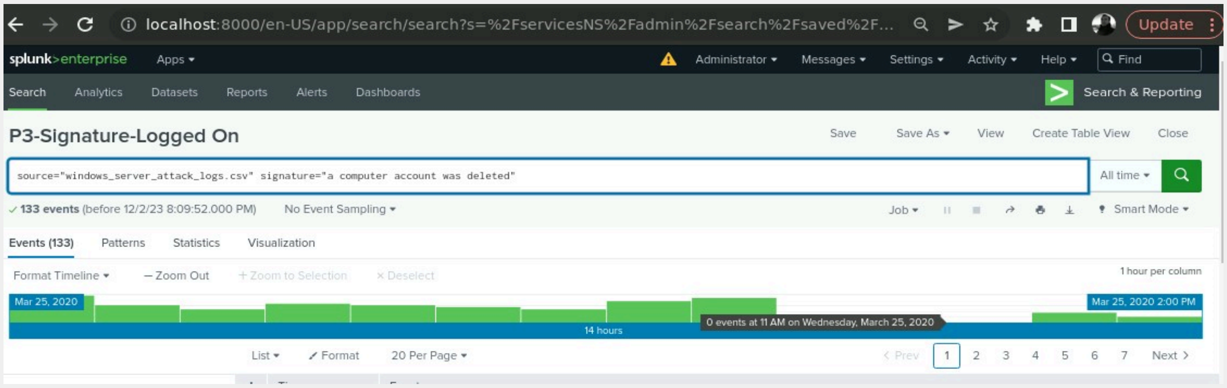
Deleted User Accounts

```
source="windows_server_attack_logs.csv" signature="A computer account was deleted" | timechart span=1h count | stats avg(count) as average
```

✓ 133 events (before 12/1/23 10:53:41.000 PM)

average
9.5

Screenshot of deleted account activity for windows server attack logs:



```
source="windows_server_attack_logs.csv" signature="a computer account was deleted"
```

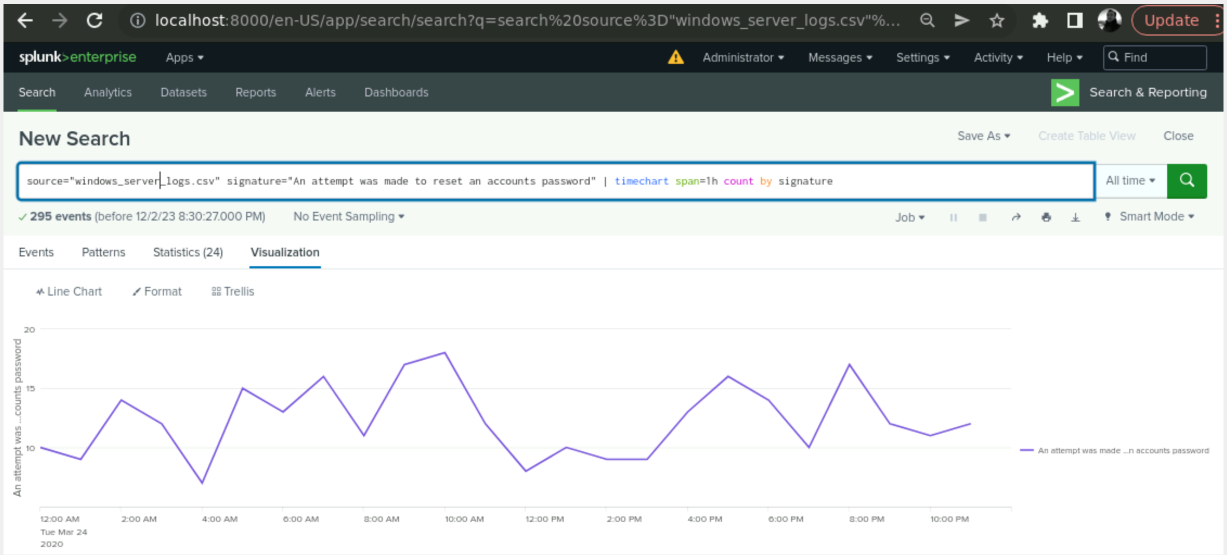
✓ 133 events (before 12/2/23 8:09:52.000 PM) No Event Sampling

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

Two suspicious signatures stand out: "**attempt to reset account password**" and "**user account locked out**". Counts for these signatures are notably higher than in the previous log.

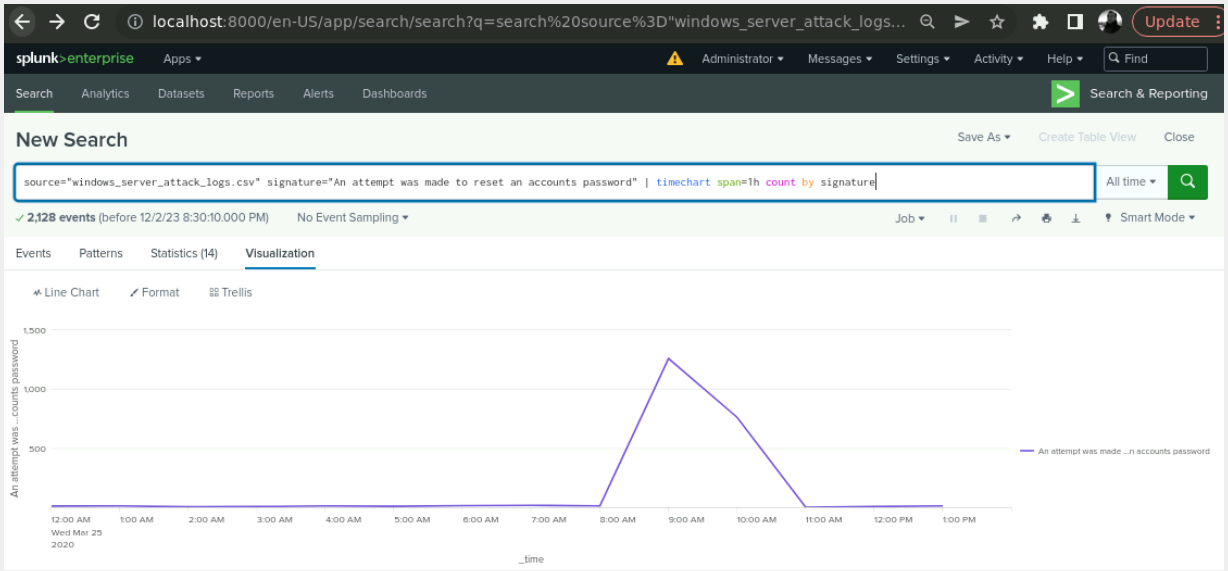
Screenshot of signature=“**An attempt was made to reset an account password**” on 03/24/2020.



```
source="windows_server_logs.csv" signature="An attempt was made to reset an accounts password" | timechart span=1h count by signature
```

✓ 295 events (before 12/2/23 8:30:27.000 PM) No Event Sampling

Screenshot of signature=“An attempt was made to reset an account password” on 03/25/2020.



localhost:8000/en-US/app/search/search?q=search%20source%3D"windows_server_attack_logs...

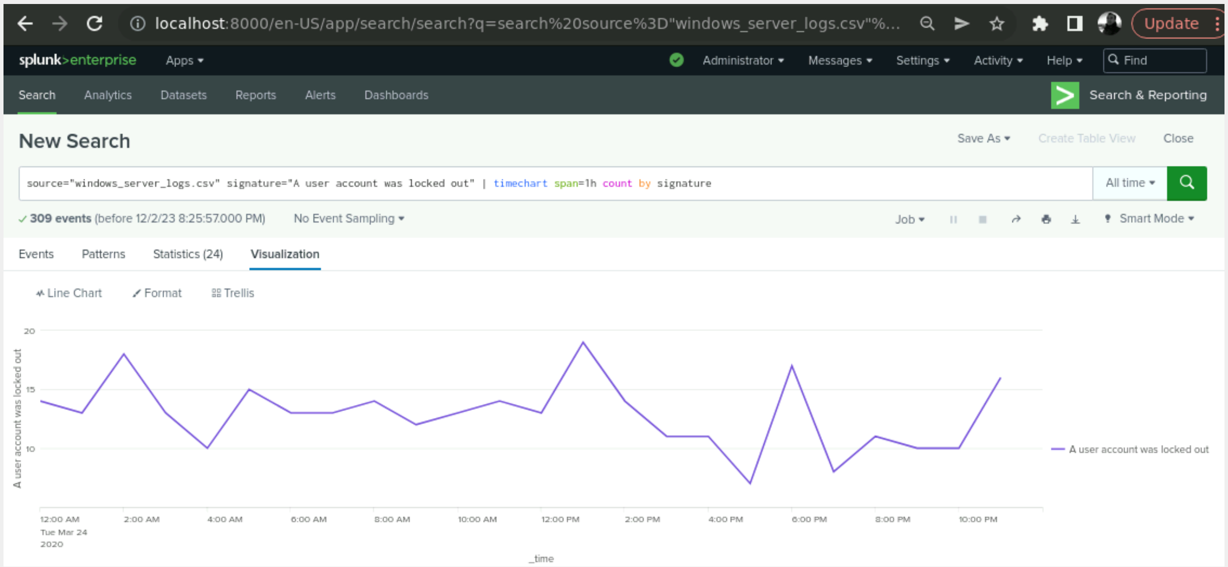
New Search

```
source="windows_server_attack_logs.csv" signature="An attempt was made to reset an accounts password" | timechart span=1h count by signature
```

All time

✓ 2,128 events (before 12/2/23 8:30:10.000 PM) No Event Sampling

Screenshot of signature=“A user account was locked out” on 03/24/2020.



localhost:8000/en-US/app/search/search?q=search%20source%3D"windows_server_logs.csv"%...

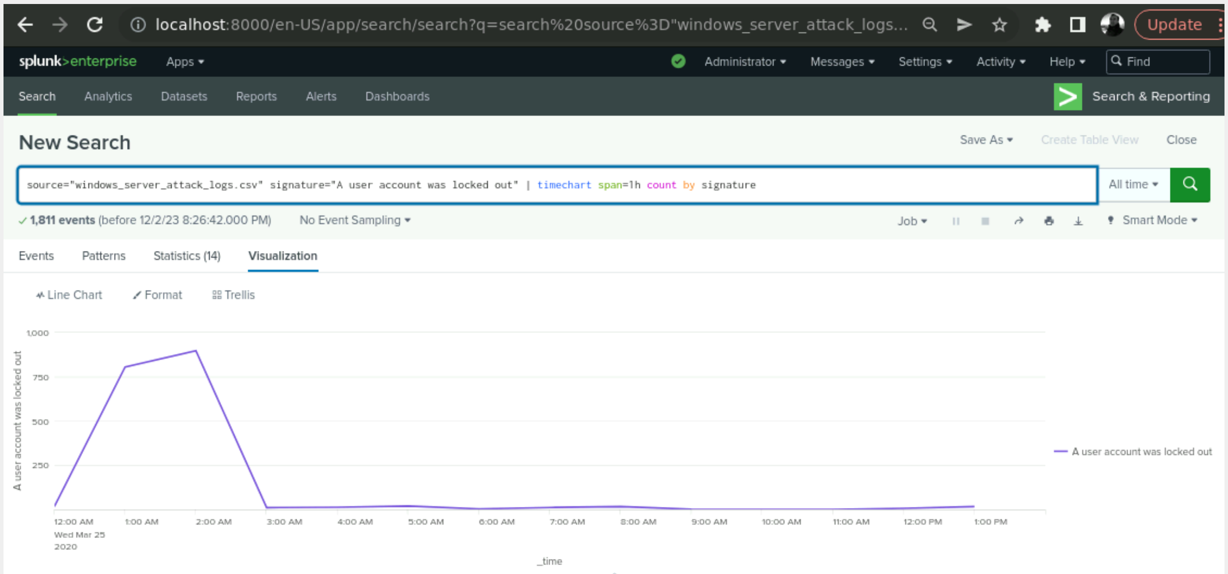
New Search

```
source="windows_server_logs.csv" signature="A user account was locked out" | timechart span=1h count by signature
```

All time

✓ 309 events (before 12/2/23 8:25:57.000 PM) No Event Sampling

Screenshot of signature=“A user account was locked out” on 03/25/2020.



```
source="windows_server_attack_logs.csv" signature="A user account was locked out" | timechart span=1h count by signature
```

✓ 1,811 events (before 12/2/23 8:26:42.000 PM)

- What signatures stand out?

> ➢ A user account was locked out.
> ➢ An attempt was made to reset an account's password.

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

> ➢ The "**user account locked out**" was observed from 1:49:54 am and stopped at 2:54:47 am on March 25, 2020.
> ➢ The "**attempt to reset account password**" happened from 9:32:38 am to 10:54:24 am.on the same day.
> ➢ The "**account successfully logged in**" was noted from 11:00:49 am to 12:50:51 pm on the same day totaling 273 events.

- What is the peak count of the different signatures?

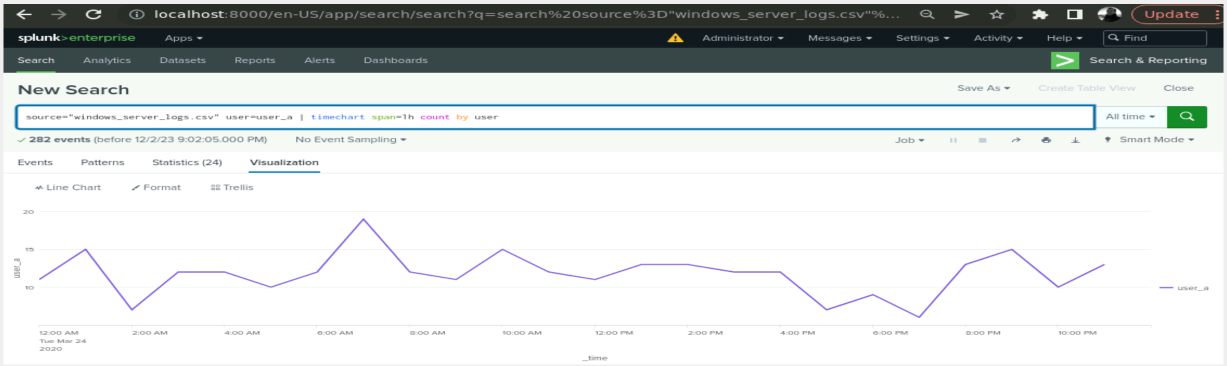
For "**user account locked out**," the highest count was 896, for "**attempt to reset account password**" it was 1,258, and for "account successfully logged in" it was 273.

Dashboard Analysis for Users

- Does anything stand out as suspicious?

Yes, **user_a** and **user_k** are flagged as suspicious on Mar 25, 2023 due to their high peak counts in the line graph.

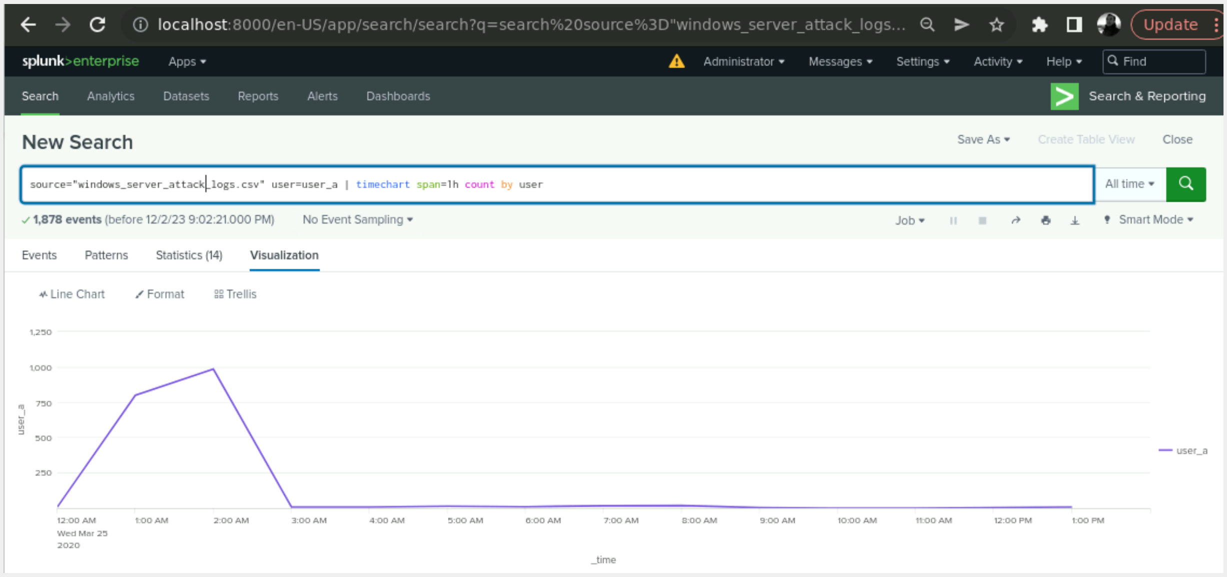
Screenshot of **user_a** activity on 03/24/2020



```
source="windows_server_logs.csv" user=user_a | timechart span=1h count by user
```

✓ 282 events (before 12/2/23 9:02:05.000 PM)

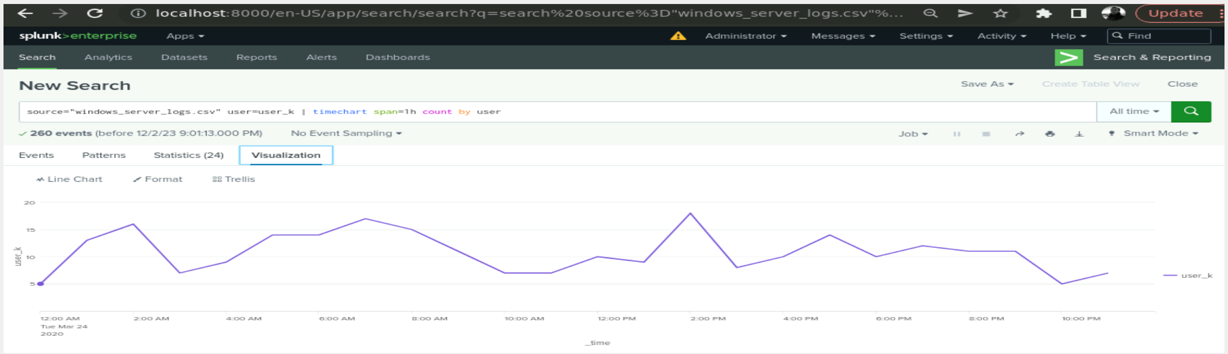
Screenshot of user_a activity on 03/25/2020.



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

✓ 1,878 events (before 12/2/23 9:02:21.000 PM)

Screenshot of **user_k** activity on 03/24/2020.



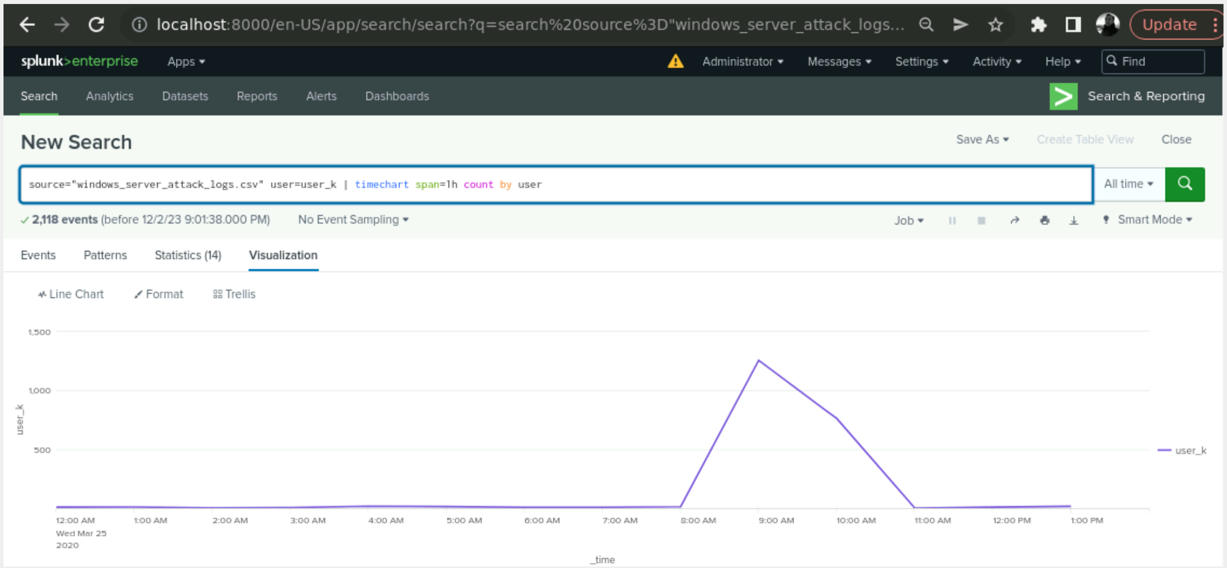
localhost:8000/en-US/app/search/search?q=search%20source%3D"windows_server_logs.csv"%...

New Search

```
source="windows_server_logs.csv" user=user_k | timechart span=1h count by user
```

✓ 260 events (before 12/2/23 9:01:13.000 PM) No Event Sampling

Screenshot of user_k activity on 03/24/2020.



localhost:8000/en-US/app/search/search?q=search%20source%3D"windows_server_attack_logs...

New Search

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

✓ 2,118 events (before 12/2/23 9:01:38.000 PM) No Event Sampling

- Which users stand out?

The “**user_a**” and “**user_k**” are outstanding users.

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

The **user_a**'s activity occurred between 1:12:06 am and 2:55:56 am on the same day. The **user_k** was engaged in activity from 9:32:38 am to 10:54:24 am on the same day.

- What is the peak count of the different users?

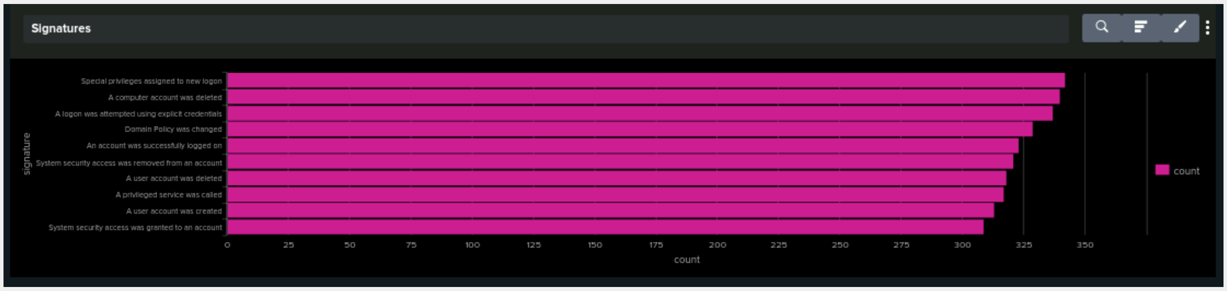
The peak count for **user_a** was 984, and for **user_k**, it was 1,256.

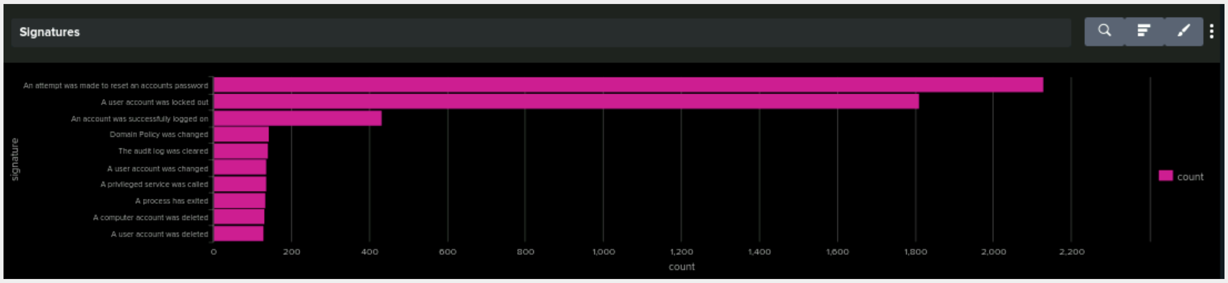
Dashboard Analysis for Signatures with Bar, Graph, and Pie Charts

- Does anything stand out as suspicious?

The three signatures "**user was locked out**," "**account successfully logged on**," and "**attempt made to reset account password**" are noteworthy for their high counts, raising suspicion.

Screenshot for signature volume activity on Mar 24, 2020.





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

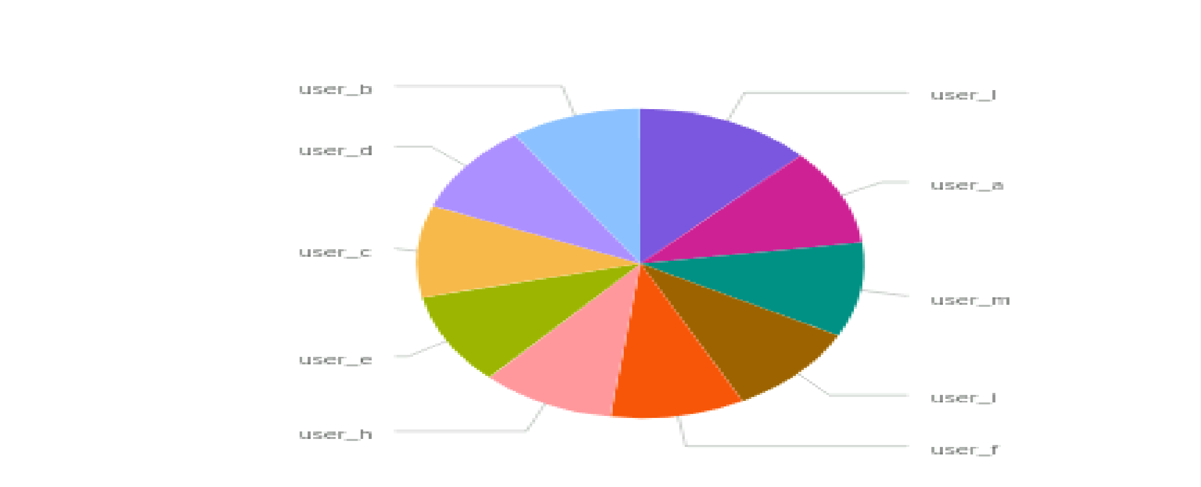
Yes, the results from the bar chart seem to match the findings from the time chart.

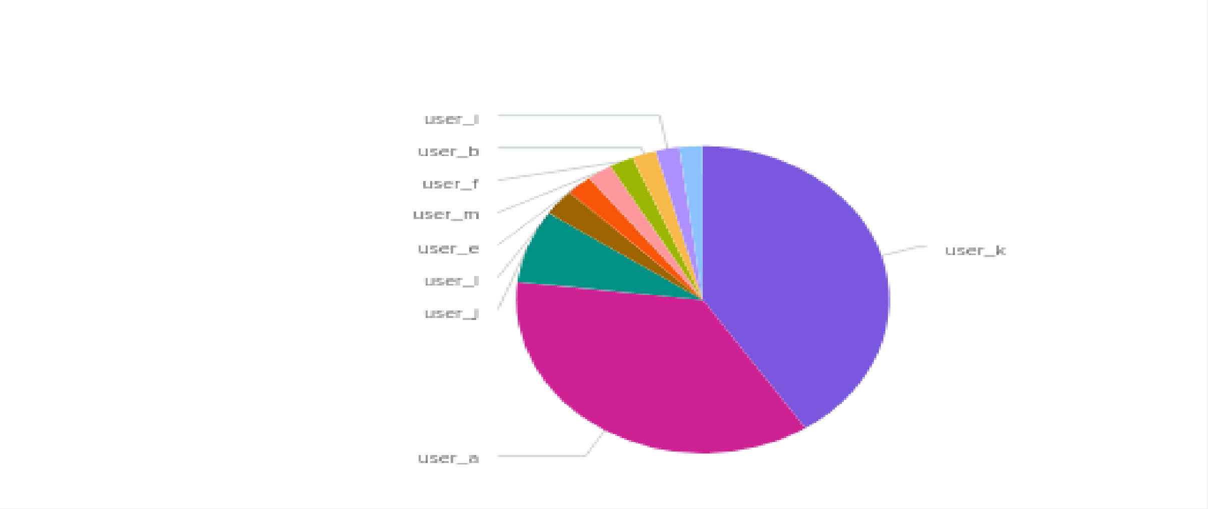
Dashboard Analysis for Users with Bar, Graph, and Pie Charts

- Does anything stand out as suspicious?

The two users, the **user_a** and **user_k** are flagged as suspicious, evident from their high counts and significant proportions in the pie chart.

Screenshot:





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

Yes, the results from the pie chart seem to match the findings from the time chart.

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?

Advantages:

- ➢ **Comprehensive Insights:** Statistical charts provide a comprehensive view of user activities, enhancing our understanding of the data.
- ➢ **Spotting Anomalies:** Charts help identify outliers or anomalies by highlighting deviations from normal statistical patterns.
- ➢ **In-Depth Comparison:** These charts help compare user behavior in detail, showing distributions, averages, and other statistical measures not seen in other chart styles.

Disadvantages:

- ➢ **Understanding Challenge:** Unfamiliar people with statistics may struggle to interpret statistical charts.
- ➢ **Beyond Time Frames:** Statistical charts, unlike line graphs, lack a time frame, making it challenging to grasp the progression of user behavior over time.
- ➢ **Navigating Visual Interpretation Challenges:** Understanding these charts visually may be tougher than interpreting the direct comparisons presented by pie charts or bar graphs.

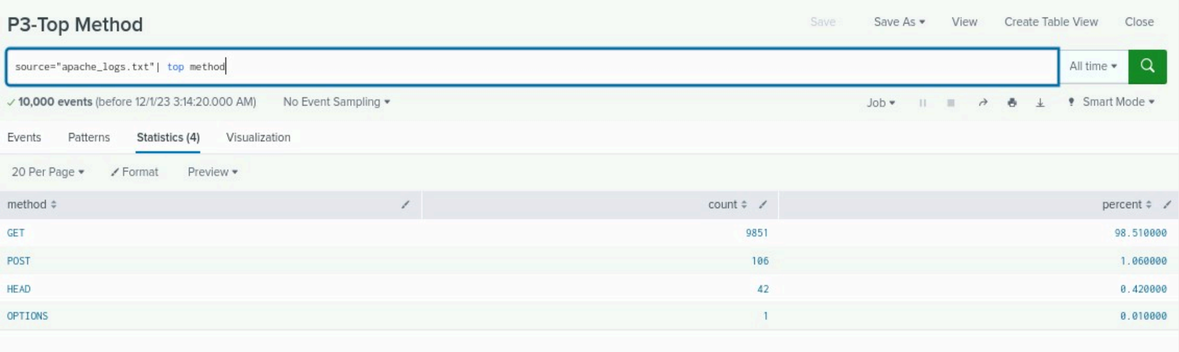
Apache Web Server Log Questions

Report Analysis for Methods

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

Shift in HTTP Behavior: A suspicious change is observed in the behavior of HTTP methods. The significant decrease in GET requests and the dramatic increase in POST requests occurred after the attack.

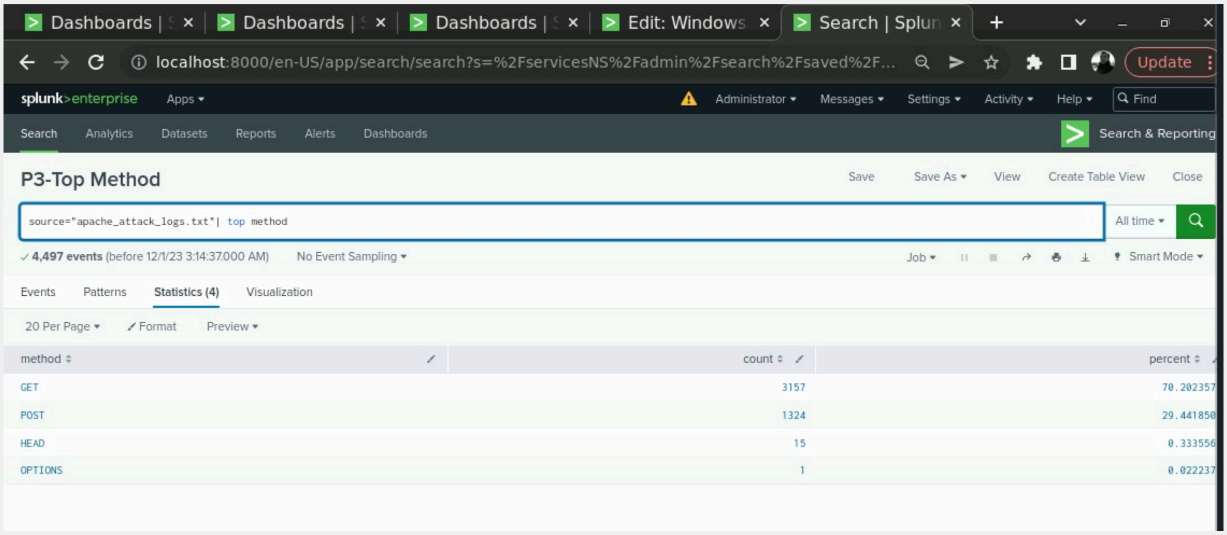
Screenshot of Method activity:



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

✓ 10,000 events (before 12/1/23 3:14:20.000 AM)

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



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

✓ 4,497 events (before 12/1/23 3:14:37.000 AM)

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?

GET, as a method in HTTP, is utilized for requesting data from a specific resource. Its main function is to fetch information from the server without any other side effects.

POST, as a method in HTTP, is utilized to send data to a server, intending to create or update a resource. The data is embedded in the request's body, and this can lead to the creation of a new resource, updates to existing ones, or both.

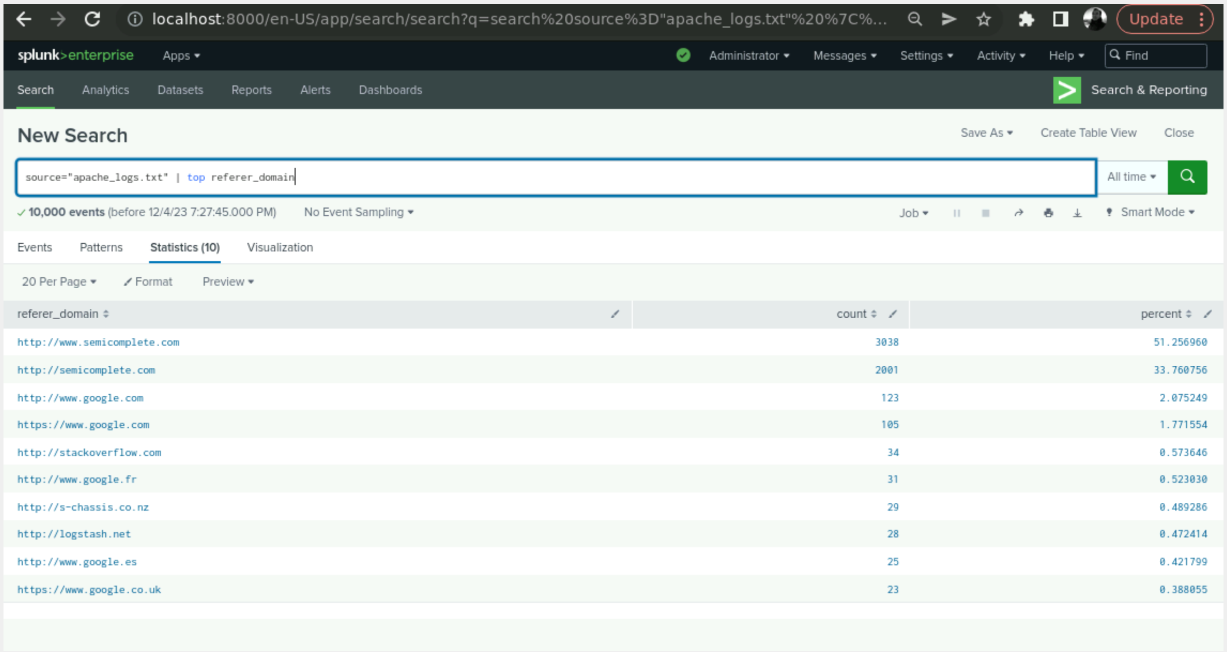
Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

No suspicious changes noted in the activities on those two days.

Despite a decrease from 10,000 events on 03/24/2020 to 4,497 on 03/25/2020, the order and percentage of the top five domains remain very similar. The decline in domain activity, possibly due to authentication issues, does not suggest a potential DNS brute force attack based on the observed information in the search.

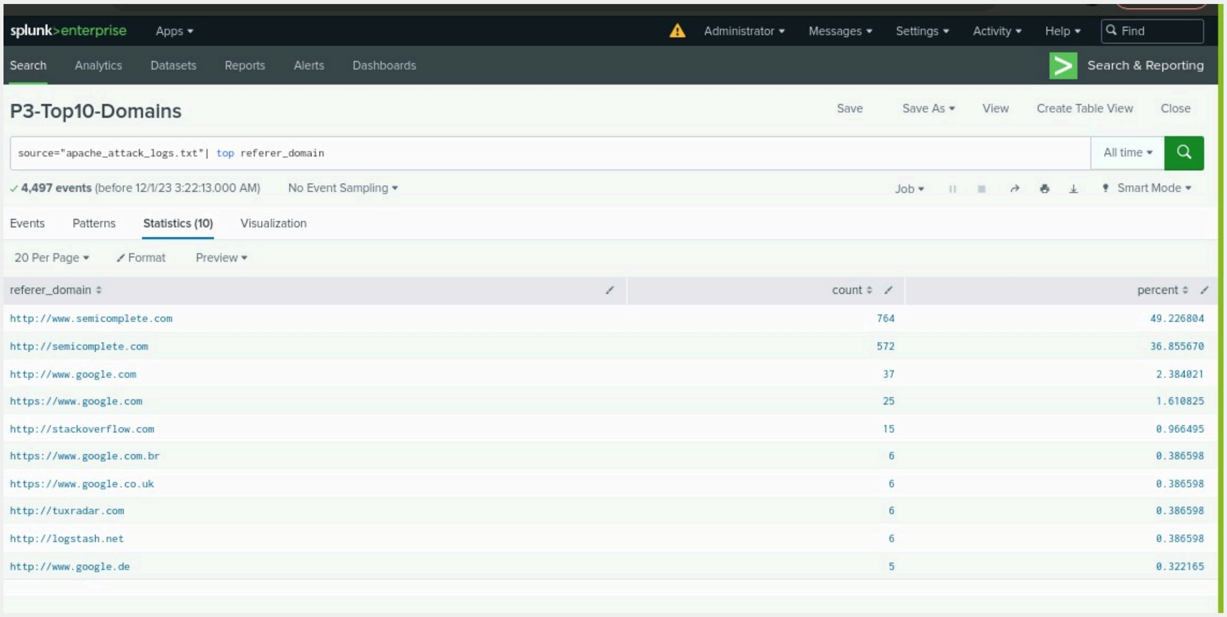
Screenshot of referrer domain for apache logs:



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

✓ 10,000 events (before 12/4/23 7:27:45.000 PM)

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



P3-Top10-Domains

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

✓ 4,497 events (before 12/1/23 3:22:13.000 AM) No Event Sampling

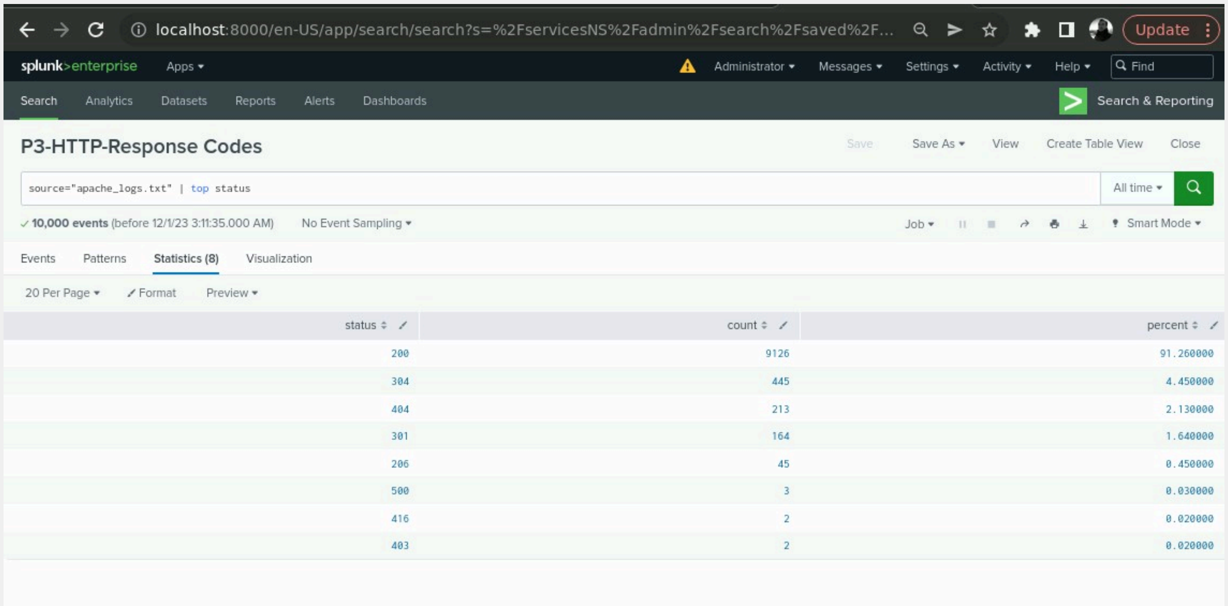
referer_domain	count	percent
http://www.semicomplete.com	764	49.226804
http://semicomplete.com	572	36.855670
http://www.google.com	37	2.384021
https://www.google.com	25	1.610825
http://stackoverflow.com	15	0.966495
https://www.google.com.br	6	0.386598
https://www.google.co.uk	6	0.386598
http://tuxradar.com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

```
Suspicious changes in HTTP response codes are evident. Successful responses
(200 - OK) decreased significantly from 91.2% to 83.3%. Meanwhile, client
error responses (404 - Not Found) sharply increased from 2.1% to 15.1% after
the attack on 03/25/2020, suggesting possible attempts to identify
vulnerabilities or misconfigurations by making requests for non-existent
resources.

The attacker may be aiming to gain access by executing numerous requests
within a specific timeframe on 03/25/2020.
```

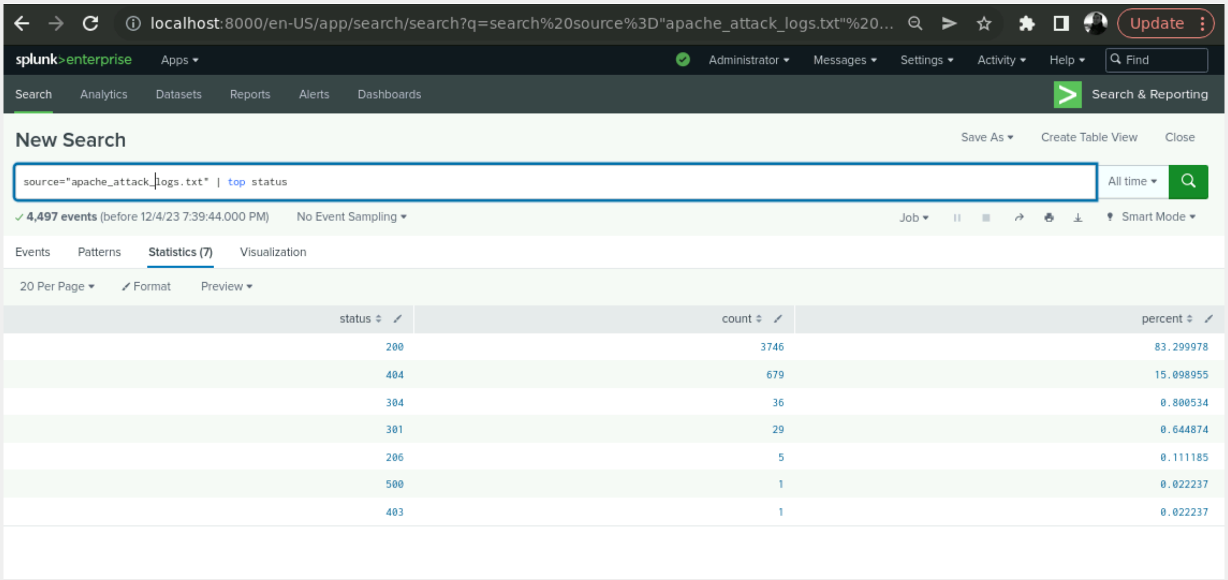


P3-HTTP-Response Codes

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

✓ 10,000 events (before 12/1/23 3:11:35.000 AM)

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 12/4/23 7:39:44.000 PM)

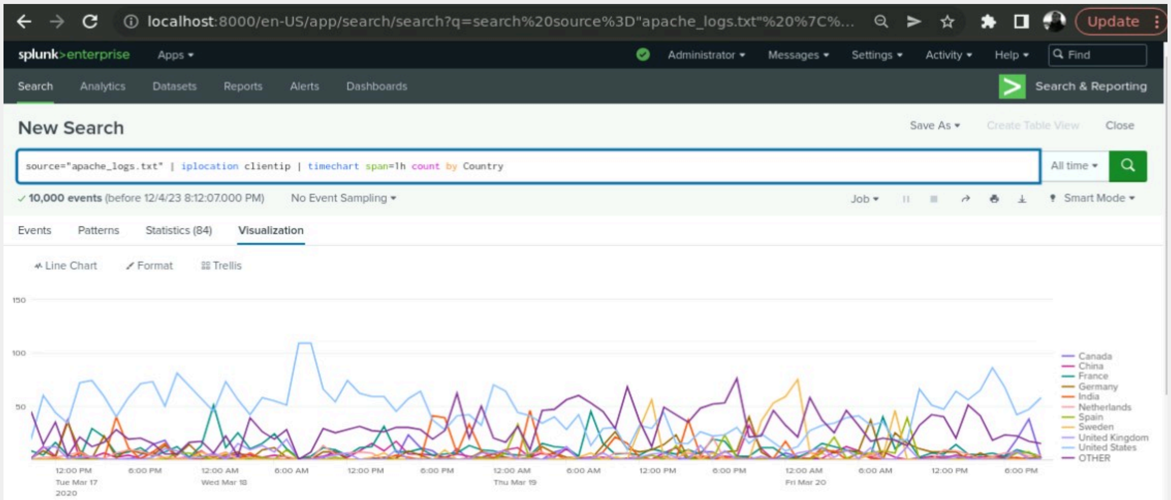
status	count	percent
200	3746	83.299978
404	679	15.098955
304	36	0.800534
301	29	0.644874
206	5	0.111185
500	1	0.022237
403	1	0.022237

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

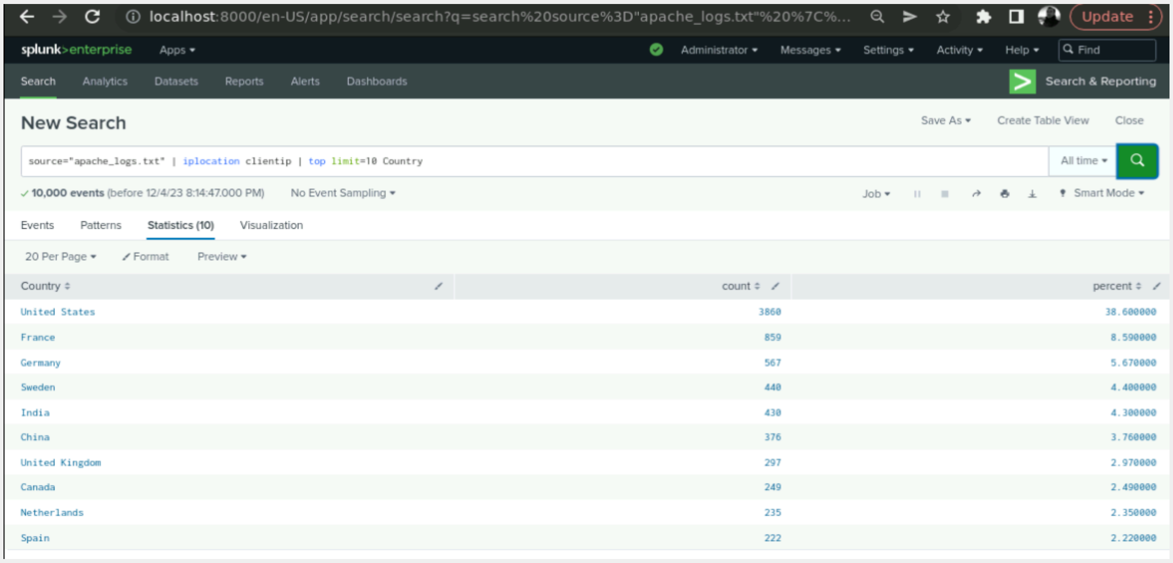
There's a lot of strange anomalous high activity happening internationally in **Ukraine**. At 8:05:59 PM on March 25, 2020, the number of events 864 is much higher than any other time, in both the regular and attack logs.

Screenshot of International Attack activity:



```
source="apache_logs.txt" | iplocation clientip | timechart span=1h count by Country
```

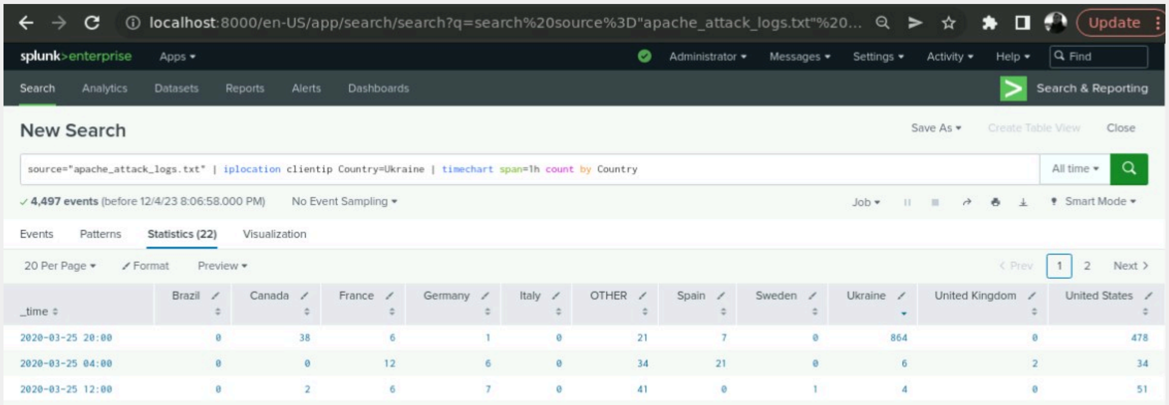
✓ 10,000 events (before 12/4/23 8:12:07.000 PM)   No Event Sampling ▾



```
source="apache_logs.txt" | iplocation clientip | top limit=10 Country
```

✓ 10,000 events (before 12/4/23 8:14:47.000 PM)   No Event Sampling ▾

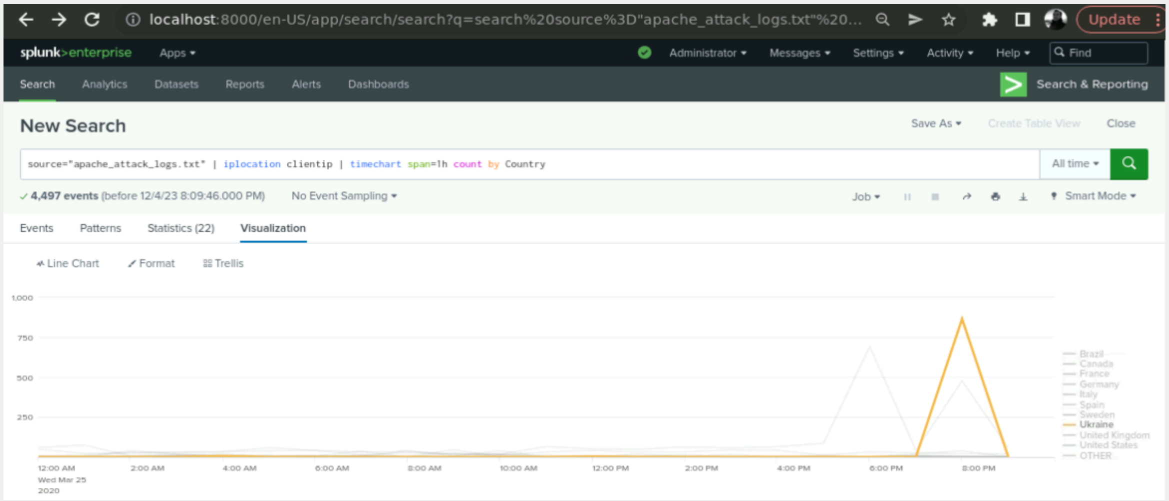
Country	count	percent
United States	3860	38.600000
France	859	8.590000
Germany	567	5.670000
Sweden	440	4.400000
India	430	4.300000
China	376	3.760000
United Kingdom	297	2.970000
Canada	249	2.490000
Netherlands	235	2.350000
Spain	222	2.220000



```
source="apache_attack_logs.txt" | iplocation clientip Country=Ukraine | timechart span=1h count by Country
```

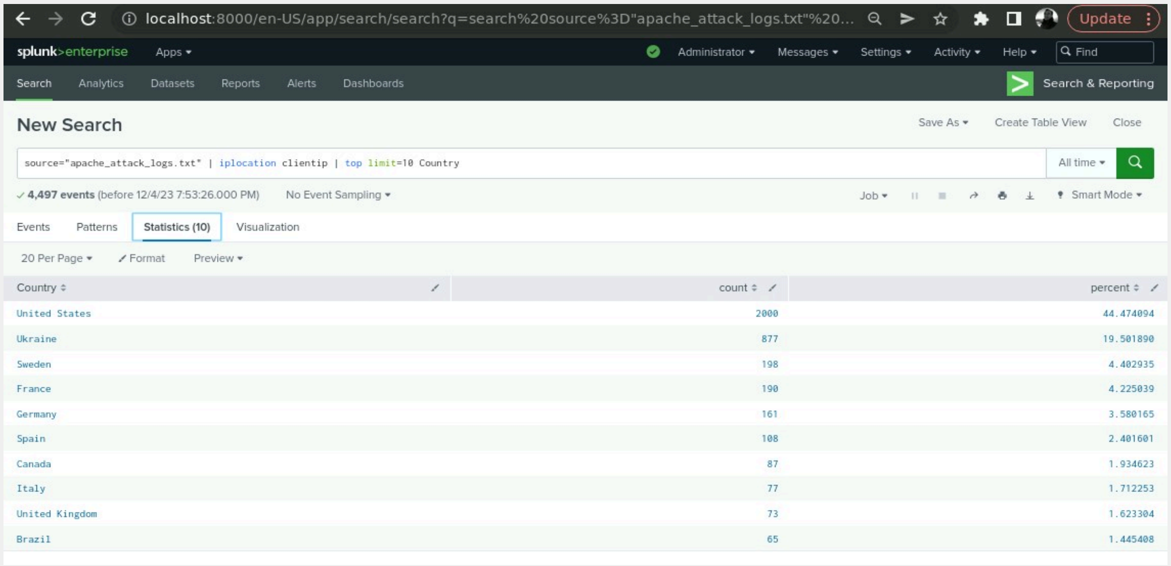
✓ 4,497 events (before 12/4/23 8:06:58.000 PM)   No Event Sampling ▾

_time	Brazil	Canada	France	Germany	Italy	OTHER	Spain	Sweden	Ukraine	United Kingdom	United States
2020-03-25 20:00	0	38	6	1	0	21	7	0	864	0	478
2020-03-25 04:00	0	0	12	6	0	34	21	0	6	2	34
2020-03-25 12:00	0	2	6	7	0	41	0	1	4	0	51



```
source="apache_attack_logs.txt" | iplocation clientip | timechart span=1h count by Country
```

✓ 4,497 events (before 12/4/23 8:09:46.000 PM) No Event Sampling



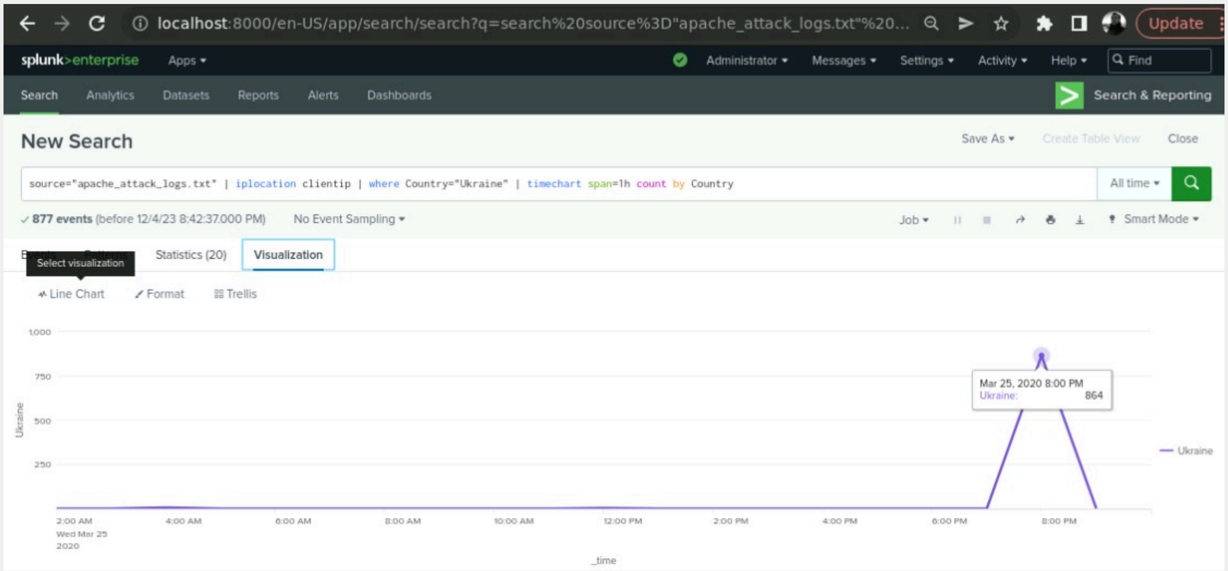
```
source="apache_attack_logs.txt" | iplocation clientip | top limit=10 Country
```

✓ 4,497 events (before 12/4/23 7:53:26.000 PM) No Event Sampling

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?

```
On March 25, 2020, at 8:05:59 PM, there were 864 events, significantly more
than any other hour.
```



localhost:8000/en-US/app/search/search?q=search%20source%3D"apache_attack_logs.txt"%20...

New Search

```
source="apache_attack_logs.txt" | iplocation clientip | where Country="Ukraine" | timechart span=1h count by Country
```

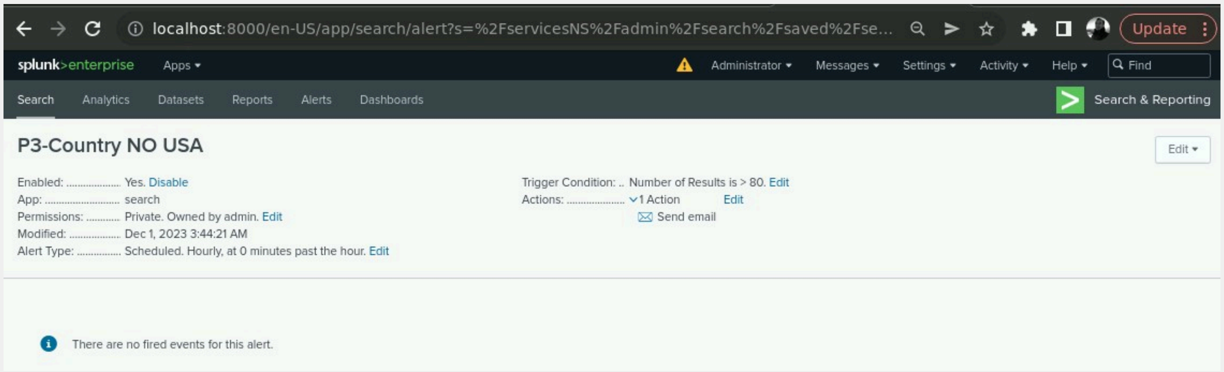
✓ 877 events (before 12/4/23 8:42:37.000 PM) No Event Sampling ▾

Mar 25, 2020 8:00 PM
Ukraine: 864

- Would your alert be triggered for this activity?

Yes, an alert would be triggered because this activity surpasses my threshold of 80, with a count found for Ukrainian activity was 864 counts.

Screenshot of threshold alert:



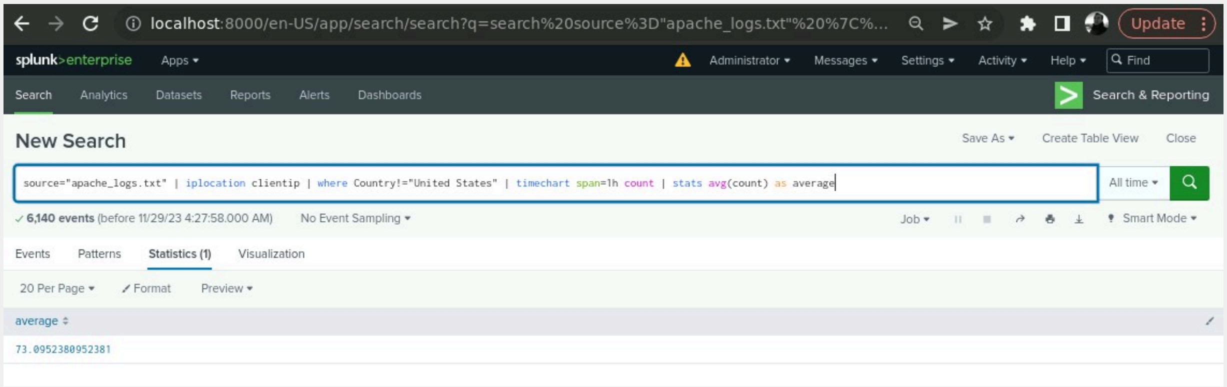
localhost:8000/en-US/app/search/alert?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2Fse...

P3-Country NO USA

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Dec 1, 2023 3:44:21 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 80. Edit
Actions: .... 1 Action Edit
Send email

There are no fired events for this alert.



```
source="apache_logs.txt" | iplocation clientip | where Country!="United States" | timechart span=1h count | stats avg(count) as average
```

✓ 6,140 events (before 11/29/23 4:27:58.000 AM) No Event Sampling

average
73.0952380952381

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

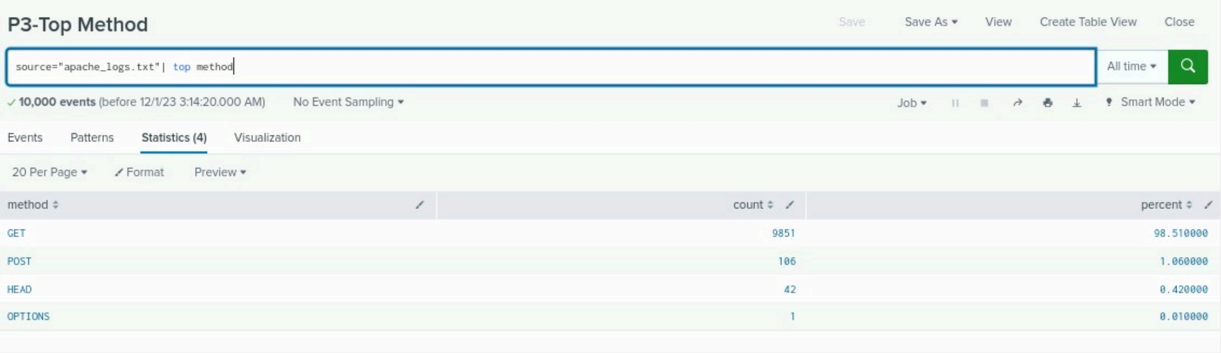
```
No change of threshold is needed after reviewing!
```

Alert Analysis for HTTP POST Activity

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

Yes, the level of HTTP **POST** activity is raising eyebrows. At 8:05:59 PM on March 25, 2020, the count of HTTP **POST** requests is much higher than during any other hour.The HTTP **POST** activity increased in percentage from 1% on 03/24/2020 to 29.4% on 03/25/2020.

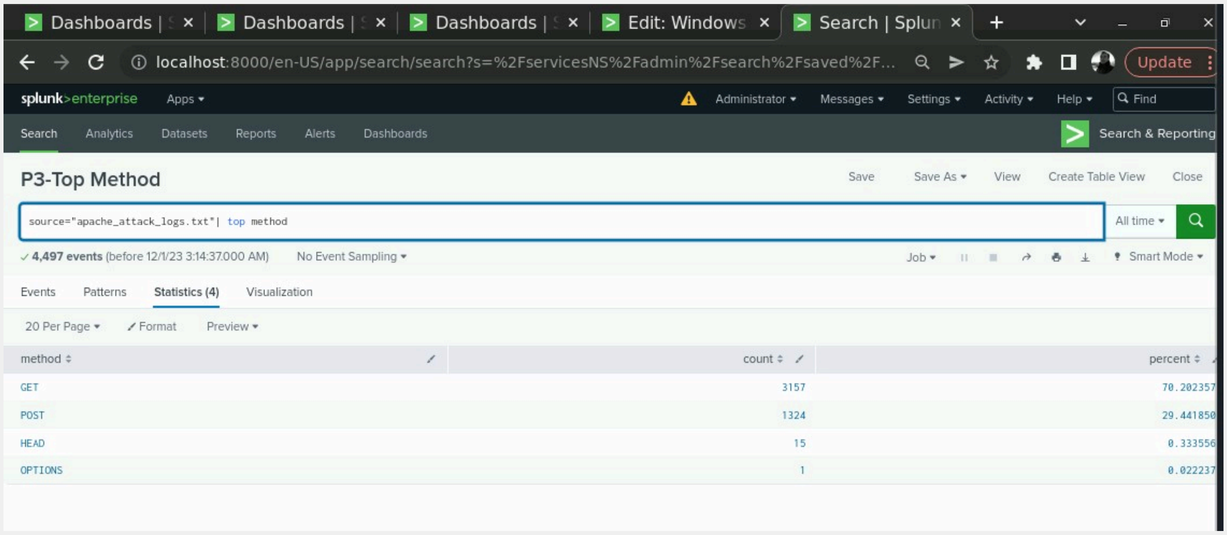
Screenshots



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

✓ 10,000 events (before 12/1/23 3:14:20.000 AM) No Event Sampling

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



P3-Top Method

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

✓ 4,497 events (before 12/1/23 3:14:37.000 AM)

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

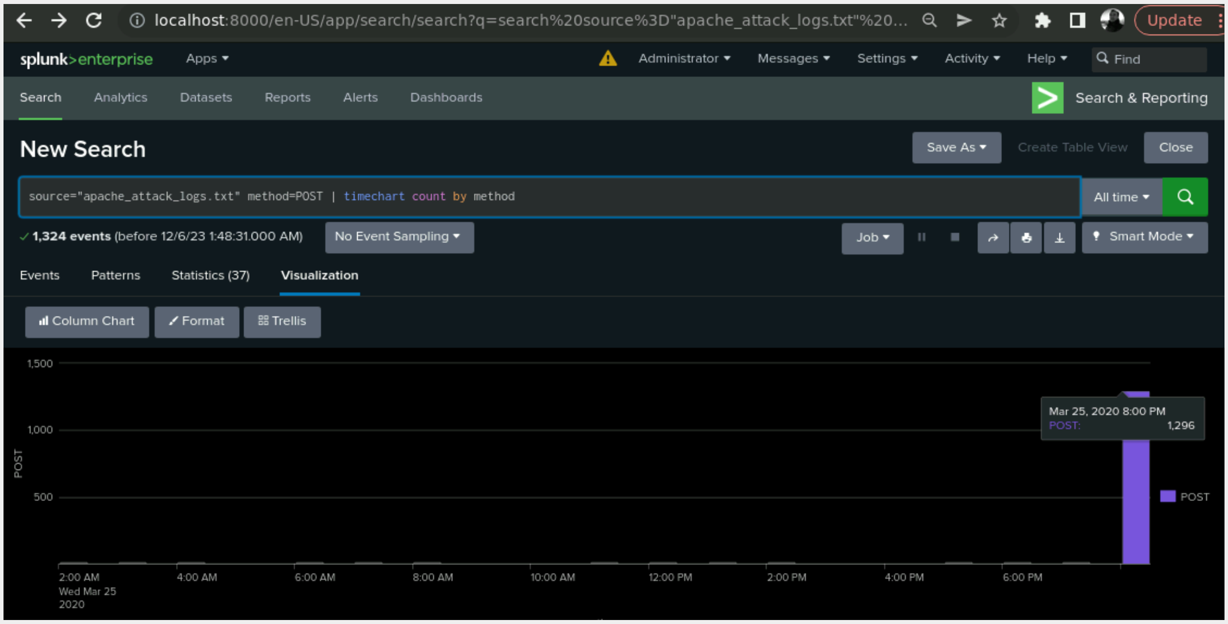
- If so, what was the count of the hour(s) it occurred in?

On March 25, 2020, at 8:05:59 PM, there were 1,296 events, significantly more than any other hour.

Deeper analysis revealed a concentration of increased HTTP **POST** method activity, all occurring at 08:05:59 pm in the web app **VSI_Account_logon.php**.

This pattern suggests a potential brute force attack aimed at gaining system access. The consistency in the attack timing indicates a possible netbot involvement, and the intensity of this brute force attack could lead to a denial-of-service (DDoS) scenario, impacting server availability.

HTTP POST Screenshot



```
source="apache_attack_logs.txt" method=POST | timechart count by method
```

✓ 1,324 events (before 12/6/23 1:48:31.000 AM)

- When did it occur?

The odd amount of HTTP **POST** activity happened at 8:05:59 PM on March 25, 2020.

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

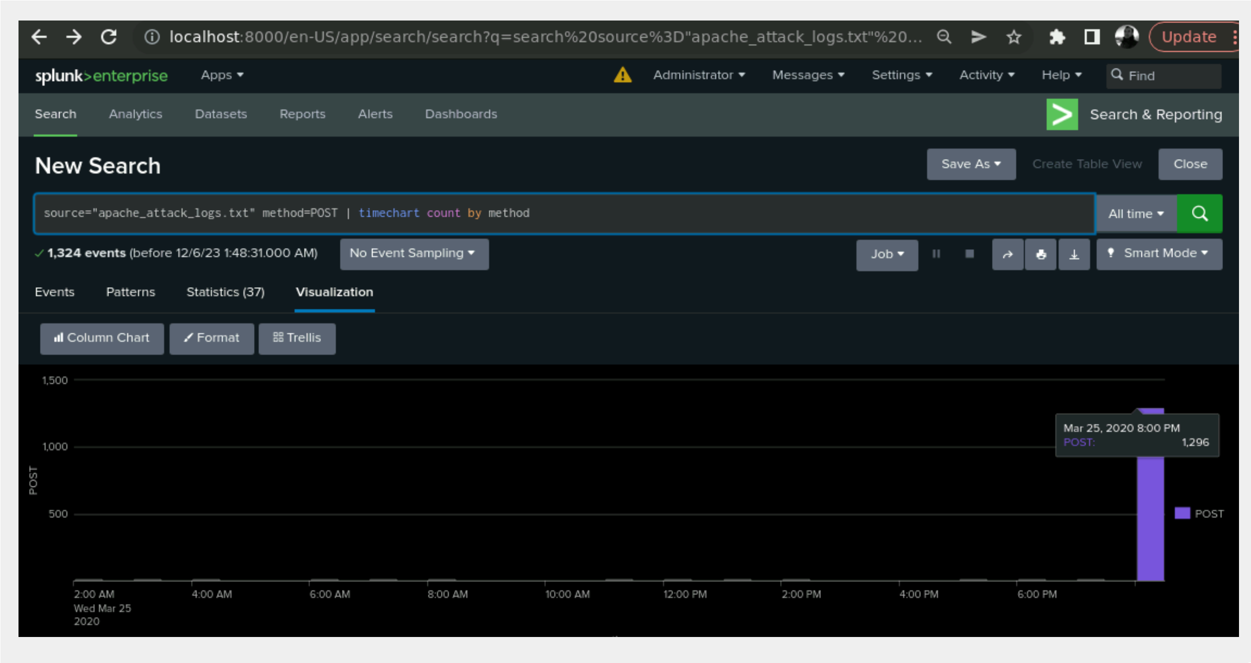
Yes,considering the suspicious activity, it might raise the threshold. The current limit of 10 was far surpassed during this event. Yet, the new threshold should be set to catch smaller, yet possibly important, rises in HTTP **POST** activity.

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

Yes, the use of the HTTP **POST** method has gone up a lot during the attack.

Screenshot of the HTTP POST method :



```
source="apache_attack_logs.txt" method=POST | timechart count by method
```

✓ 1,324 events (before 12/6/23 1:48:31.000 AM)

- Which method seems to be used in the attack?

The usage of the HTTP **POST** method is apparent in the attack.

- At what times did the attack start and stop?

On March 25, 2020, the attack started at 08:05:59 pm and stopped at 08:05:59 pm.

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

During the attack, the HTTP **POST** method reached its highest count at 1,296.

Dashboard Analysis for Cluster Map

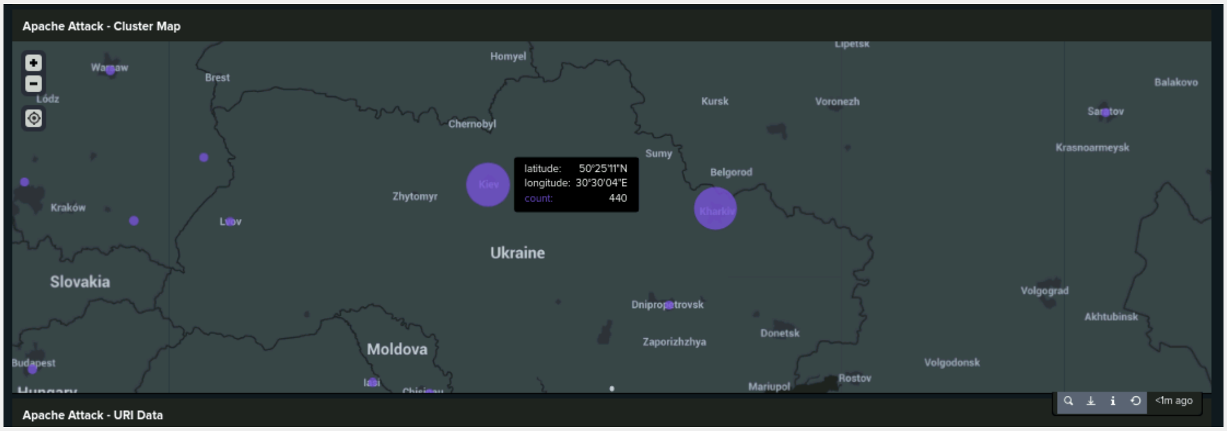
- Does anything stand out as suspicious?

Notably, besides the U.S., France exhibited relatively high activity on 03/24/2020. However, on 03/25/2020, **Ukraine** experienced a substantial increase in activity.

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

A significant amount of activity coming from Ukraine was 887, specifically from Kiev was 440 and Kharkiv was 432. They were unusually high and raised suspicion activities.

Screenshot of Cluster Map showing the zones on the map:



latitude: 50°25'11"N
longitude: 30°30'04"E
count: 440

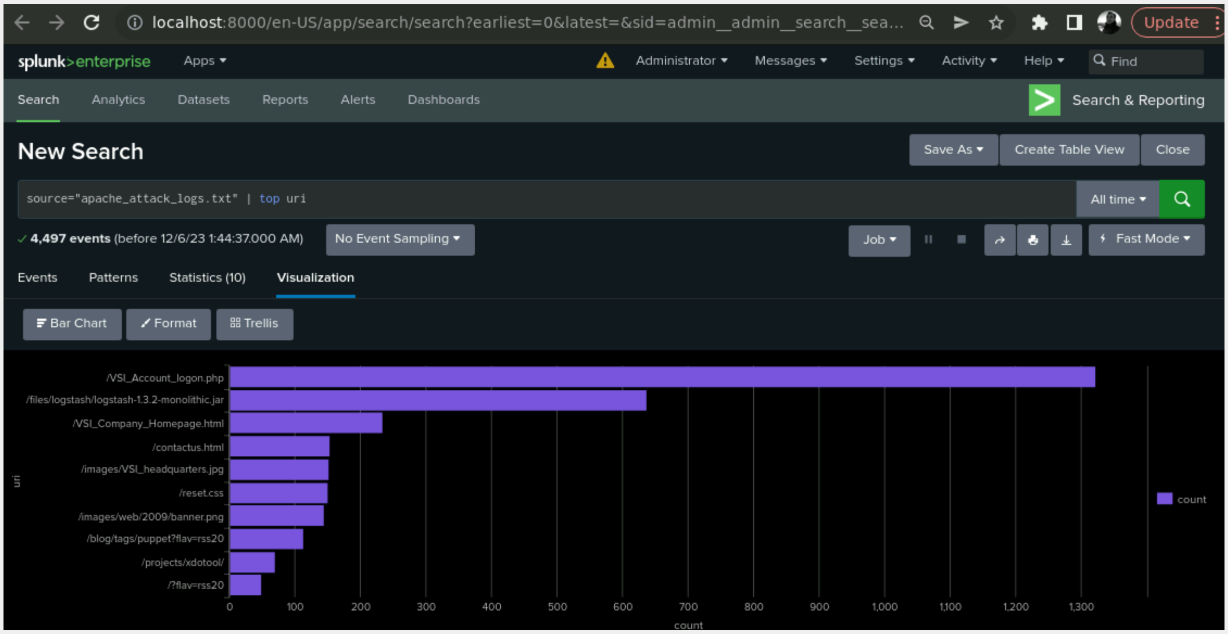
- What is the count of that city?

The count for Kiev is 440.

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

Yes, in the bar graph, the URI "**VSI_Account_logon.php**" catches attention as it has the highest 1,323 counts.



New Search

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

✓ 4,497 events (before 12/6/23 1:44:37.000 AM)

- What URI is hit the most?

The most frequently targeted URIs is "**VSI_Account_logon.php**".

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

The attacker aimed to guess account passwords, evident from the high volume of **POST** requests commonly used for authentication. This aligns with a brute-force attack, supported by various evidence. The server being down, detected by the web plug-in (Splunk Website Monitoring), and the absence of deleted accounts during the attack hour suggest a possible Denial-of-Service (DDoS) attack.

Based on the accessed URI, it's confirmed the attacker employed a netbot for a brute-force attack on the "**VSI_Account_logon.php**” webapp, potentially causing an unintentional Denial-of-Service (DDoS) due to the overwhelming netbot assault.