Cybersecurity

Project 3 Review Questions

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

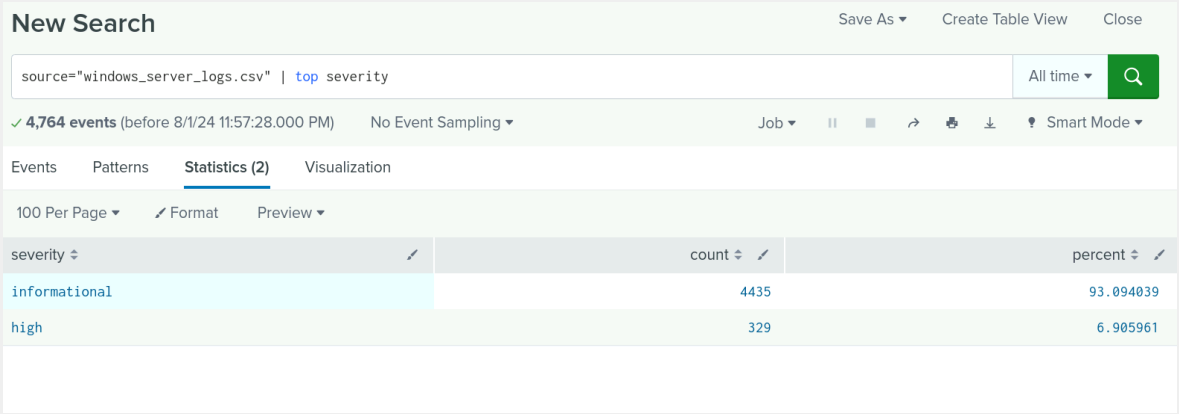
Windows Server Log Questions

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

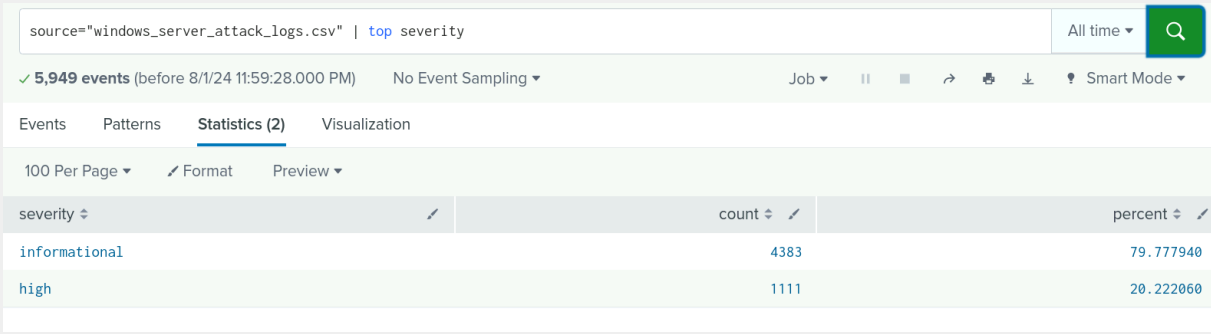
Yes. There has been a substantial rise in high-severity events, jumping from 329 to 1111 occurrences. This equates to a growth from 6.91% to 20.22% of the total severity count. A significant increase in high-severity events during the attack is a red flag indicating potential system compromise during the attack.

Windows Normal Activity Log:



severity	count	percent
informational	4435	93.094039
high	329	6.905961

Windows Attack Activity Log:



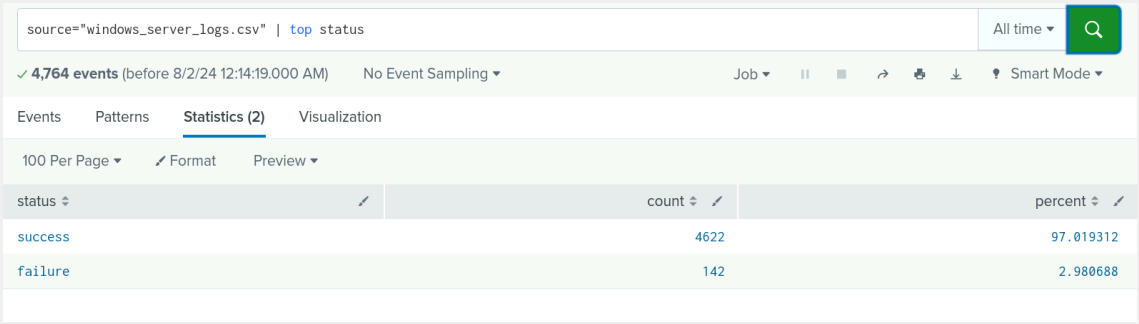
severity	count	percent
informational	4383	79.777940
high	1111	20.222060

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

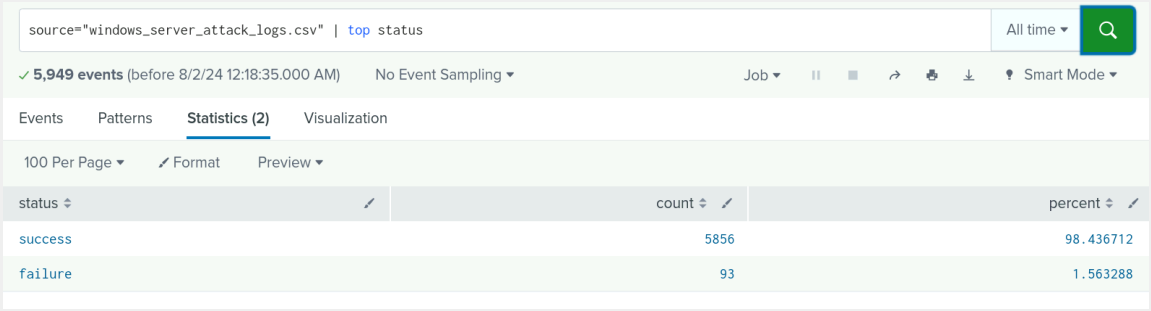
Yes. A decrease in the percentage of failed activities within the attack logs when compared to previous metrics is very suspicious (from 142 to 93 but the successes have increased from 4622 to 5856). This anomaly suggests potential unauthorized access and successful malicious actions. Further investigation is required to confirm this security breach.

Windows Normal Activity Log:



status	count	percent
success	4622	97.019312
failure	142	2.980688

Windows Attack Activity Log::



status	count	percent
success	5856	98.436712
failure	93	1.563288

Alert Analysis for Failed Windows Activity

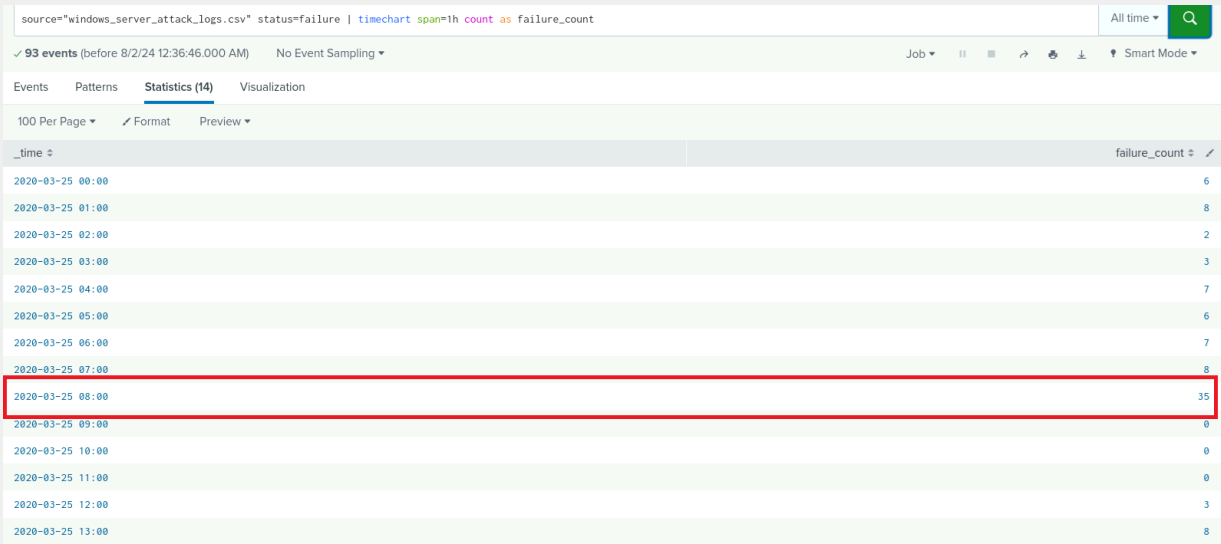
- Did you detect a suspicious volume of failed activity?

```
Yes, our alert did detect a suspicious volume of failed Windows activities.
```

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

```
The count was 35 failed Windows activities.

Windows Attack Activity Log:
```



_time	failure_count
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

- When did it occur?

```
It occurred on 2020-03-25 at 08:00 AM.
```

- Would your alert be triggered for this activity?

```
Yes, the alert would  be triggered for this activity because 35 is higher
than the threshold of 10 that was set.
```

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

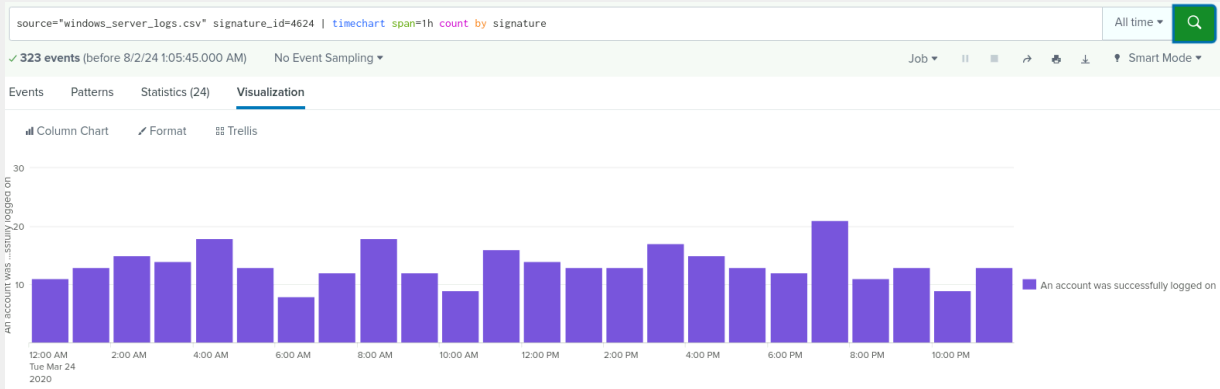
```
No. The threshold is very low and it would detect abnormal activities.
```

Alert Analysis for Successful Logins

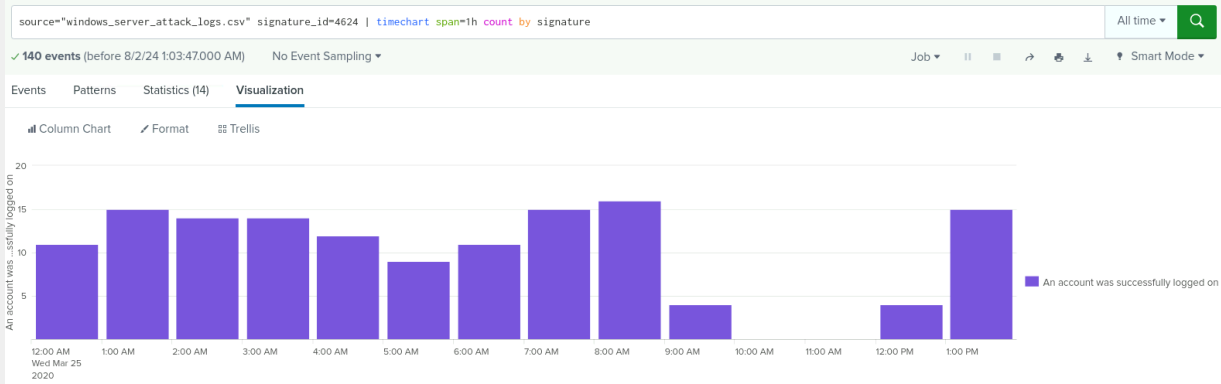
- Did you detect a suspicious volume of successful logins?

There is little difference in successful logins between the 24-03-2020 (normal activity logs) and 25-03-2020 (attack activity log). There was a drop in the successful logins between 10:00 AM and 12PM.

Windows Normal Activity Log:



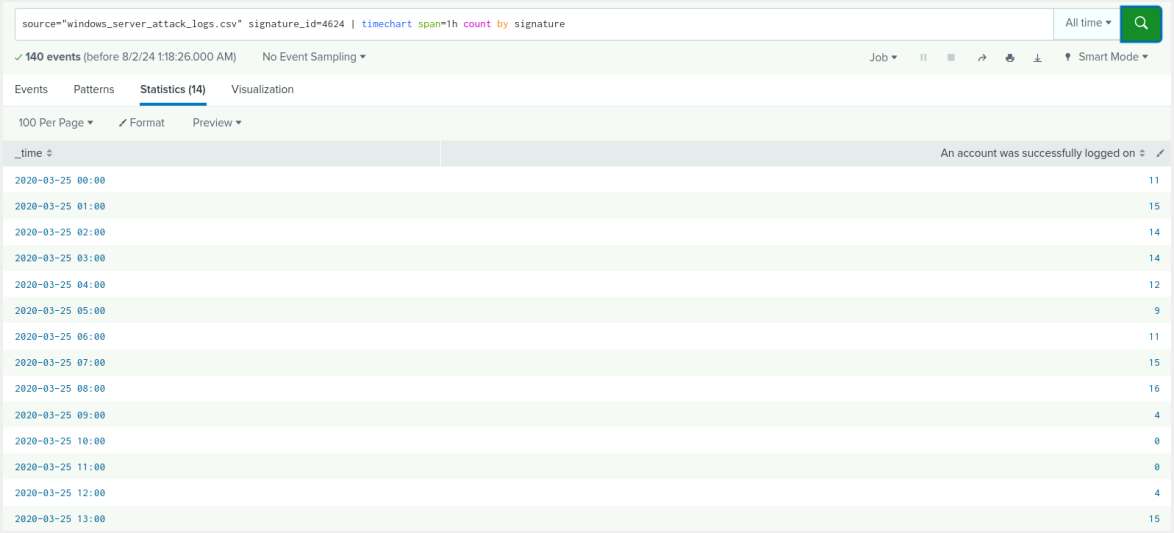
Windows Attack Activity Log:



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

```
There was a peak of 16 successful logins at 8:00 AM, followed by a sharp
decline to 4 at 9:00 AM. No successful logins were recorded between 10:00 AM
and 11:00 AM, after which the number rose back to 4 at 12:00 PM.

Windows Attack Activity Log:
```

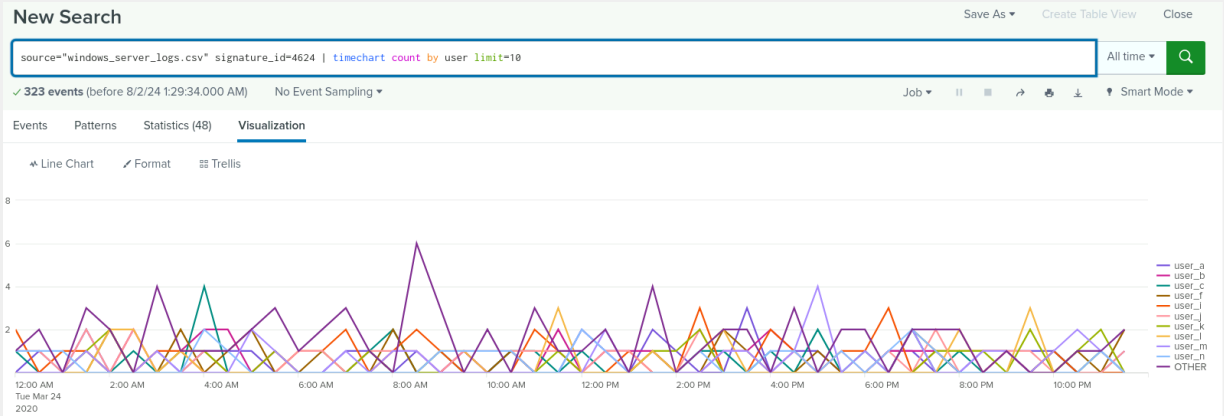


_time	An account was successfully logged on
2020-03-25 00:00	11
2020-03-25 01:00	15
2020-03-25 02:00	14
2020-03-25 03:00	14
2020-03-25 04:00	12
2020-03-25 05:00	9
2020-03-25 06:00	11
2020-03-25 07:00	15
2020-03-25 08:00	16
2020-03-25 09:00	4
2020-03-25 10:00	0
2020-03-25 11:00	0
2020-03-25 12:00	4
2020-03-25 13:00	15

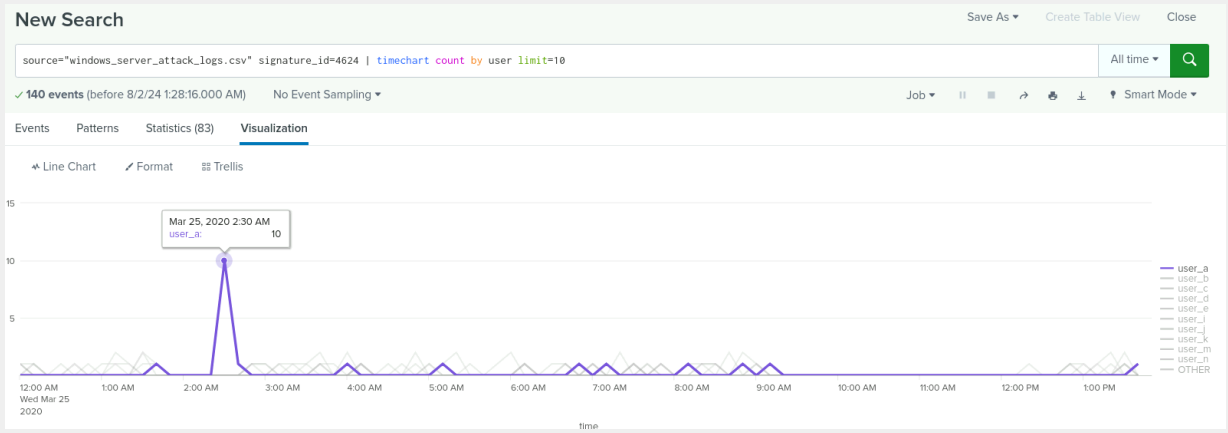
- Who is the primary user logging in?

```
The primary user logged in was User_a.

Windows Normal Activity Log:
```



```
Windows Attack Activity Log:
```



- When did it occur?

```
25-03-2020 around 02:00 AM
```

- Would your alert be triggered for this activity?

```
No,the alert will not be triggered by this activity as we set our
threshold count to 20.
```

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

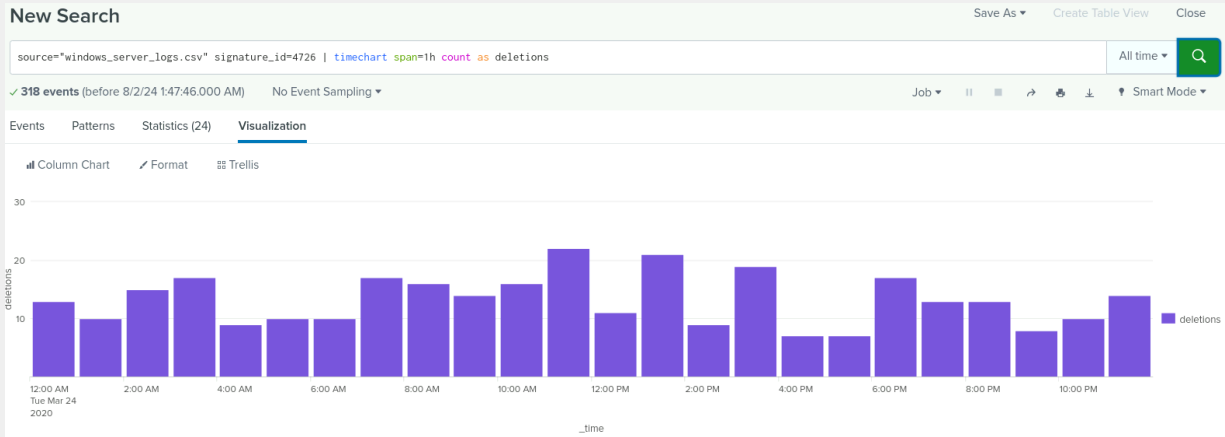
```
Considering our present understanding, probably a small adjustment to the
threshold is possible, but a more informed decision requires a deeper
examination of the log data to optimize alert sensitivity and reduce
fatigue.
```

Alert Analysis for Deleted Accounts

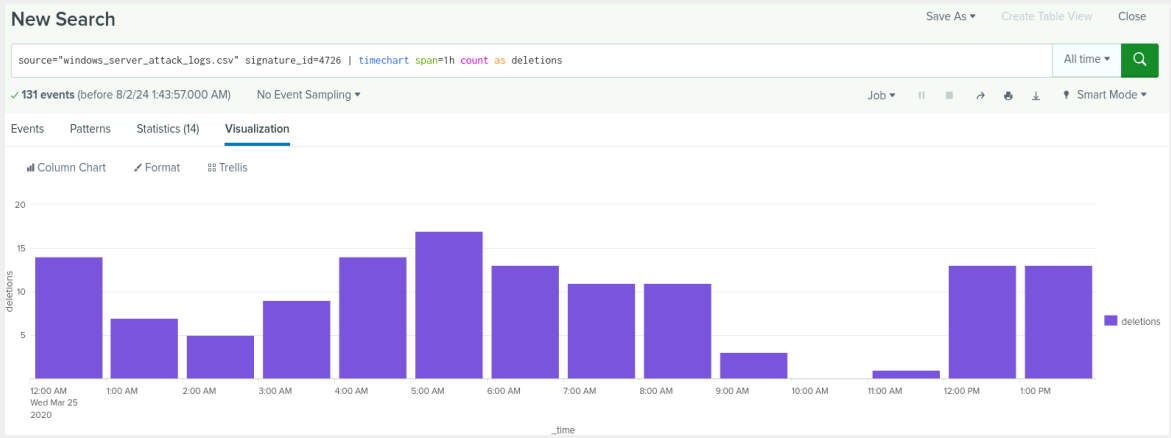
- Did you detect a suspicious volume of deleted accounts?

```
Between 09:00 AM and 11:00 AM there was a significant drop in the number of
deletions (but not in excessive numbers).
```

Windows Normal Activity Log:



Windows Attack Activity Log:



Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
Yes, there are two suspicious signatures: "attempt to
reset account password" and "user account locked out". The counts for these
two signatures are significantly higher relative to previous log data from
windows_server_logs.
```

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

All time

✓ **5,949 events** (before 8/2/24 12:29:05.000 PM) No Event Sampling

Job Smart Mode

Events Patterns **Statistics (14)** Visualization

100 Per Page Format Preview

_time	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
2020-03-25 00:00	19	14	14	8	10	16	11	10	10	12	68
2020-03-25 01:00	12	8	20	13	7	805	15	11	16	16	50
2020-03-25 02:00	9	2	3	16	9	896	14	3	17	8	30
2020-03-25 03:00	13	13	13	12	16	10	14	6	16	14	47
2020-03-25 04:00	12	15	18	8	11	12	12	11	10	16	62
2020-03-25 05:00	11	11	14	12	16	19	9	8	14	10	68
2020-03-25 06:00	9	11	14	12	17	3	11	14	8	13	66
2020-03-25 07:00	15	14	8	15	17	11	15	16	20	7	69
2020-03-25 08:00	17	11	13	23	11	16	16	12	11	16	59
2020-03-25 09:00	5	5	2	1	3	1	4	1258	0	4	10
2020-03-25 10:00	0	0	0	0	0	0	23	761	0	0	0
2020-03-25 11:00	0	0	0	0	0	0	196	0	0	0	0
2020-03-25 12:00	7	14	9	7	11	6	77	6	6	9	45
2020-03-25 13:00	4	12	8	7	9	16	15	12	15	17	49

Normal Activity Log:

New Search

Save As Create Table View Close

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

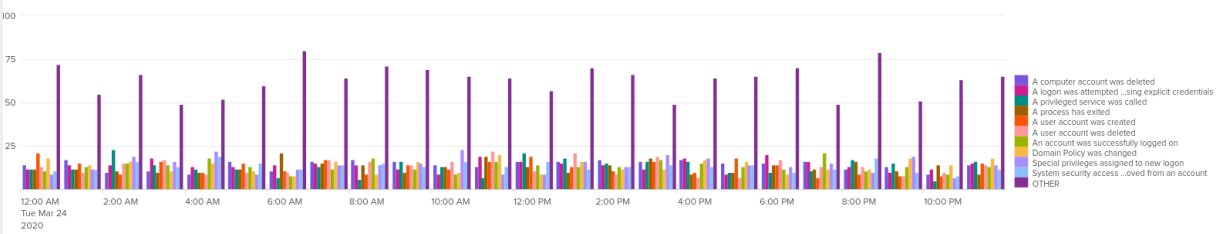
All time

✓ **4,764 events** (before 8/2/24 1:50:59.000 AM) No Event Sampling

Job Smart Mode

Events Patterns Statistics (24) **Visualization**

Column Chart Format Trellis



Attack Activity Log:

New Search

Save As Create Table View Close

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

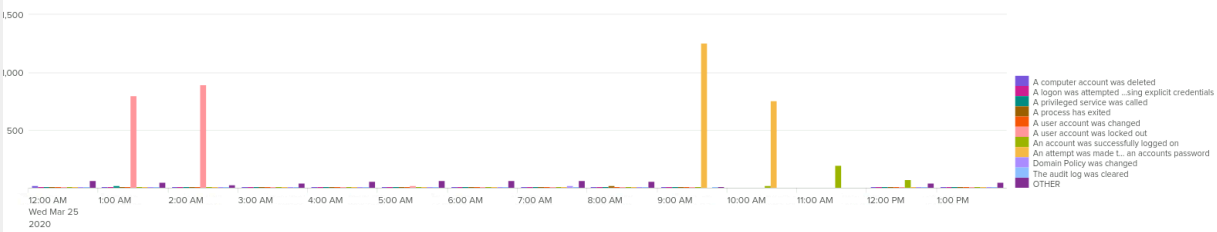
All time

✓ **5,949 events** (before 8/2/24 1:51:44.000 AM) No Event Sampling

Job Smart Mode

Events Patterns Statistics (14) **Visualization**

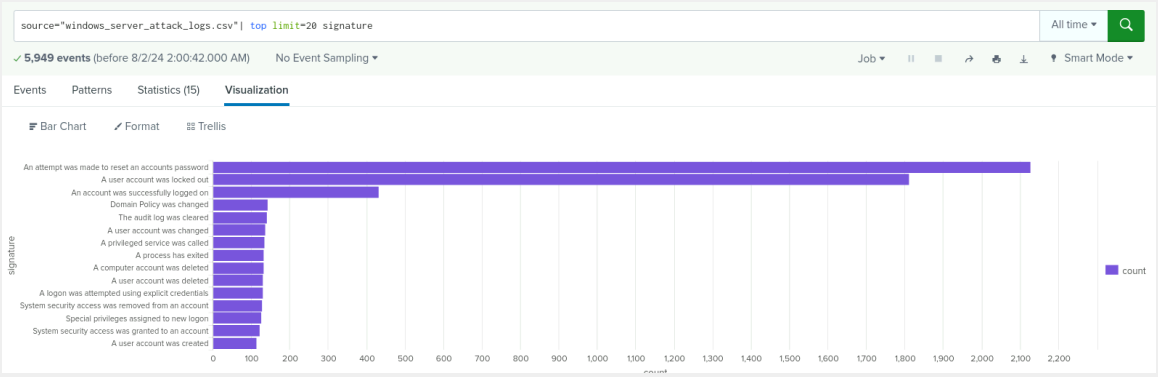
Column Chart Format Trellis



- What signatures stand out?

```
There are two signature that stands out:
```

- "An attempt was made to reset an accouns password" - with 2128 attempts.
- "A user account was locked out" - with 1811



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

```
- For “An user account was locked out” between 1:00 AM - 2:00 AM
- For “An attempt was made to reset an account password” between 09:00
  AM and 10:00 AM
```

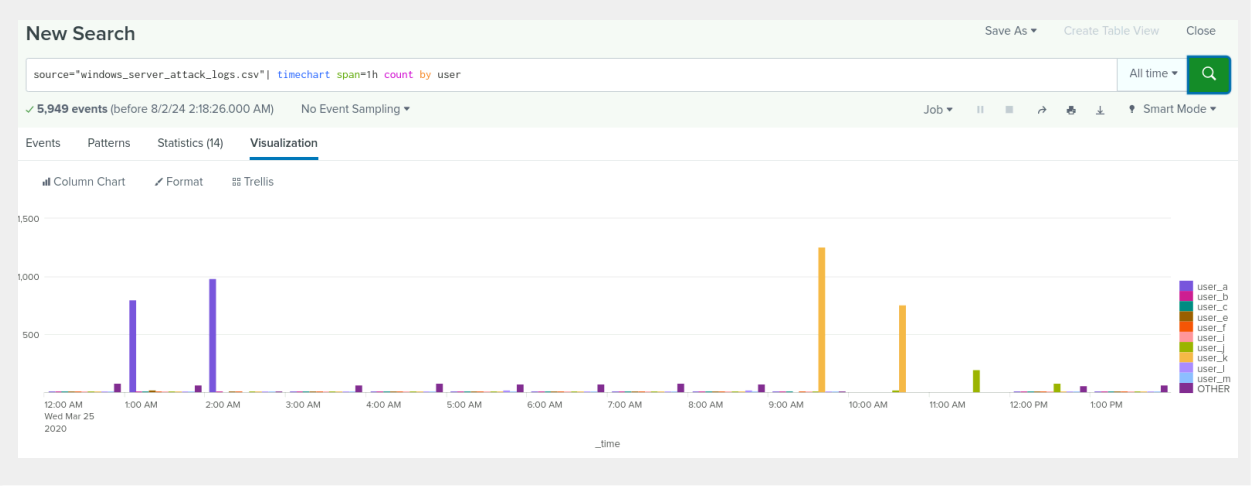
- What is the peak count of the different signatures?

```
- The peak for “An User Account was locked out” was at 896
- The peak for “An attempt was made to reset an account password” was at
  1258
```

Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
Yes, in the “Users by Hour” visualization chart below there are two users
who have significant increases in activity:
1. User_a
2. User_k
```



- Which users stand out?

```
User_k and user_a
```

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

```
User_a between 01:00 AM and 02:30 AM.
User_k between 09:00 AM and 10:00 AM
```

- What is the peak count of the different users?

```
The peak count was:
    • User_a 984
    • User_k 1256
```

New Search

Save As Create Table View Close

New Search

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

All time

✓ 5,949 events (before 8/2/24 2:26:21.000 AM) No Event Sampling Job Smart Mode

Events Patterns Statistics (14) Visualization

100 Per Page Format Preview

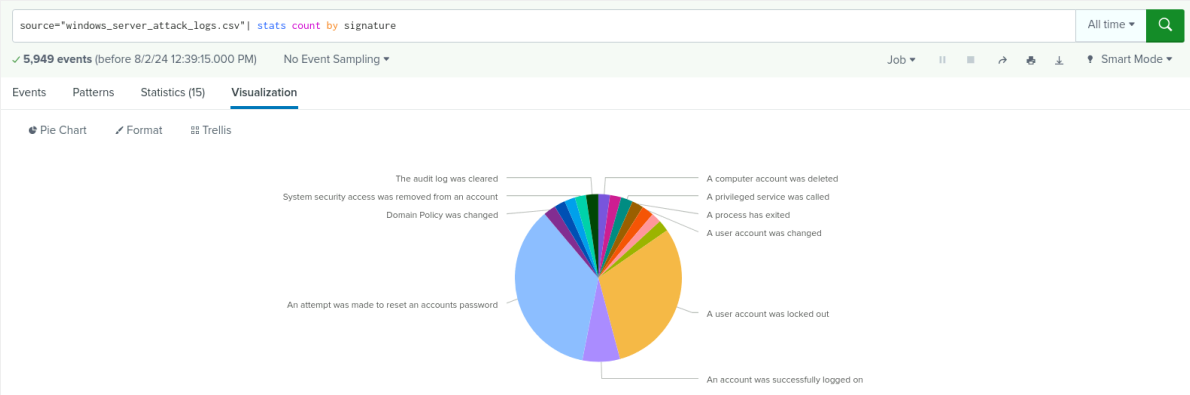
_time	user_a	user_b	user_c	user_e	user_f	user_i	user_j	user_k	user_l	user_m	OTHER
2020-03-25 00:00	7	11	12	10	10	14	11	8	14	13	82
2020-03-25 01:00	799	18	12	20	9	15	6	9	9	10	66
2020-03-25 02:00	984	3	0	1	2	0	2	2	3	1	9
2020-03-25 03:00	8	13	8	17	9	12	8	4	17	10	68
2020-03-25 04:00	8	10	10	5	15	9	15	16	8	10	81
2020-03-25 05:00	13	6	9	14	9	10	9	13	19	15	75
2020-03-25 06:00	10	9	11	14	14	9	2	7	17	12	73
2020-03-25 07:00	16	11	9	15	14	8	18	7	10	16	83
2020-03-25 08:00	18	14	7	9	12	12	13	12	25	10	73
2020-03-25 09:00	3	1	5	0	1	2	2	1256	5	1	17
2020-03-25 10:00	0	0	0	0	0	0	23	761	0	0	0
2020-03-25 11:00	0	0	0	0	0	0	196	0	0	0	0
2020-03-25 12:00	4	8	10	3	6	4	82	8	6	7	59
2020-03-25 13:00	8	5	12	9	8	11	11	15	12	8	65

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

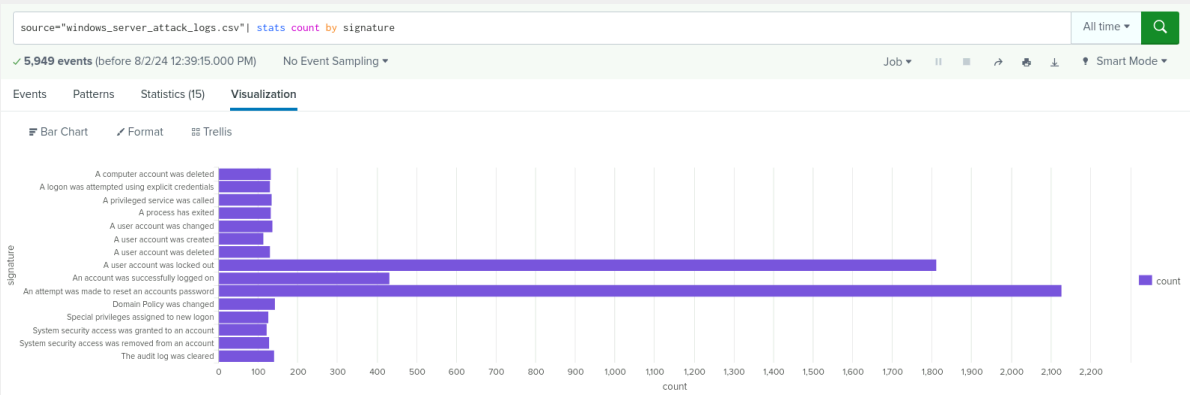
- Does anything stand out as suspicious?

```
Yes, there are two suspicious signatures: "attempt to
reset account password" and "user account locked out". The counts for these
two signatures are significantly higher relative to previous log data from
windows_server_logs.
If we look closely at the Bar Chart below there is the 3rd signature “An
account was successfully logged on” - but the count is not abnormally high.
Further investigation is needed."
```

Pie Chart:



Bar Chart:



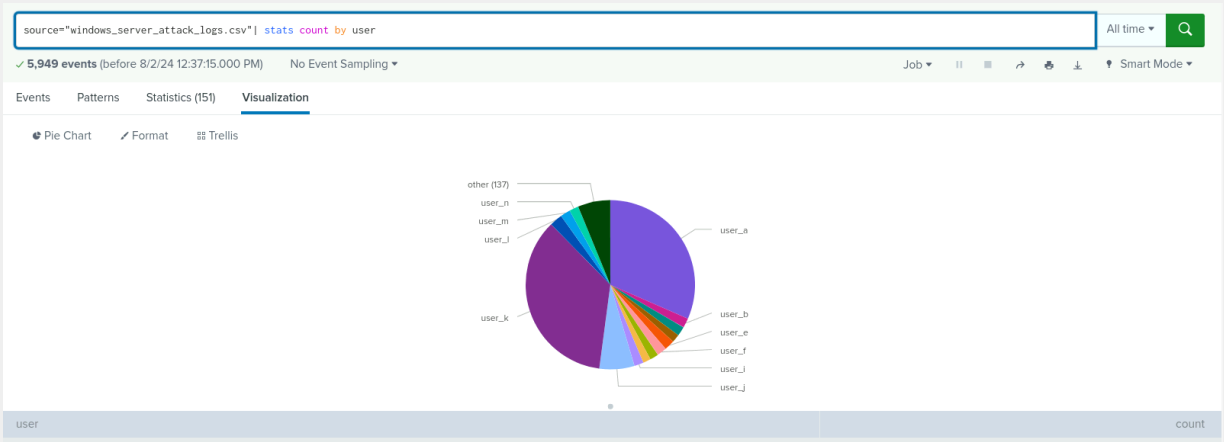
- Do the results match your findings in your time chart for signatures?

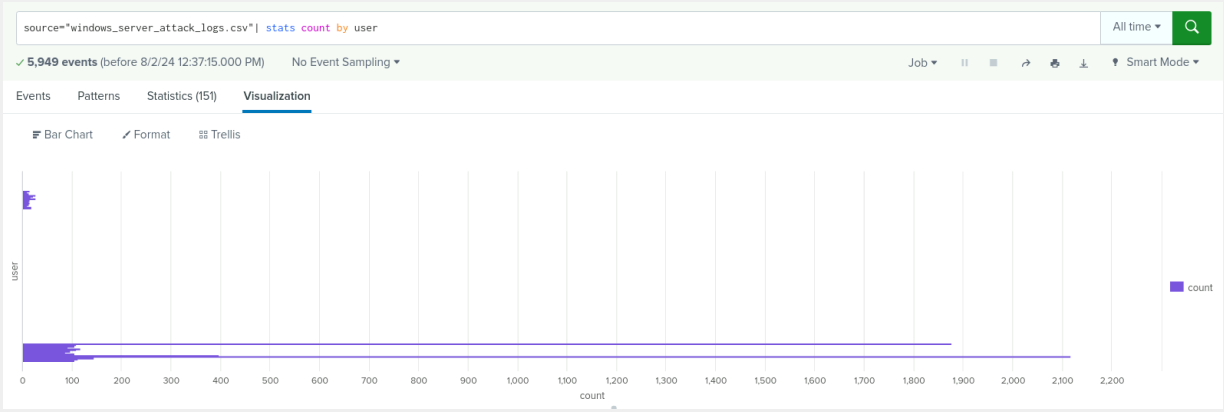
```
Yes, they match.
```

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

- Does anything stand out as suspicious?

```
Yes, there are two users who have significant increases in activity:
1. User_a
2. User_k
```





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

```
Yes, they match.
```

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?

Statistical Charts

Advantages:

- A statistical chart is a visual representation of data that helps us to easily understand and analyze users' complex data by presenting it in a graphical format.
- We can effectively visualize users' complex datasets and statistical distributions.
- We can also see signatures or users’ total amount pe event

Disadvantages:

- Statistical charts cannot illustrate changes in user behavior over time

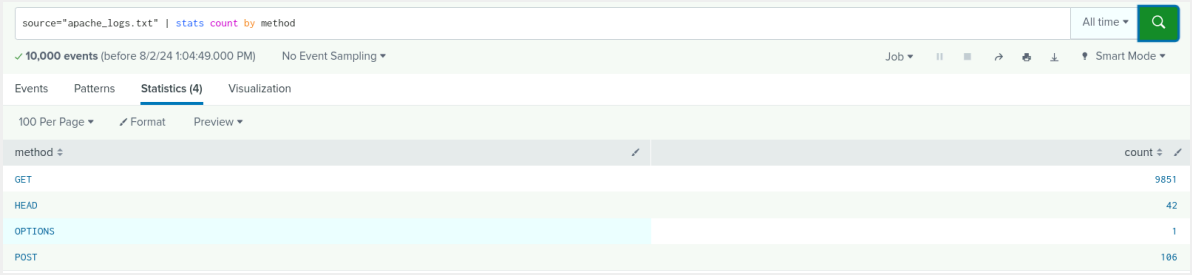
Apache Web Server Log Questions

Report Analysis for Methods

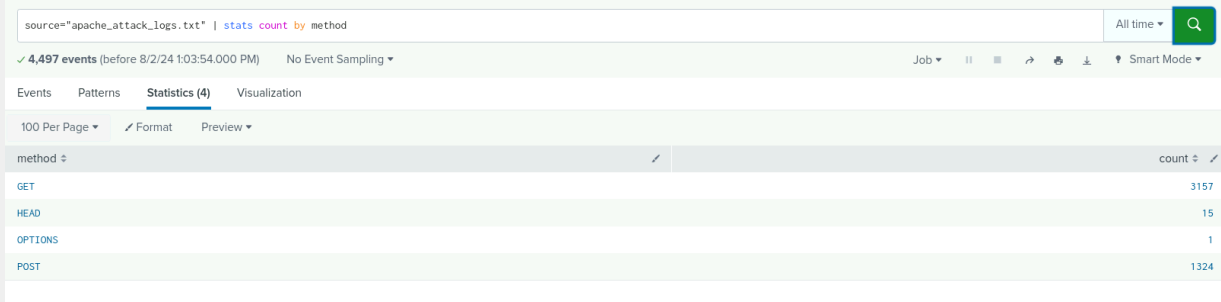
- Did you detect any suspicious changes in HTTP methods? If so, which one?

Yes, there's a notable anomaly in the HTTP method following the attack. GET requests experienced a substantial decrease, while POST requests saw a dramatic increase.

Apache Normal Activity Log:



Apache Attack Log:



method	count
GET	3157
HEAD	15
OPTIONS	1
POST	1324

- What is that method used for?

HTTP GET requests data from a server, such as a web page or a specific resource. GET requests data but does not modify it, it's like read-only operations.

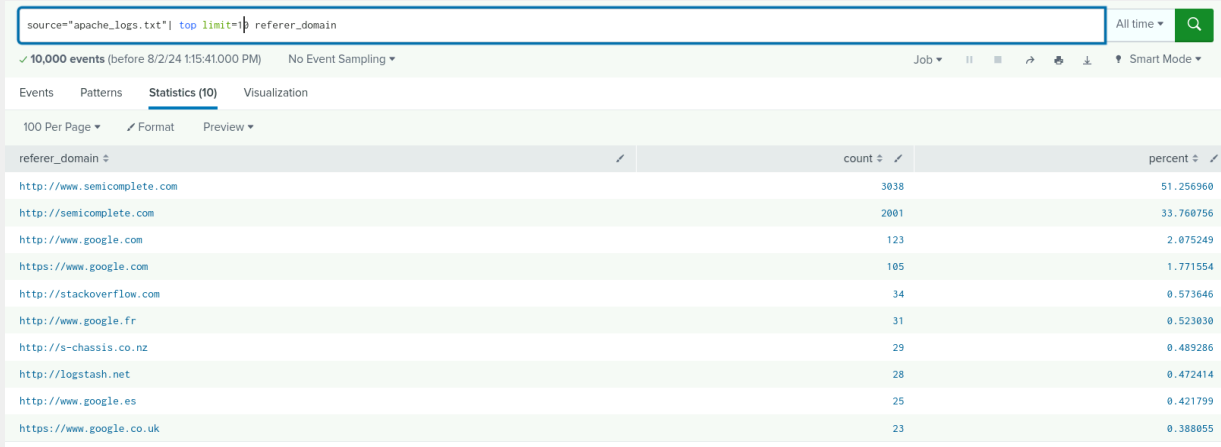
HTTP POST sends data to a server to create or update a resource, such as submitting a form or uploading a file.

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

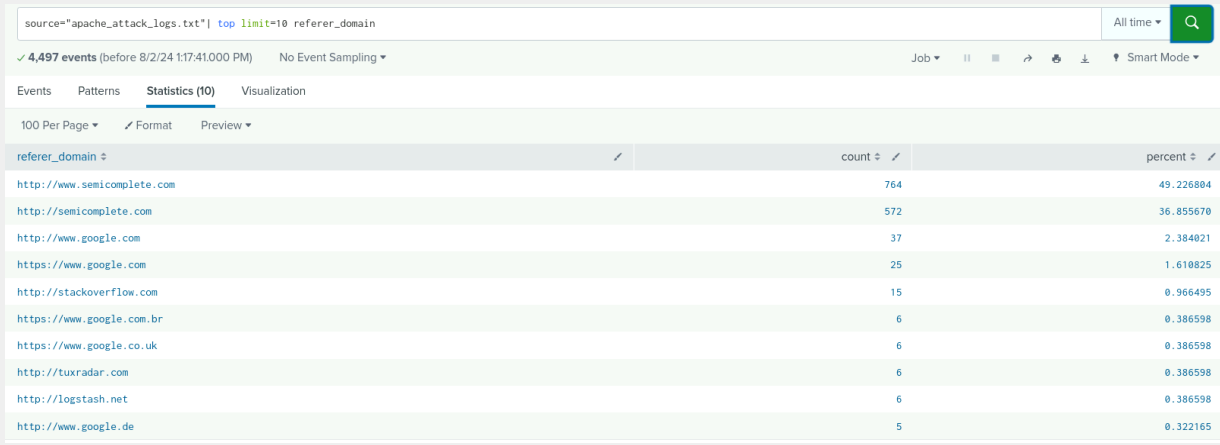
Yes, there are anomalous changes in referrer domains. The count of all referrer domains significantly dropped in the attack log.

Apache Normal Activity Log:



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

Apache Attack Log:



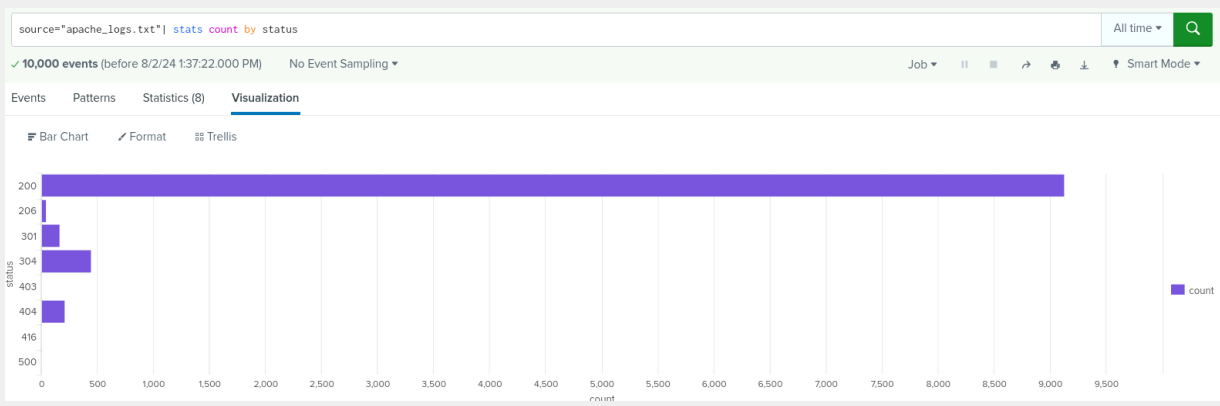
referer_domain	count	percent
http://www.semicomplete.com	764	49.226804
http://semicomplete.com	572	36.855670
http://www.google.com	37	2.384021
https://www.google.com	25	1.610825
http://stackoverflow.com	15	0.966495
https://www.google.com.br	6	0.386598
https://www.google.co.uk	6	0.386598
http://tuxradar.com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

Report Analysis for HTTP Response Codes

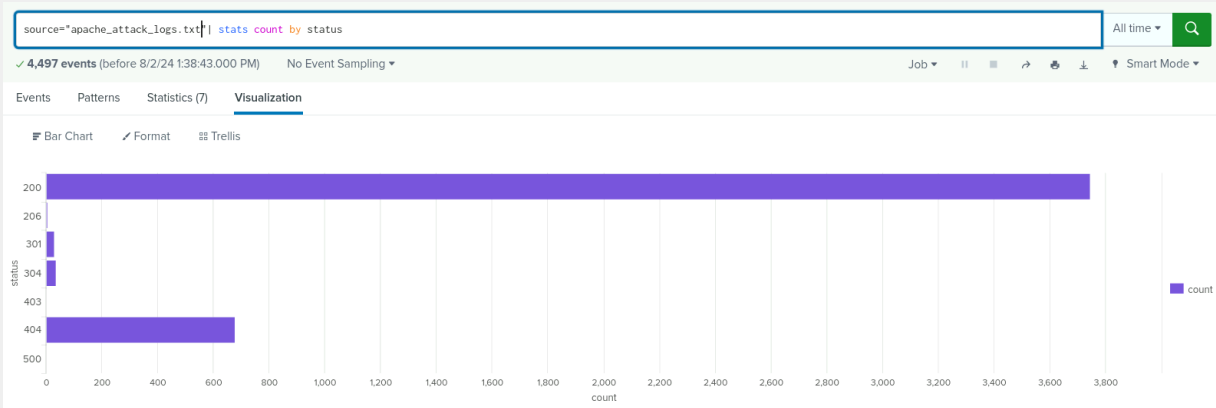
- Did you detect any suspicious changes in HTTP response codes?

Yes, there is a significant shift in HTTP response codes between the Normal Activity Log and attack logs. A substantial decrease in successful '200 OK' responses and a substantial increase in '404 Not Found' errors indicate potential malicious activity.

Apache Normal Activity log:



Apache Attack Log:

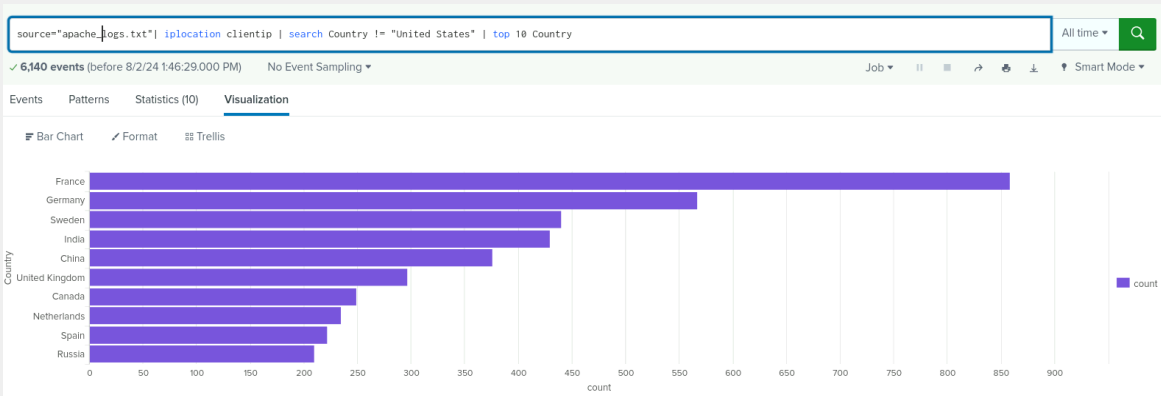


Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

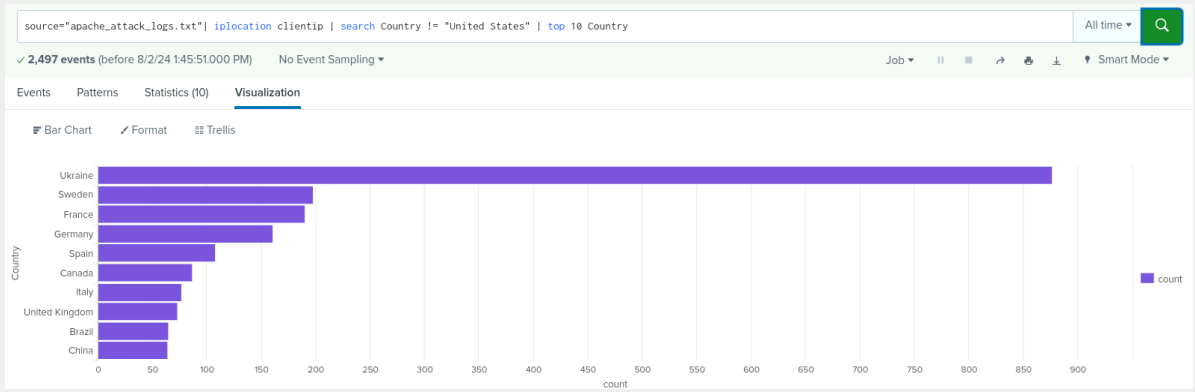
Yes, there is a suspicious increase in international activity.
The number of events at 6 PM on March 25, 2020, is abnormally high compared to all other hourly records in both normal and attack logs.

Apache Normal Activity Log:

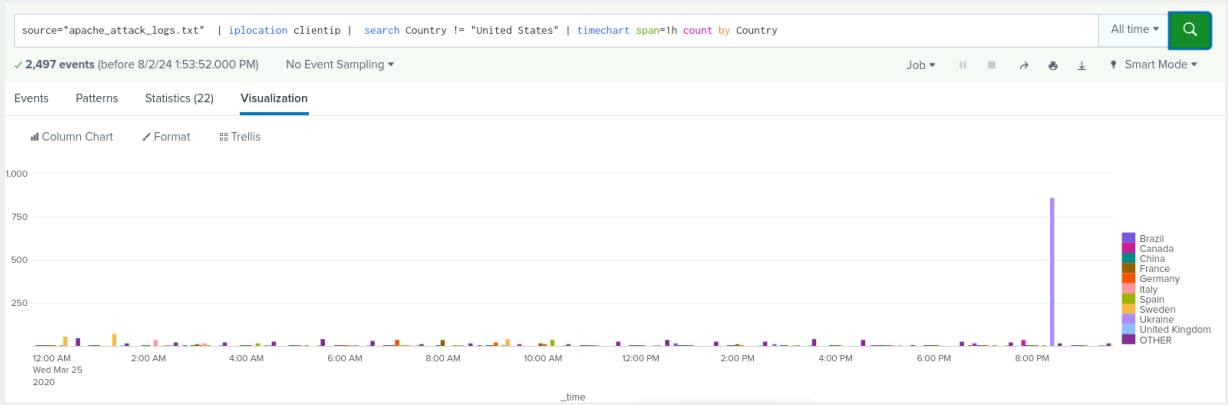


Visualization by Time:

Apache Attack Log:



Visualization by Time:



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

The count of events at 8:00 PM on 2020-03-25 was 864

- Would your alert be triggered for this activity?

```
Yes, the alert will be triggered by this activity because the threshold was
set at 126.
```

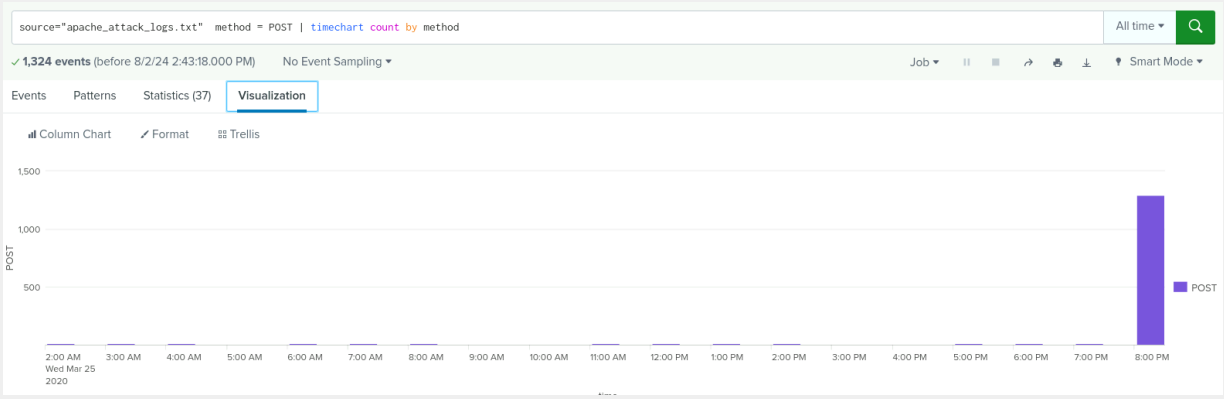
- After reviewing, would you change the threshold that you previously selected?

```
Probably yes, the threshold should be adjusted. While the current threshold
is sensitive enough to detect spikes in international activity, the
significant increase on March 25, 2020, at 8:00 PM suggests a need for
recalibration.
```

Alert Analysis for HTTP POST Activity

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

```
Yes, in the Apache attack log, there is an increase in POST requests.
```



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

```
The count is: 1296
```

- When did it occur?

```
March 25, 2020 at 8:00 PM
```

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

```
Probably yes, the threshold should likely be adjusted. The current threshold
of 10 effectively detects spikes in normal daily HTTP POST activity.
However, we should consider raising it. Further investigation and analysis
of more log data are necessary to determine the optimal threshold.
```

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
Yes, during the attack there is a significant increase in the use of the
HTTP POST method.
```

.

_time	GET	HEAD	OPTIONS	POST
2020-03-25 00:00	128	0	0	0
2020-03-25 01:00	120	0	0	0
2020-03-25 02:00	113	0	0	2
2020-03-25 03:00	125	0	0	2
2020-03-25 04:00	112	1	0	2
2020-03-25 05:00	116	8	0	0
2020-03-25 06:00	112	1	0	2
2020-03-25 07:00	120	1	0	1
2020-03-25 08:00	110	1	0	3
2020-03-25 09:00	125	0	0	0
2020-03-25 10:00	115	1	0	0
2020-03-25 11:00	111	0	0	1
2020-03-25 12:00	110	1	0	1
2020-03-25 13:00	106	0	0	7
2020-03-25 14:00	118	0	1	3
2020-03-25 15:00	125	1	0	0
2020-03-25 16:00	118	0	0	0
2020-03-25 17:00	117	0	0	2
2020-03-25 18:00	729	0	0	1
2020-03-25 19:00	122	0	0	[illegible]
2020-03-25 20:00	119	0	0	1296
2020-03-25 21:00	86	0	0	0

- Which method seems to be used in the attack?

```
The HTTP POST method.
```

- At what times did the attack start and stop?

```
Between 8:00 PM - 9:00 PM
```

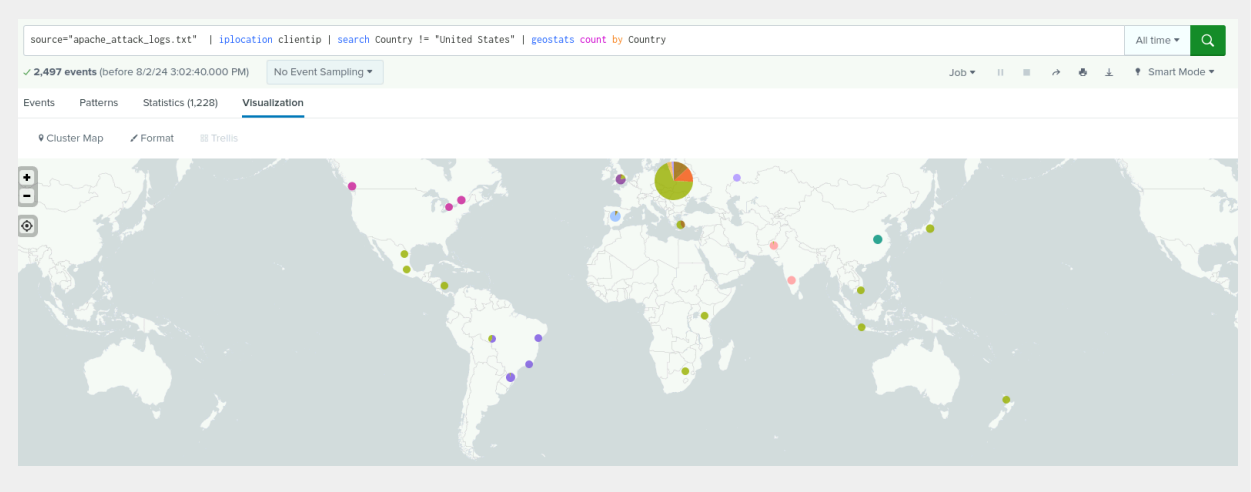
- What is the peak count of the top method during the attack?

```
The peak count is: 1296
```

Dashboard Analysis for Cluster Map

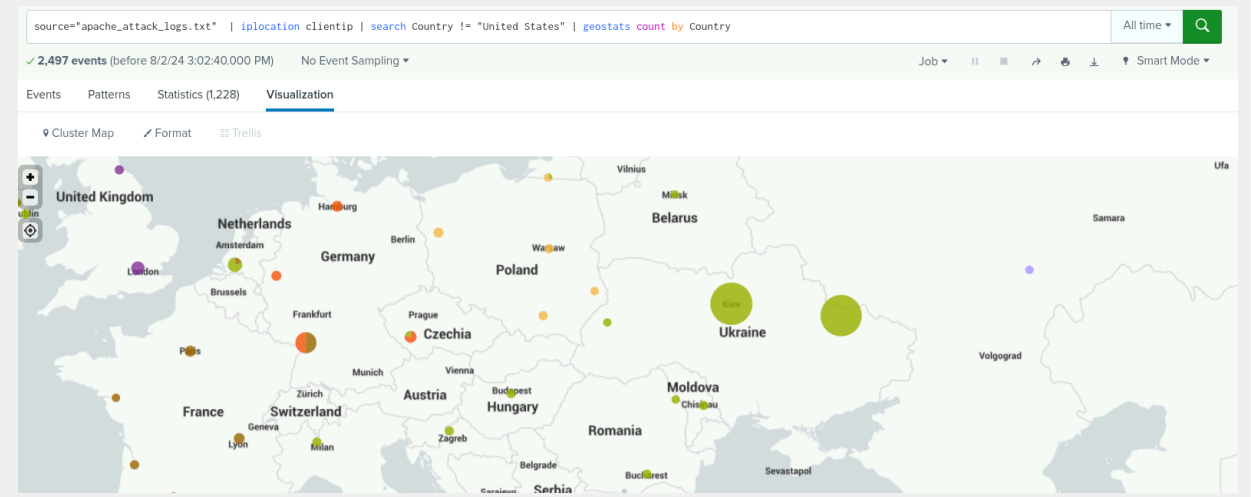
- Does anything stand out as suspicious?

```
Yes, there is abnormal activity from Eastern Europe in the Apache attack
log.
```



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

The location with a high volume of activity is Ukraine.



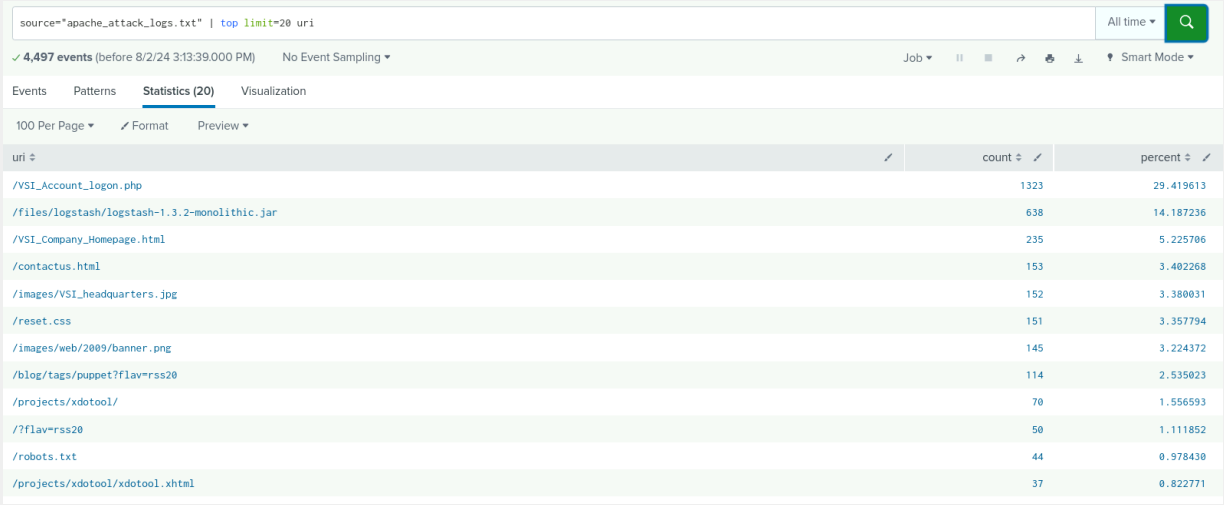
- What is the count of that city?

```
Kharkiv: 432
Kiev: 440
```

Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

```
Yes, from the apache attack log file, there is an increase in activity on
/VSI_Account_logon.php
Also there is a suspicious increase in activity on
/files/logstash/logstash-1.3.2-monolithic.jar.
```



uri	count	percent
/VSI_Account_logon.php	1323	29.419613
/files/logstash/logstash-1.3.2-monolithic.jar	638	14.187236
/VSI_Company_Homepage.html	235	5.225706
/contactus.html	153	3.402268
/images/VSI_headquarters.jpg	152	3.380031
/reset.css	151	3.357794
/images/web/2009/banner.png	145	3.224372
/blog/tags/puppet?flav=rss20	114	2.535023
/projects/xdotool/	70	1.556593
/?flav=rss20	50	1.111852
/robots.txt	44	0.978430
/projects/xdotool/xdotool.xhtml	37	0.822771

- What URI is hit the most?

```
VSI_Account_logon.php
```

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

```
The 'VSI_Account_logon.php' URI suggests an attempt to log in to an account
on the VSI platform. The increase in HTTP POST requests strongly suggest a
potential brute force attack.
```