Cybersecurity

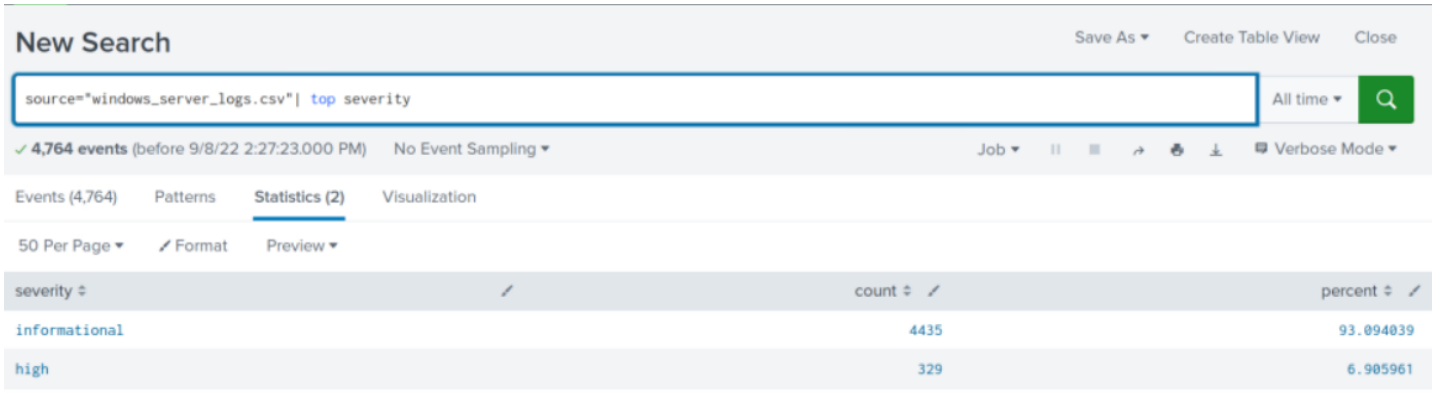
Project 3 Review Questions

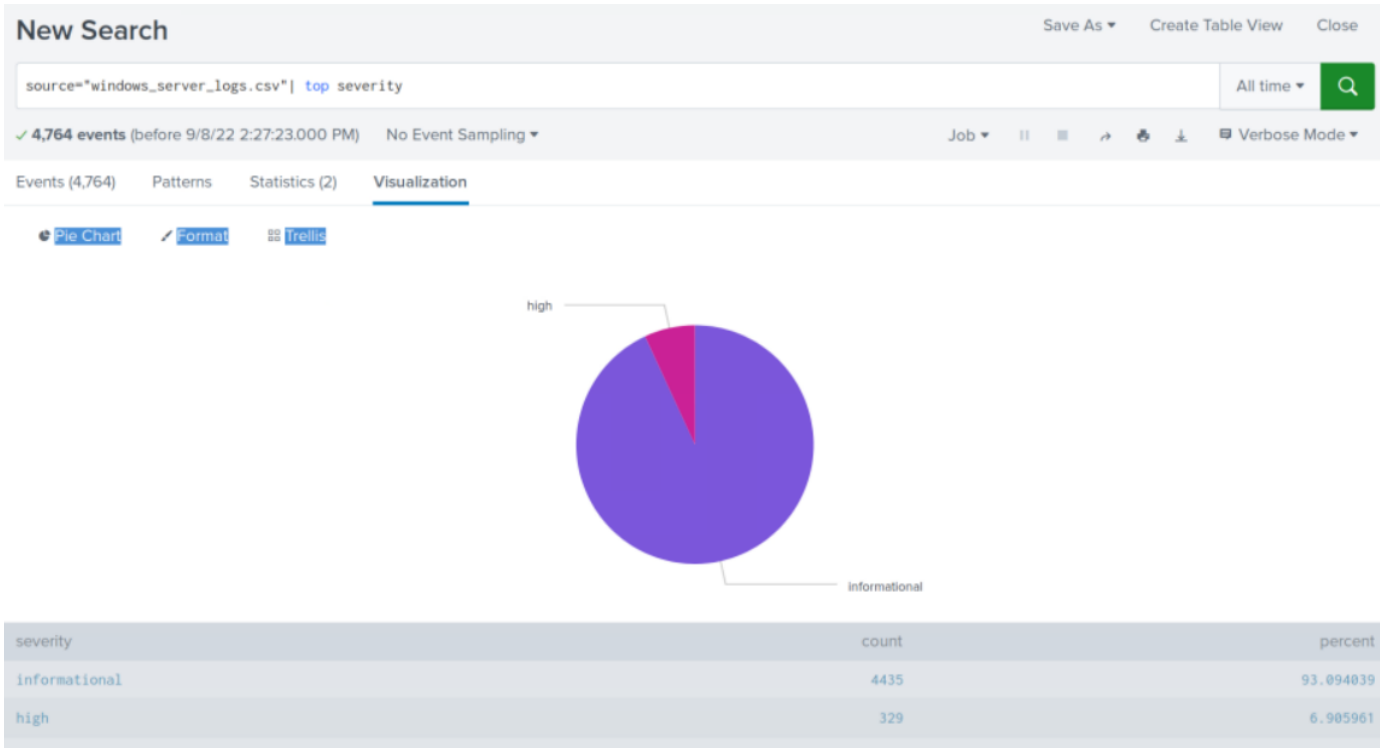
Make a copy of this document before you begin. Place your answers below each question.

Windows Server Log Questions:

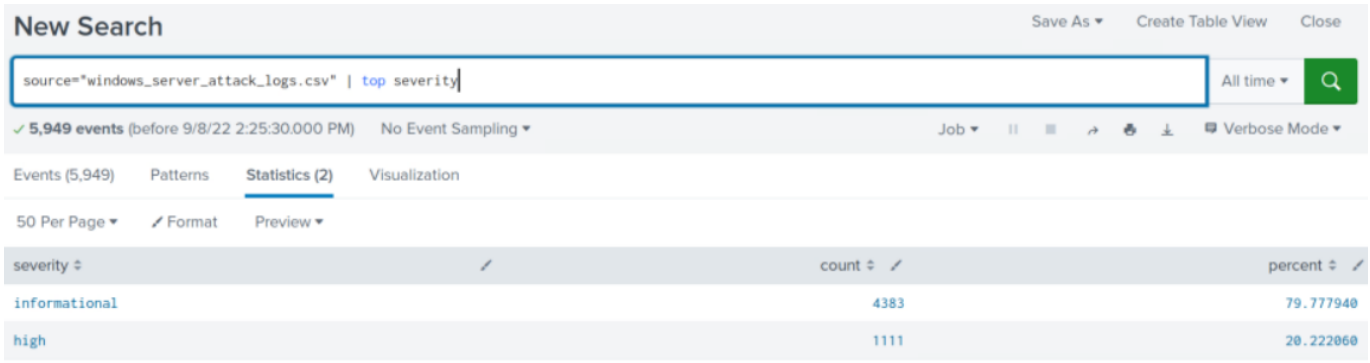
Report Analysis for Severity:

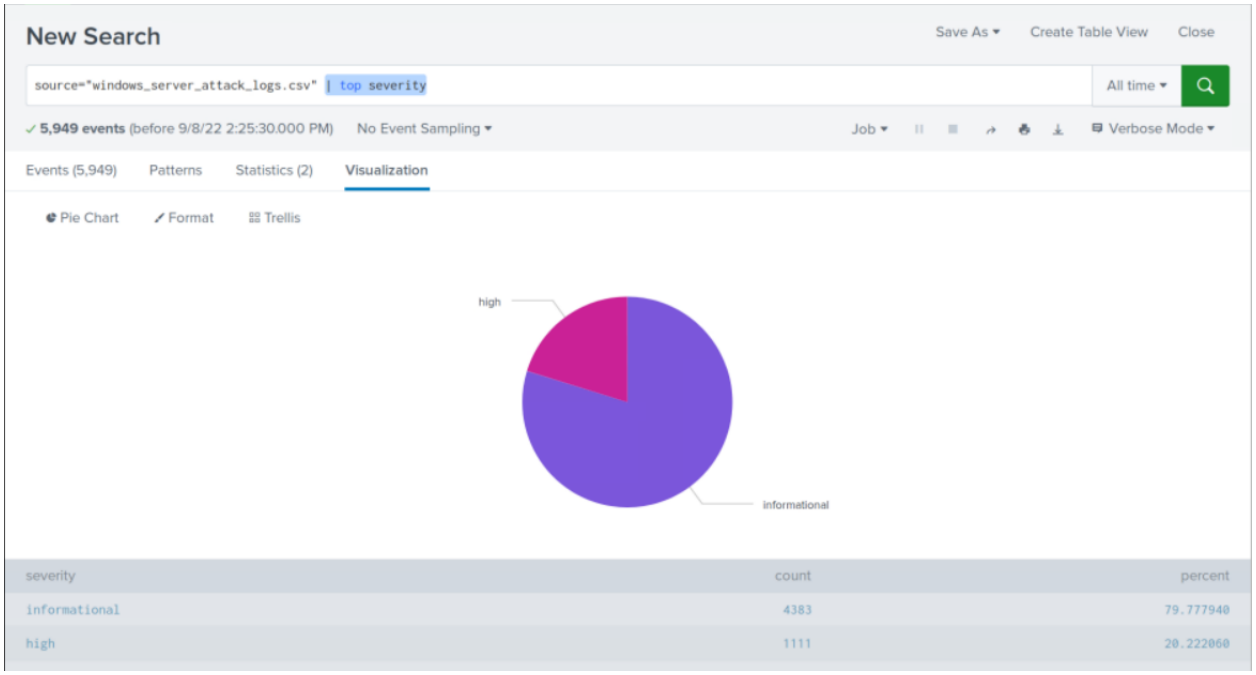
Window Server Logs:





Windows Server Attack Logs:



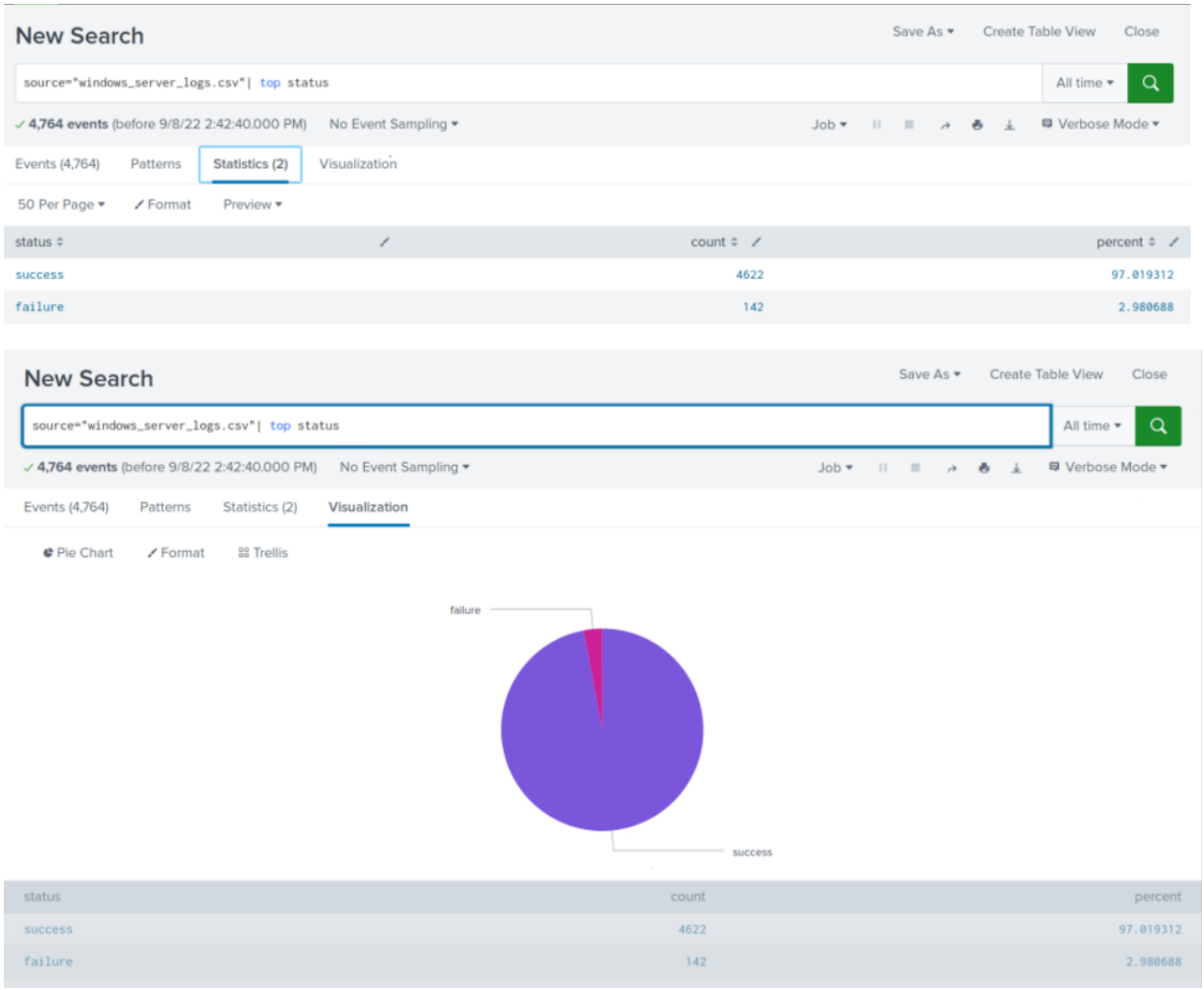


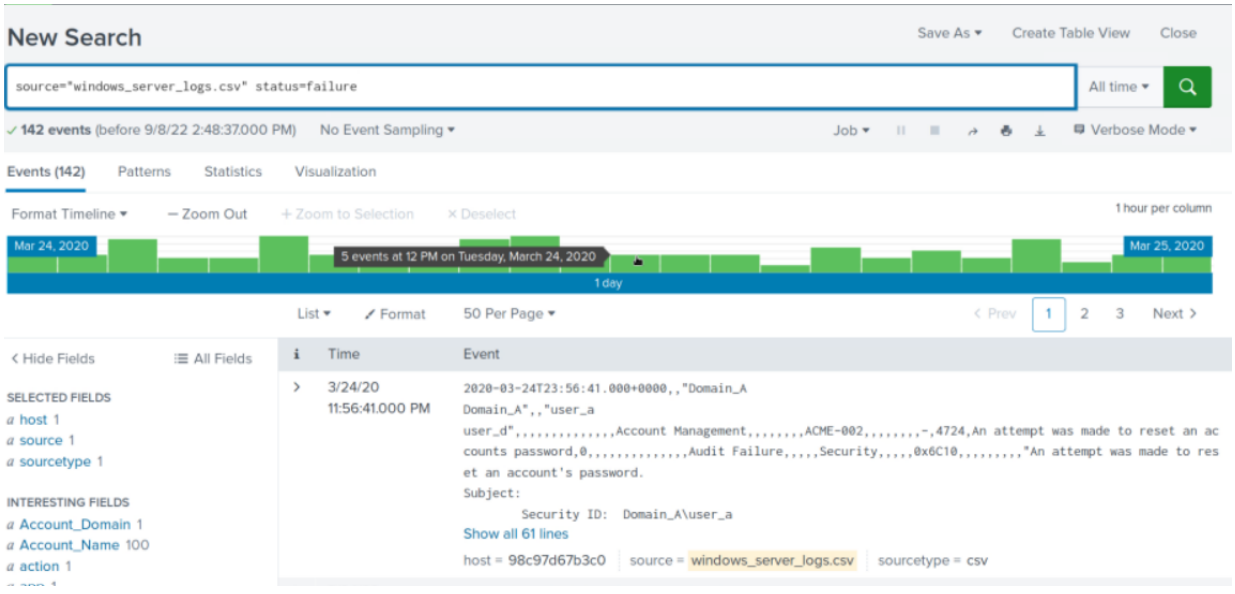
- Did you detect any suspicious changes in severity?

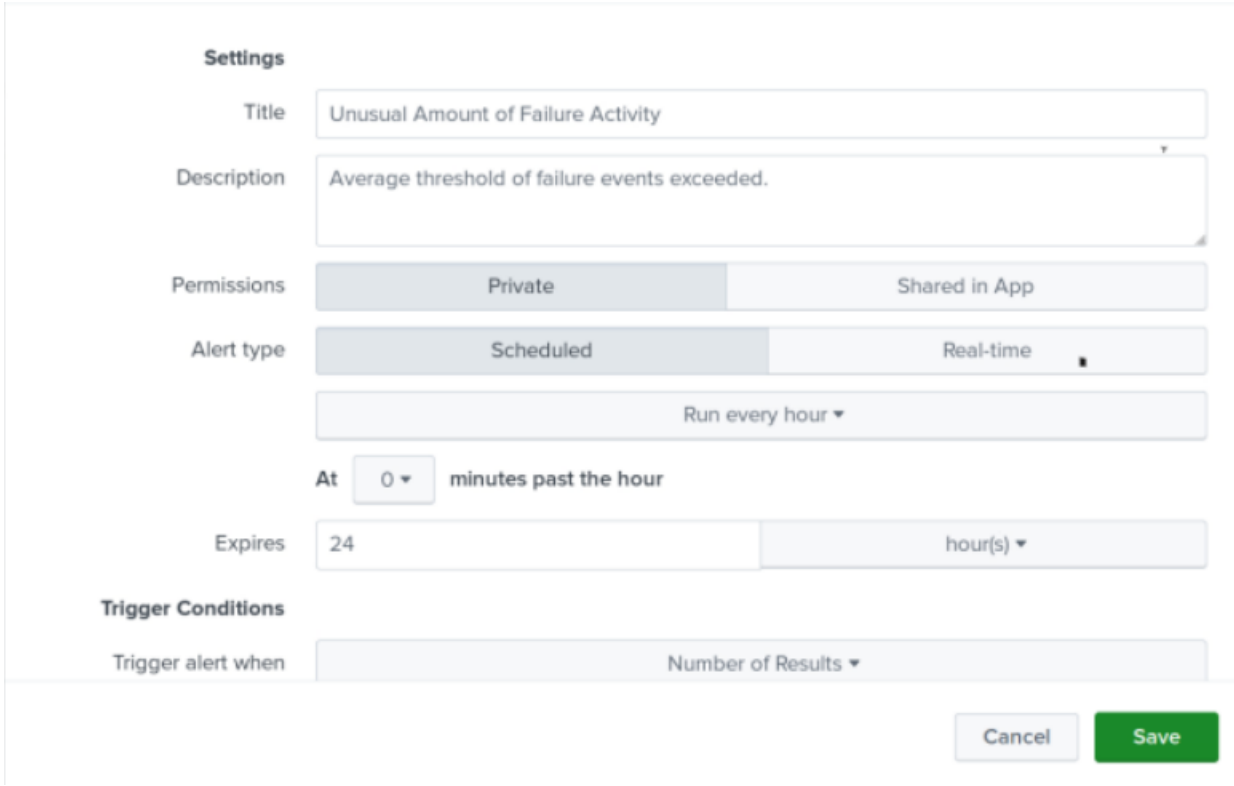
Taking the above screenshots into consideration, the high severity index jumped from 6.90% to 20.22% indicating an approximate 13% increase in severity.

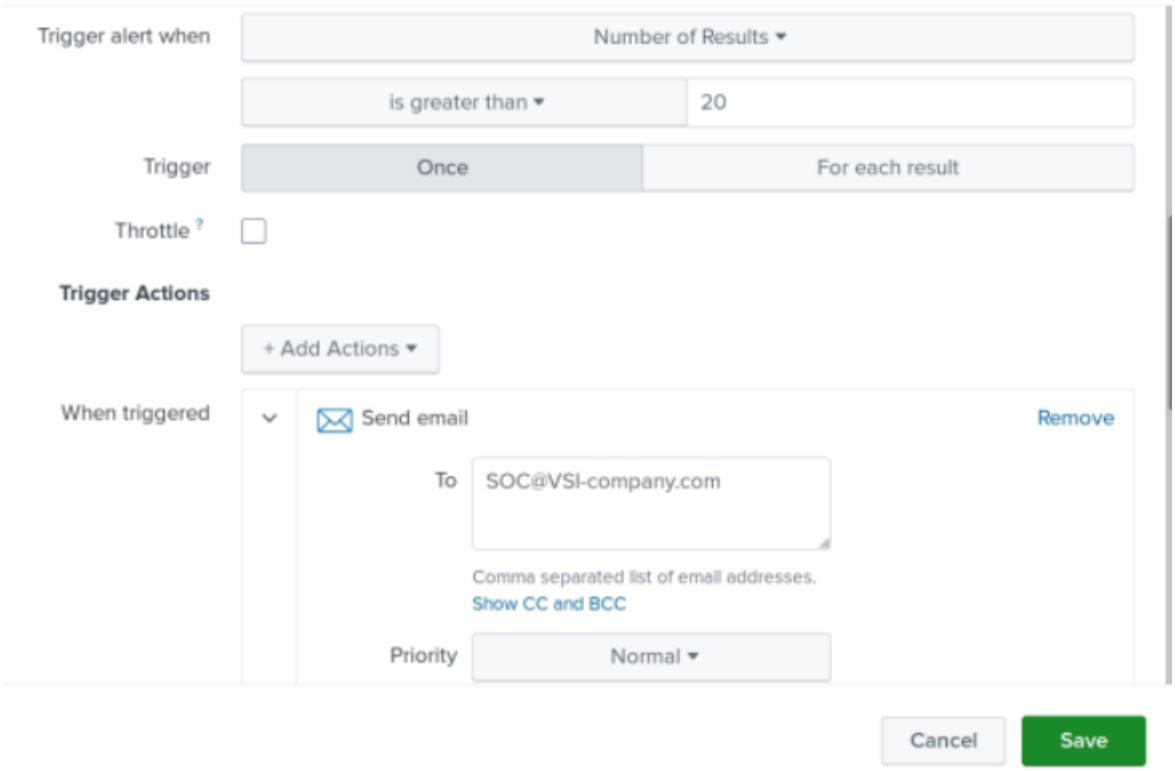
Report Analysis for Failed Activities:

Windows Server Logs:

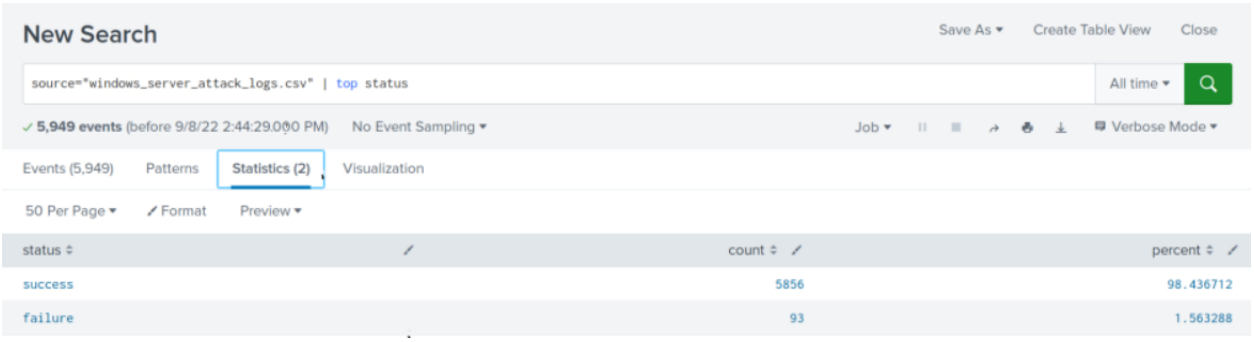


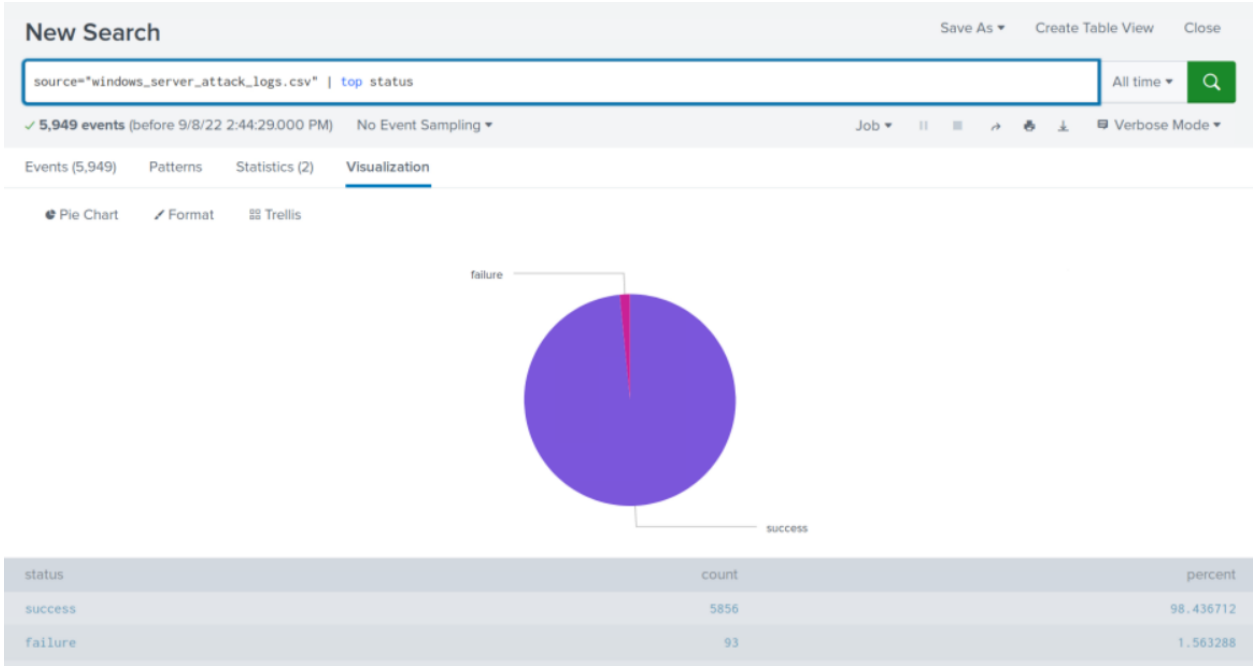

New Search
Save As
Create Table View
Close
source="windows_server_logs.csv" status=failure
All time
142 events (before 9/8/22 2:48:37.000 PM)
No Event Sampling
Job
Verbose Mode
Events (142)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Mar 24, 2020
5 events at 12 PM on Tuesday, March 24, 2020
Mar 25, 2020
1 day
List
Format
50 Per Page
Prev
1
2
3
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a Account_Domain 1
a Account_Name 100
a action 1
Time
Event
3/24/20
11:56:41.000 PM
2020-03-24T23:56:41.000+0000,,"Domain_A
Domain_A",,"user_a
user_d",,,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,-,4724,An attempt was made to reset an ac
counts password,0,,,,,,,,,,,,,Audit Failure,,,,Security,,,,0x6C10,,,,,,,,"An attempt was made to res
et an account's password.
Subject:
Security ID: Domain_A\user_a
Show all 61 lines
host = 98c97d67b3c0
source = windows_server_logs.csv
sourcetype = csv


Settings
Title
Unusual Amount of Failure Activity
Description
Average threshold of failure events exceeded.
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Run every hour
At
0
minutes past the hour
Expires
24
hour(s)
Trigger Conditions
Trigger alert when
Number of Results
Cancel
Save



Windows Attack Logs:

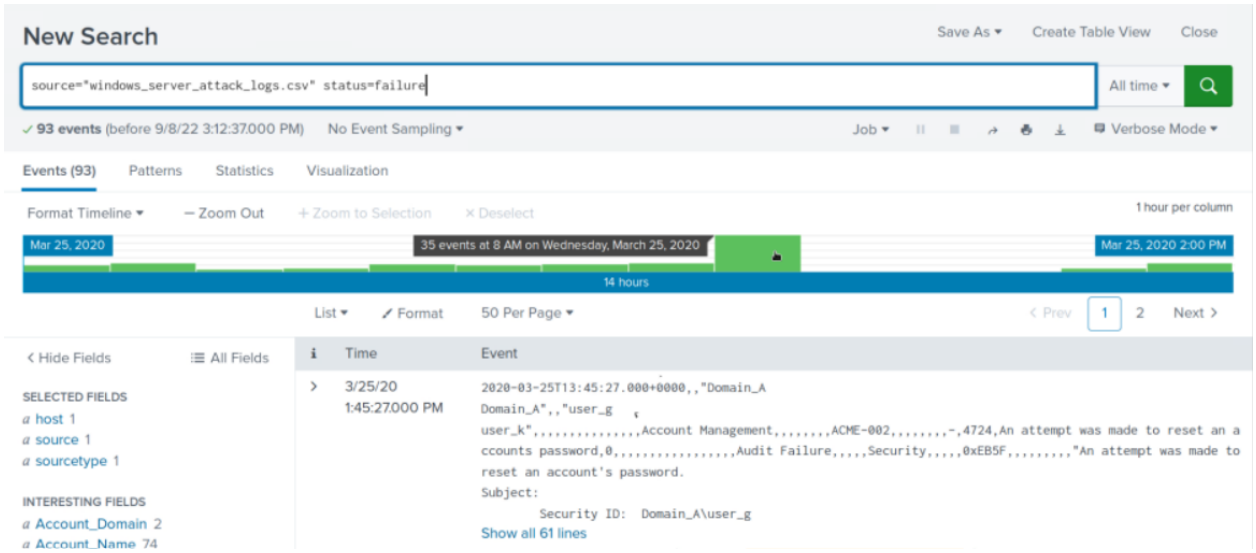


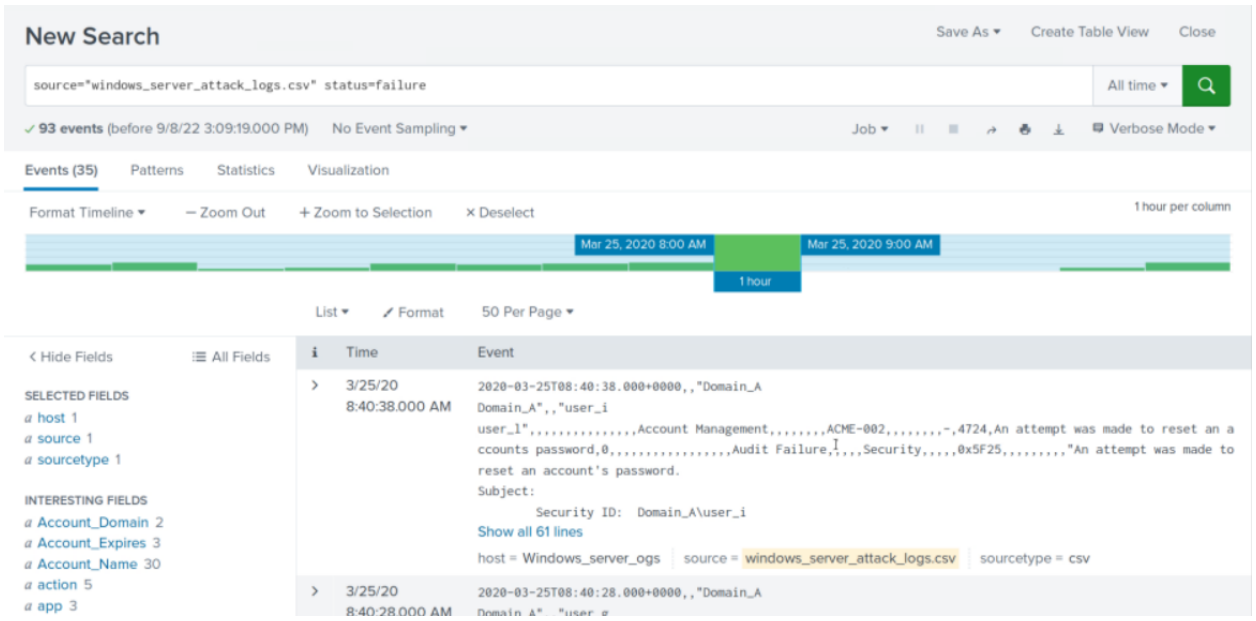


- Did you detect any suspicious changes in failed activities?

```
While the overall amount of events during the attack increased, the failure
count decreased from 142(2.98%) to 93 (1.56%).
```

Alert Analysis for Failed Windows Activity:





- Did you detect a suspicious volume of failed activity?

```
Yes, out of the 93 events that occurred in total, 35 of which occurred on
March 25th between 8:00AM and 9:00AM
```

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

```
Out of the 93 events in the attack log, the failed activity occurred between
8:00-9:00 AM with 35 events.
```

- When did it occur?

```
The failure occurred on March 25th,2020.
```

- Would your alert be triggered for this activity?

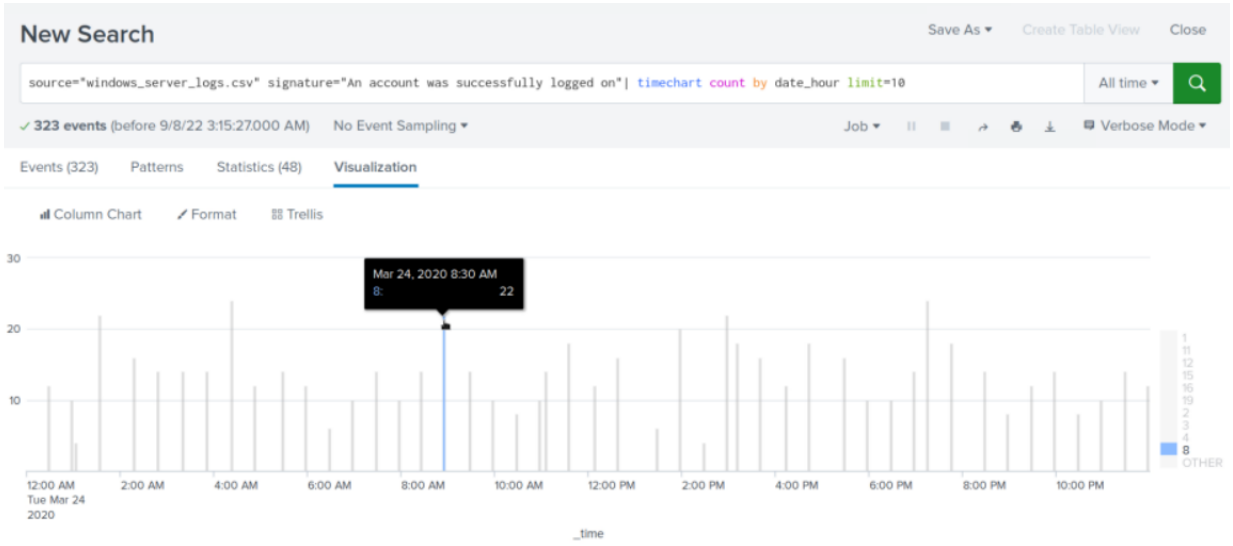
```
Yes, as our threshold was set for 7 events/hour.
```

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

```
As the threshold was appropriately set, no, however, it is consistently
important to appraise user activity and modify thresholds to make sure alert
fatigue does not happen and the baseline of user activity is always being
re-evaluated to reflect current usage patterns.
```

Alert Analysis for Successful Logins:

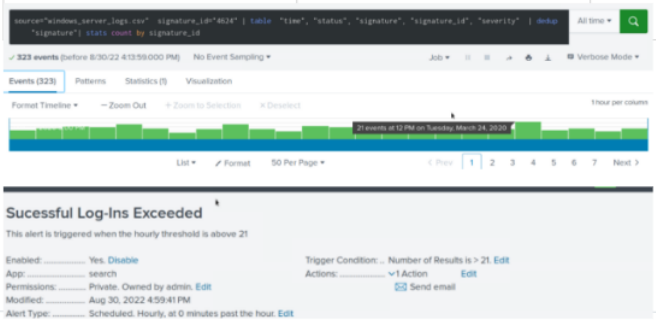
Windows Server Logs:



Alerts—Windows

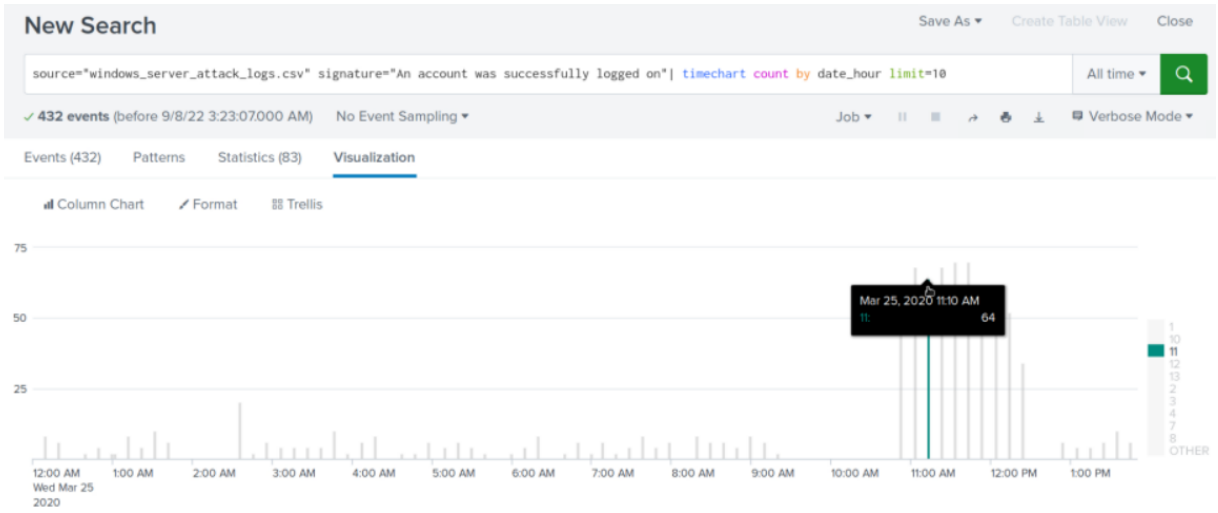
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Logins Exceeded	Notifies VSI when the hourly successful login threshold is	8-21	Above 21



JUSTIFICATION: Hourly failure alerts range from 8-21. We chose to trigger alerts at anything above the threshold of 21 successful logins.

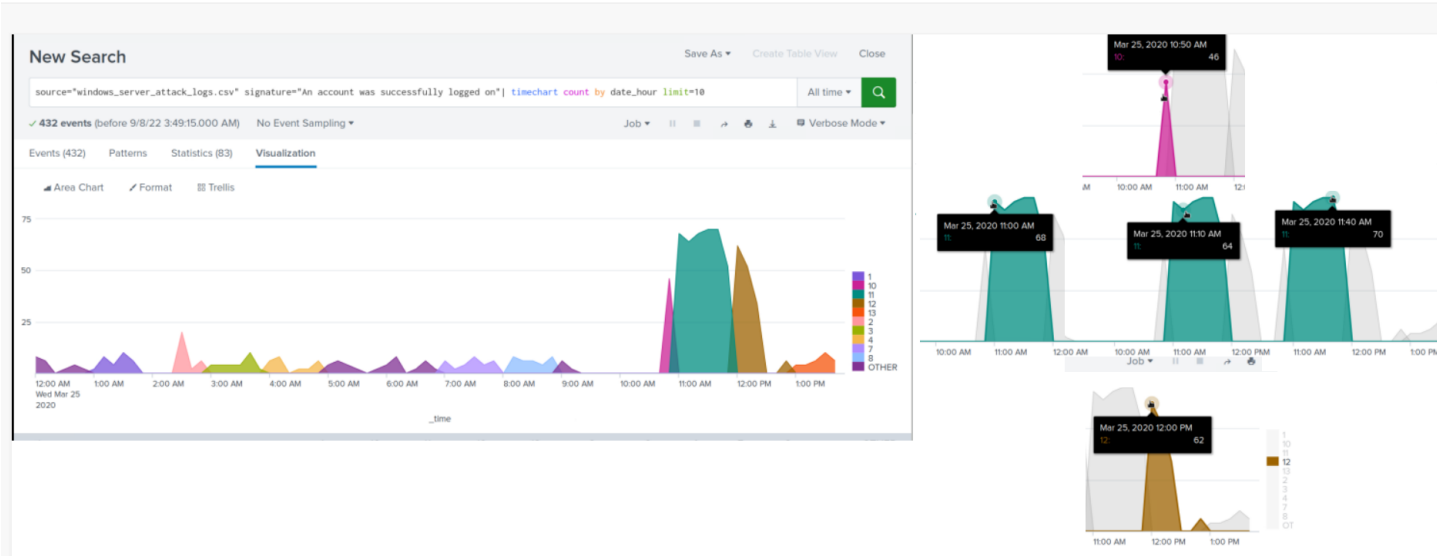
Windows Attacks Logs:



- Did you detect a suspicious volume of successful logins?

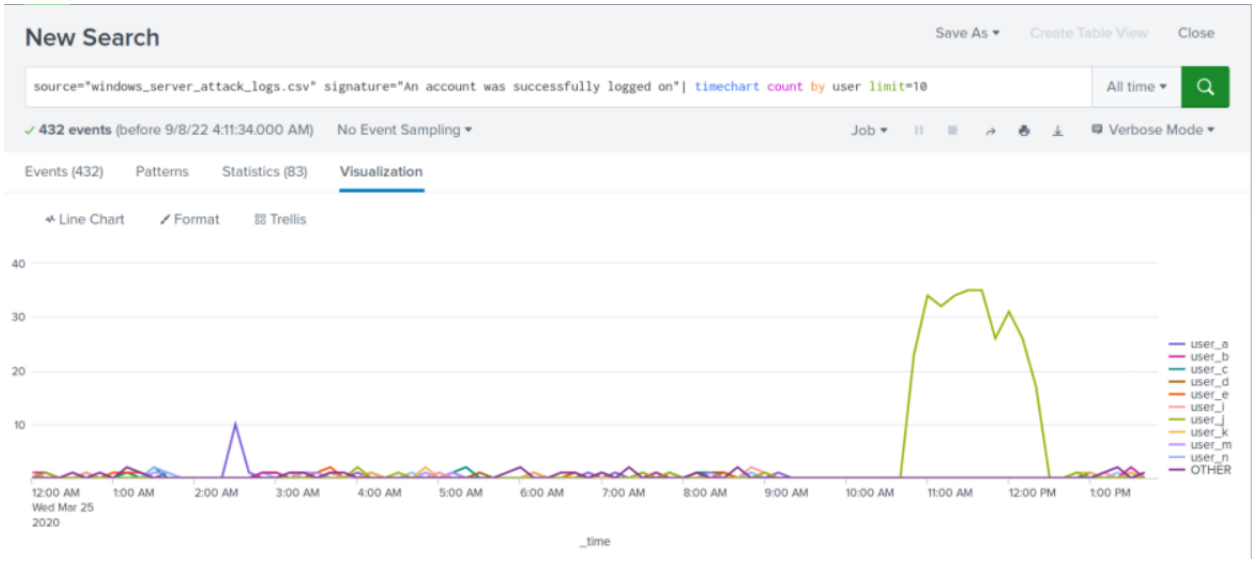
```
From the above screenshots, our alert threshold was set to trigger at any
time the login threshold was above 21 an hour.
```

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



Using the Splunk visualization tool shows that there is a spike of activity beginning around 10:50 AM and 12 PM on Wednesday, March 25th.

- Who is the primary user logging in?

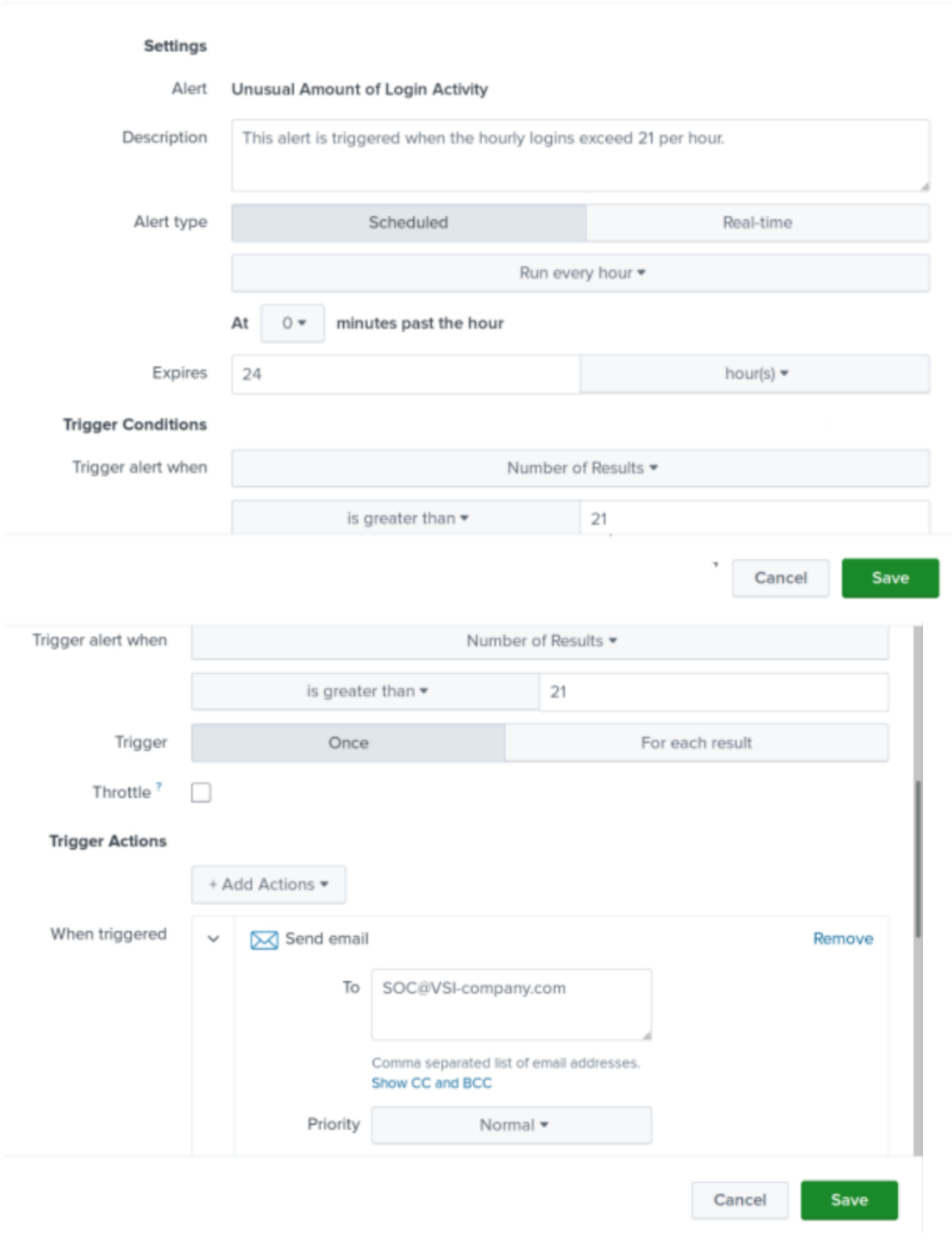


Around the suspicious login activity times observed (between 10:50 AM -12PM) User J is the primary user with the most login attempts around this time.

- When did it occur?

In looking at the provided visualization, user J successful login attempts began at 10:50AM.

- Would your alert be triggered for this activity?



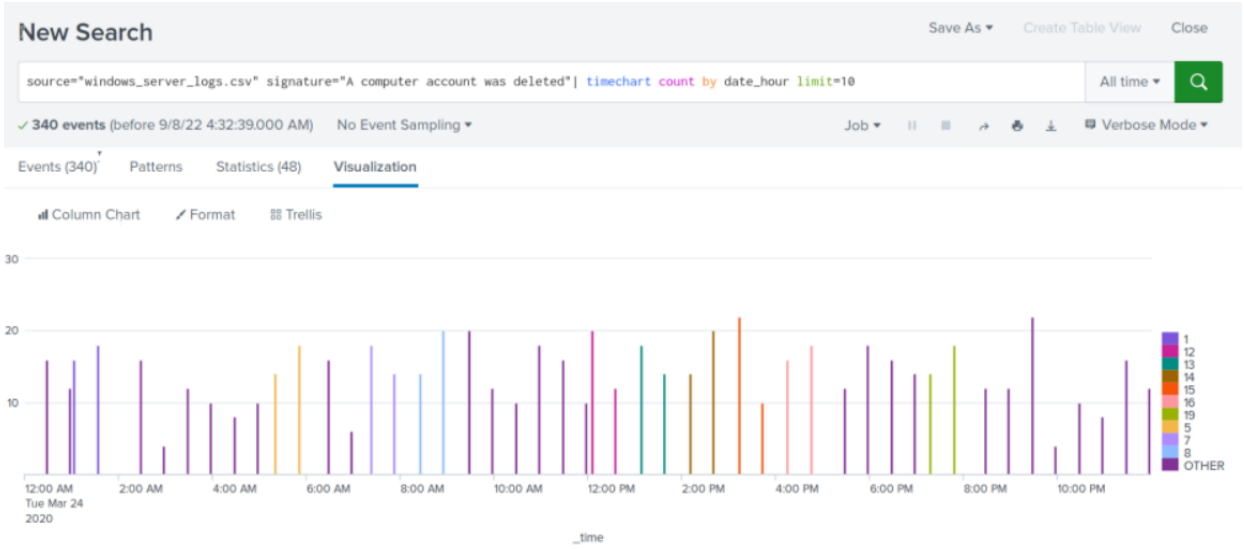
The alert threshold was set to trigger at 21 successful login events/hour.

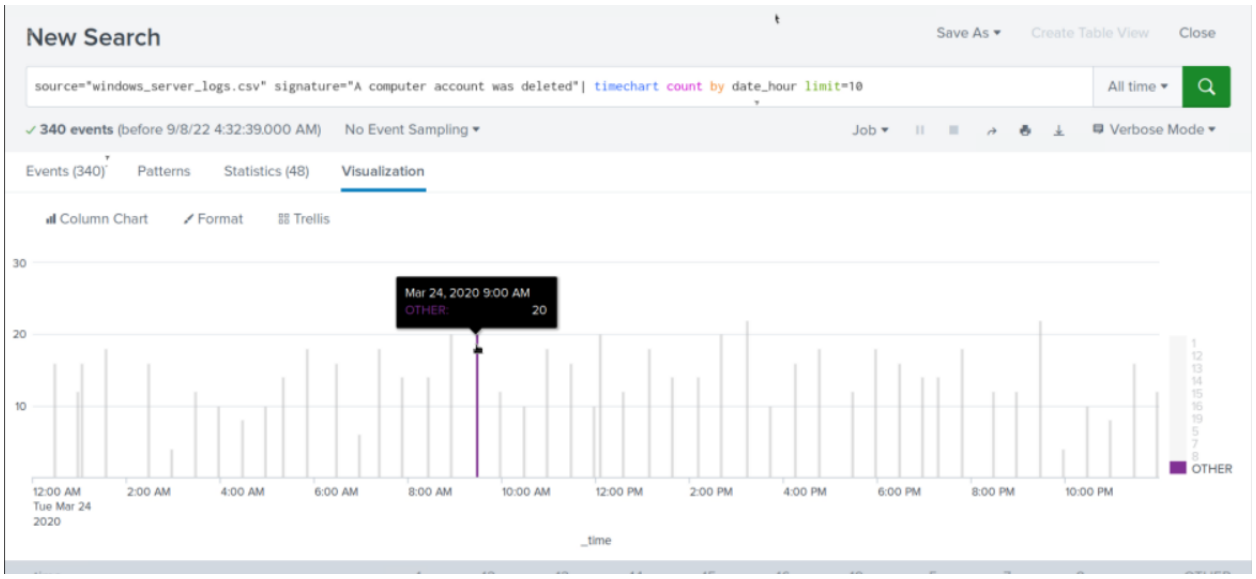
- After reviewing, would you change your threshold from what you previously selected?

```
It appears 21 or 22 is a good current threshold for VSI to currently have in
place for successful login attempts. While alert fatigue is a consideration,
in this case it seems to be a decent threshold.
```

Alert Analysis for Deleted Accounts:

Windows Server Logs:

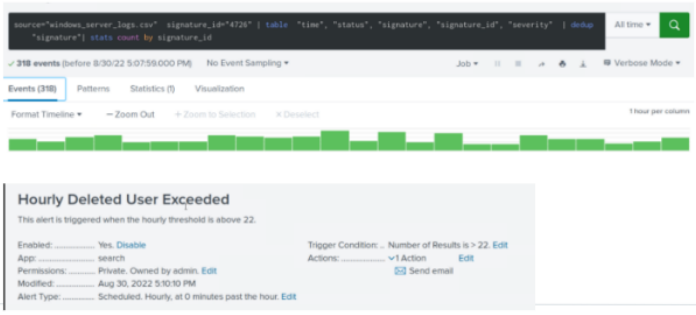




Alerts—Windows

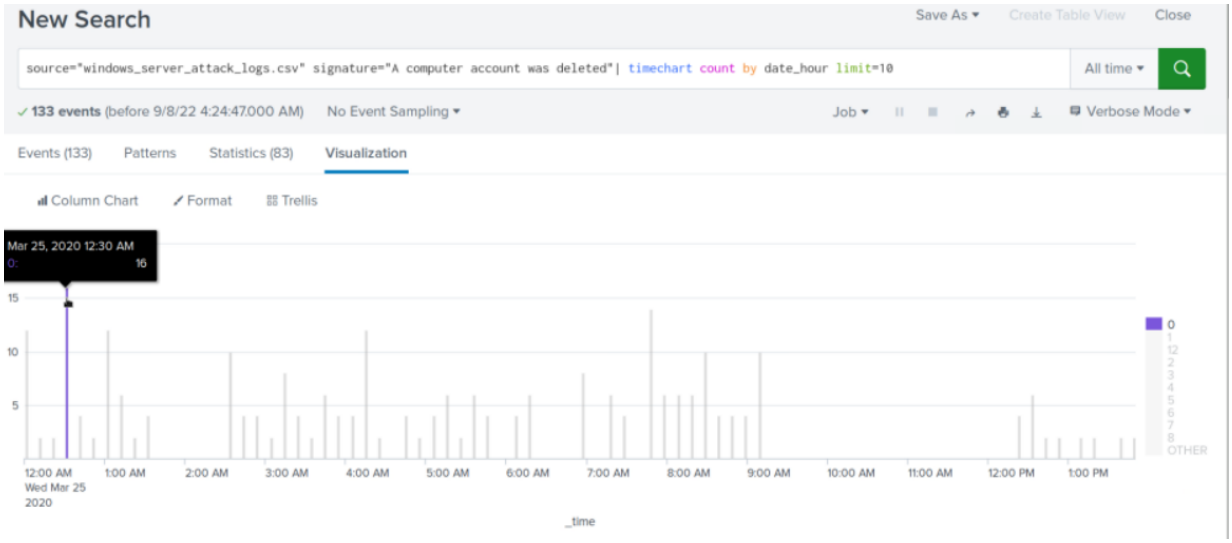
Designed the following alerts:

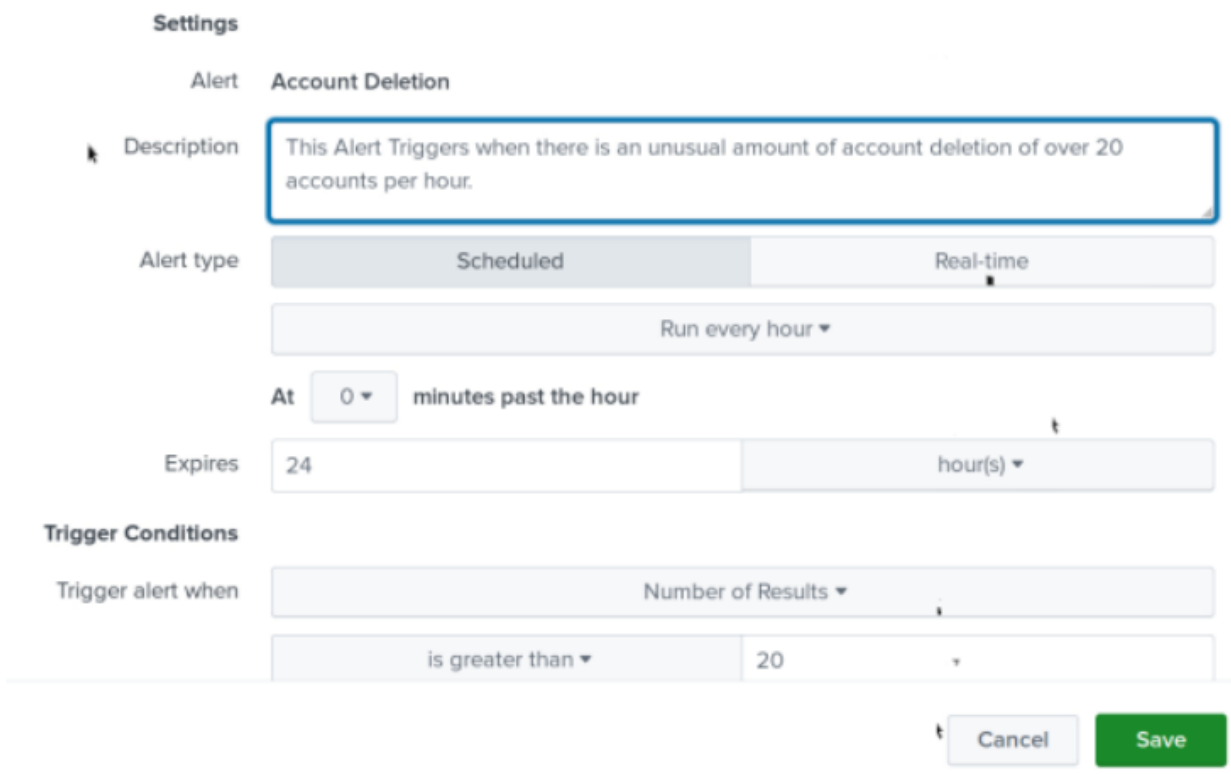
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Accounts Deleted Exceeded	Triggered when the hourly user account deleted threshold is exceeded.	7-22	Above 22

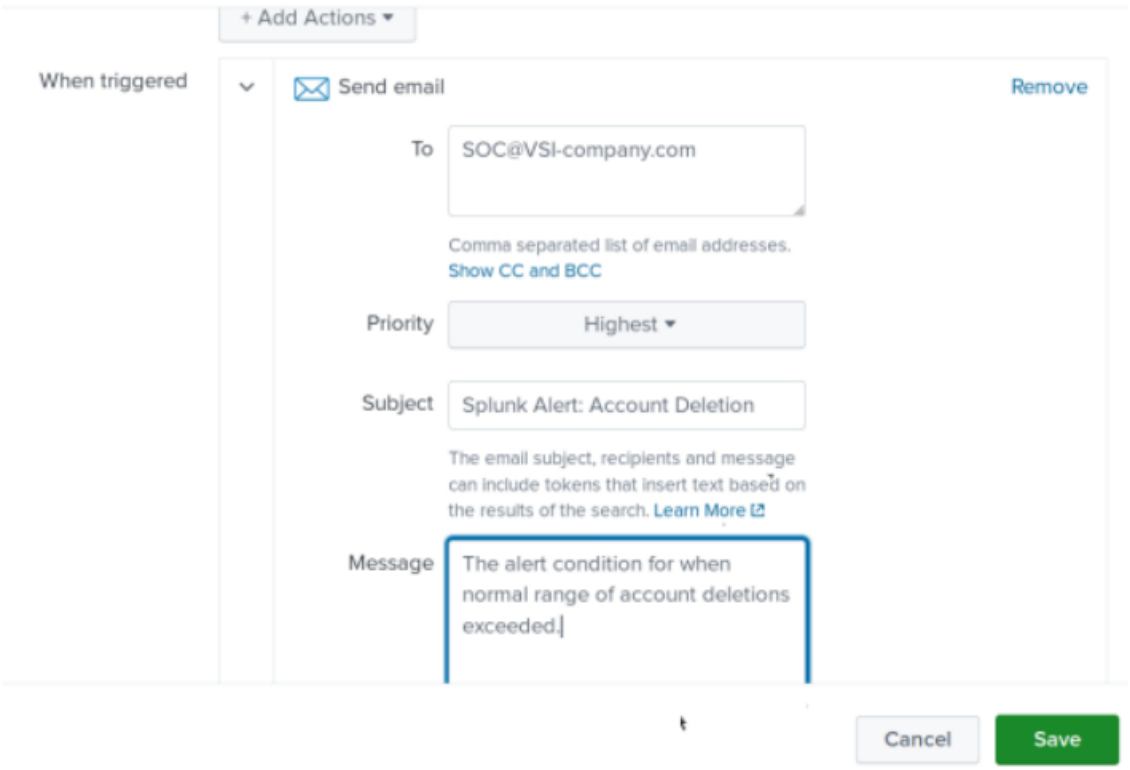


JUSTIFICATION: Hourly failure alerts range from 7-22. We chose to trigger alerts at anything above the threshold of 22 accounts deleted. If too many false positives occur, threshold can always be re-evaluated.

Windows Attack Logs:



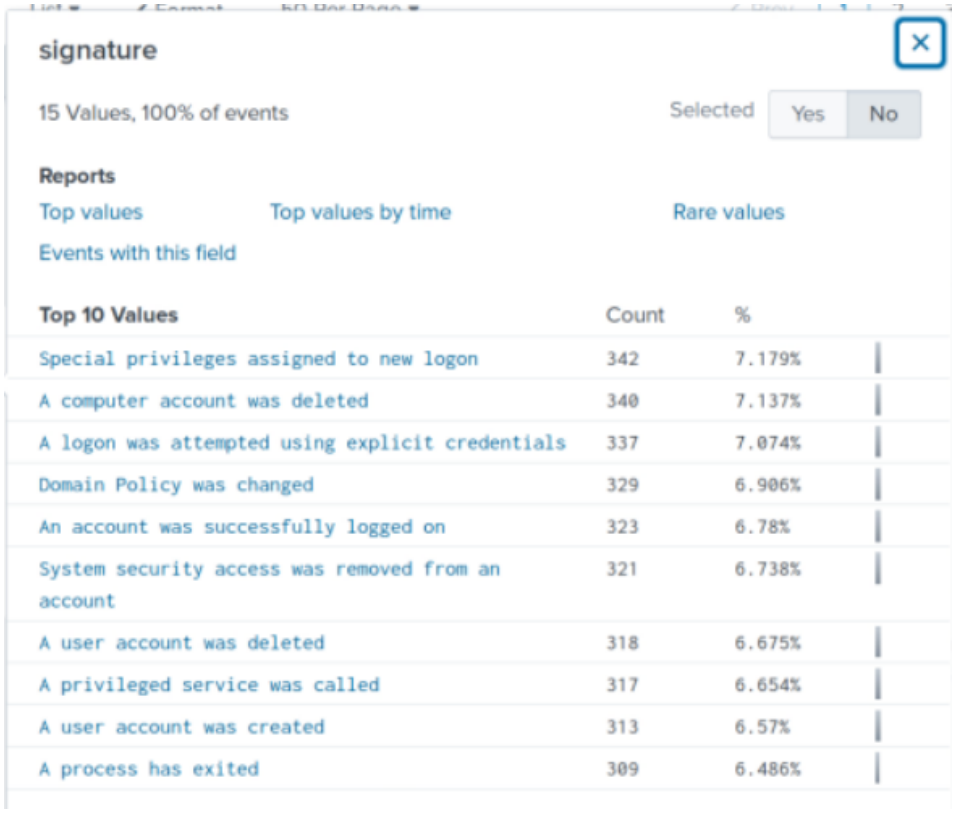


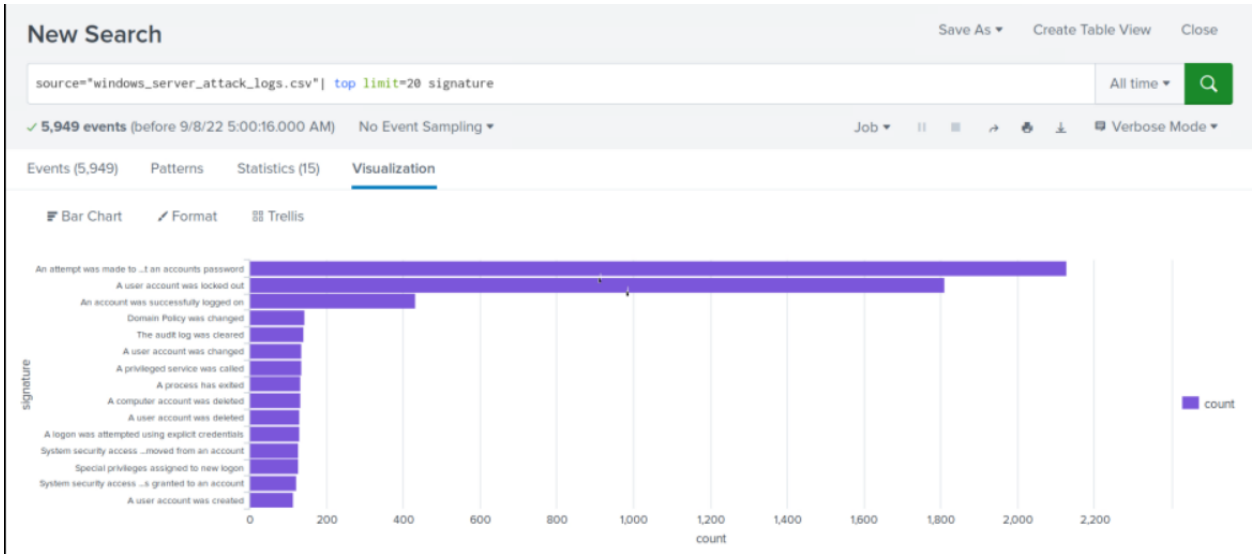


- Did you detect a suspicious volume of deleted accounts?

From the above screenshots, we set our hourly account deletion threshold based on 20 account deletions/ hour. Resultantly, when the windows servers were attacked at 12:30 AM with 16 account deletions, the alert would not have triggered.

Dashboard Analysis for Time Chart of Signatures:





- Does anything stand out as suspicious?

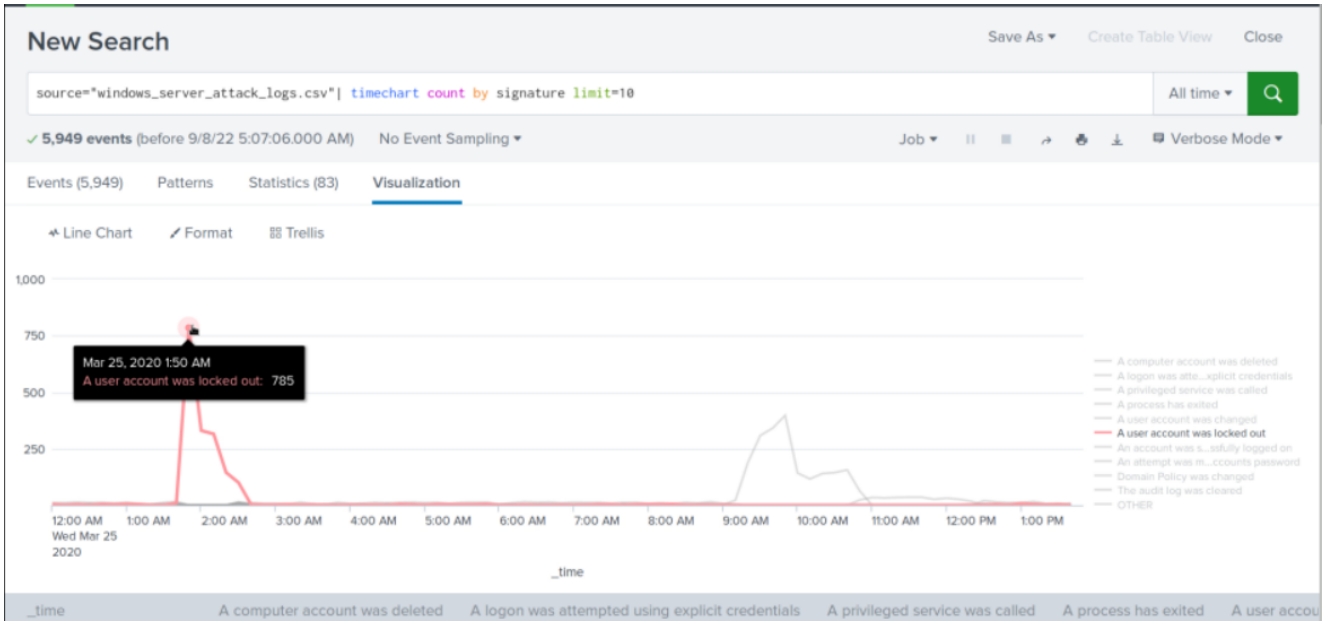
From the above screenshots, in particular the data from the attack logs, both “an attempt was made to reset an accounts password”(35.77%) and “a user

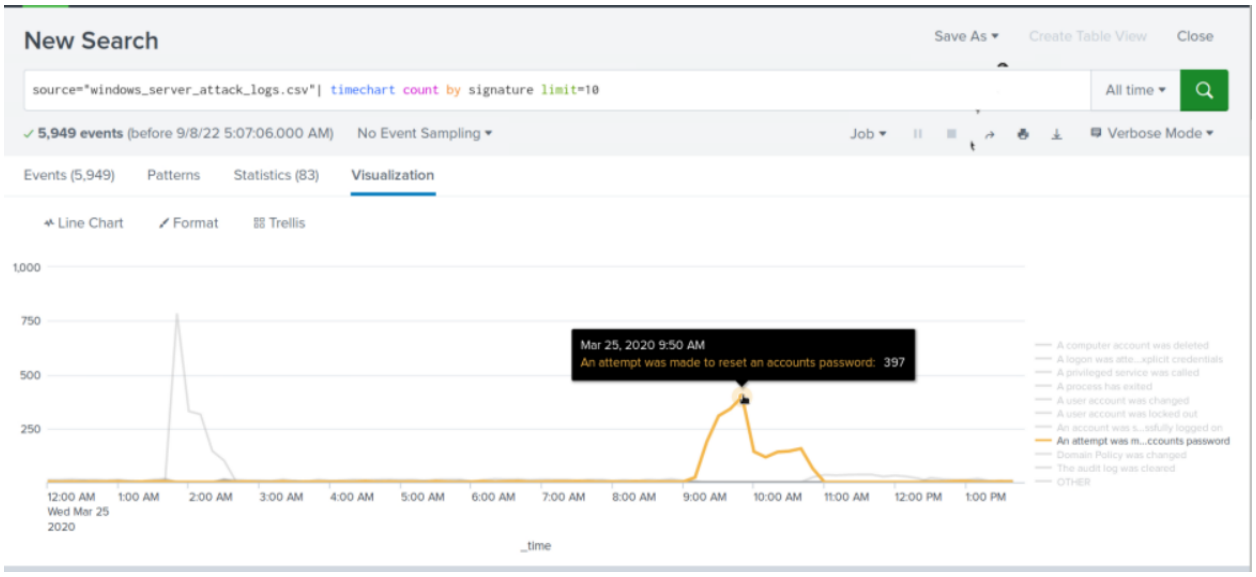
account was locked out”(30.44%) appear as malicious user action. It would also be thorough to include “an account was successfully logged on” (7.26%)

- What signatures stand out?

The two signatures that stand out in particular are :
“an attempt was made to reset an accounts password”
“a user account was locked out”

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





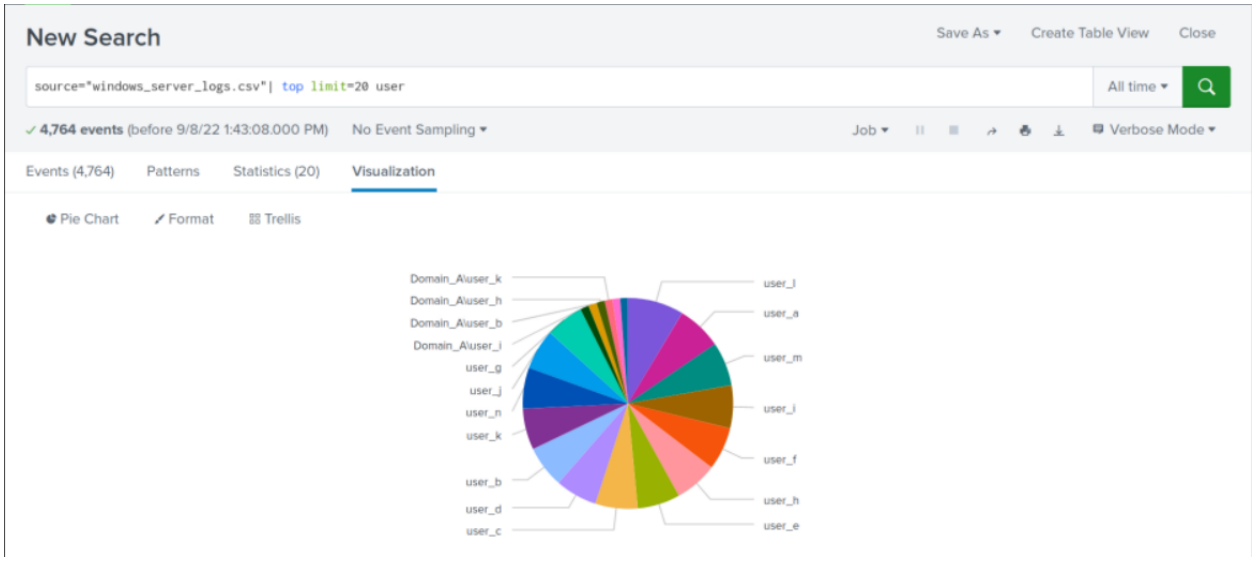
“an attempt was made to reset an accounts password” at 9:30 AM ending at 11 AM
“a user account was locked out” :1:50 AM ending at 3AM

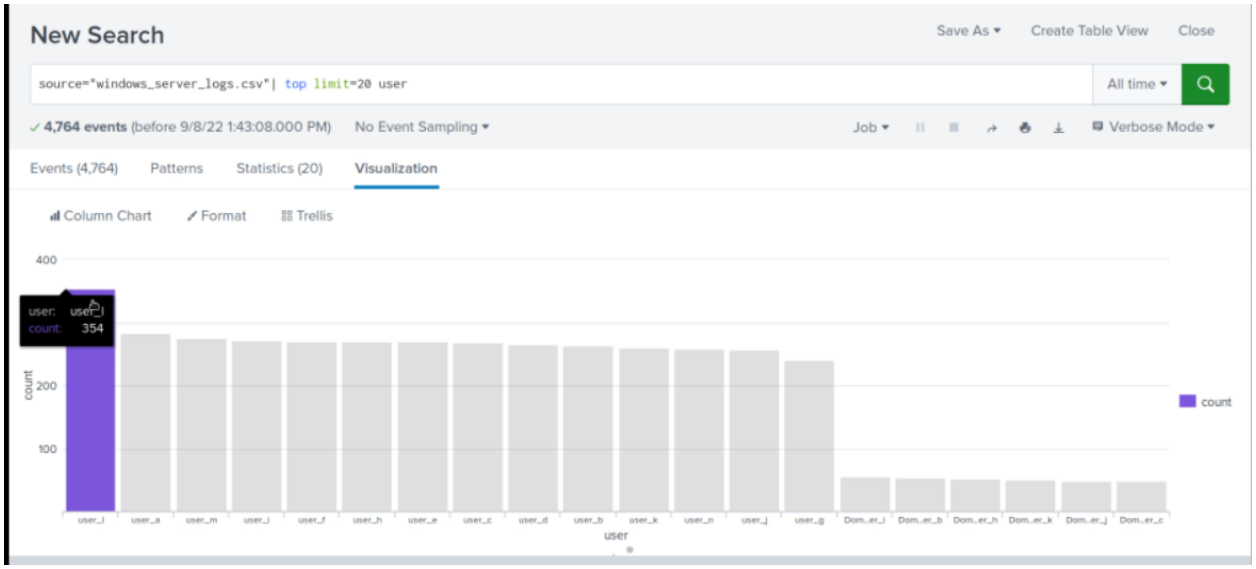
- What is the peak count of the different signatures?

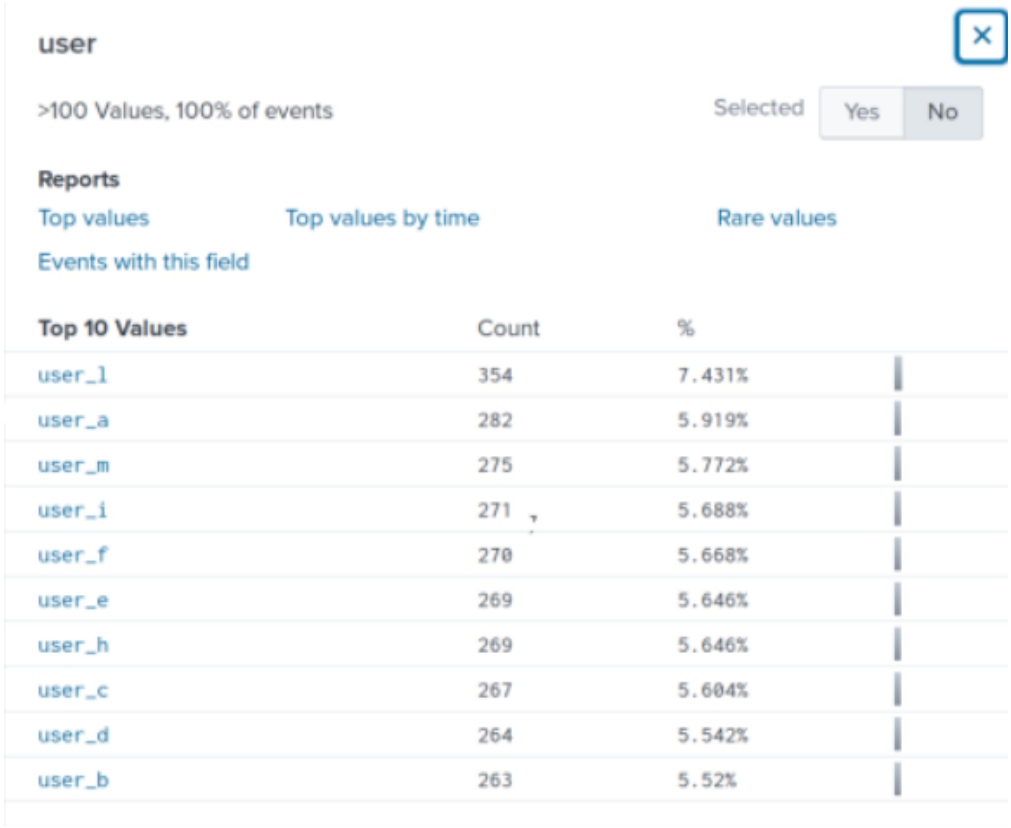
The peak counts for the events are as follows:
“an attempt was made to reset an accounts password”: 785
“a user account was locked out”: 397

Dashboard Analysis for Users :

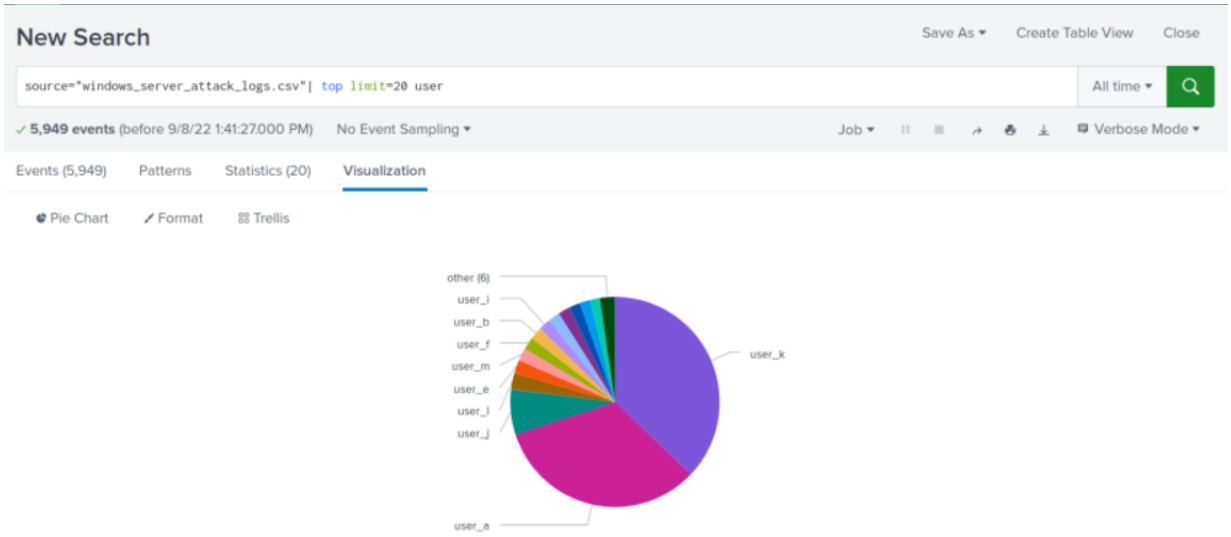
Windows Server Logs:

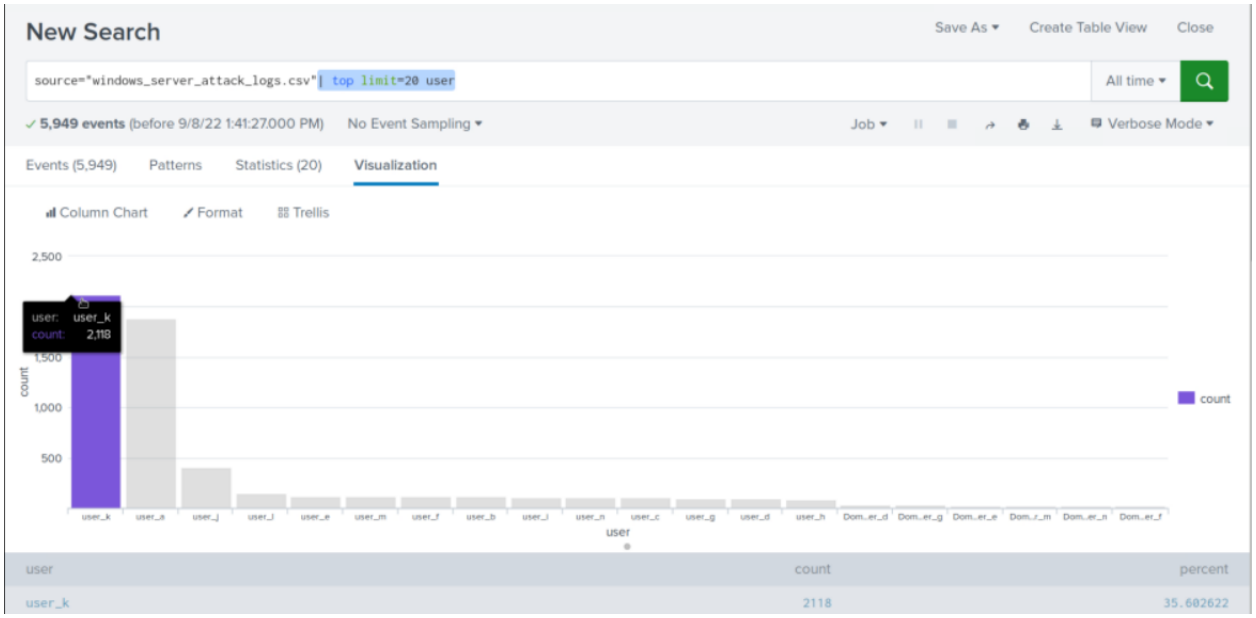


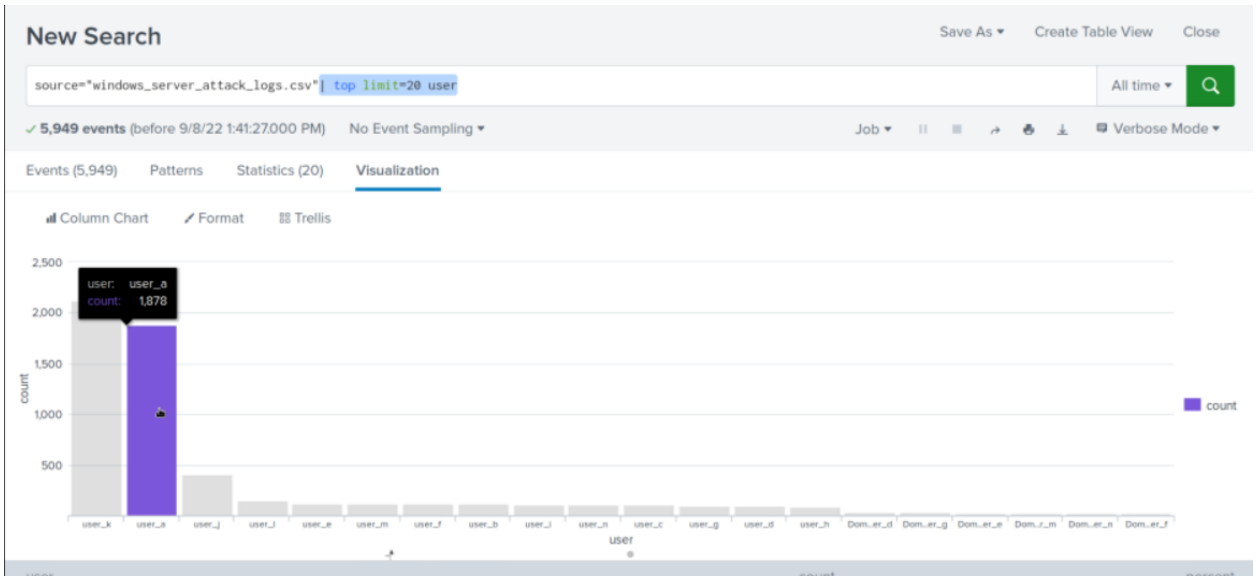


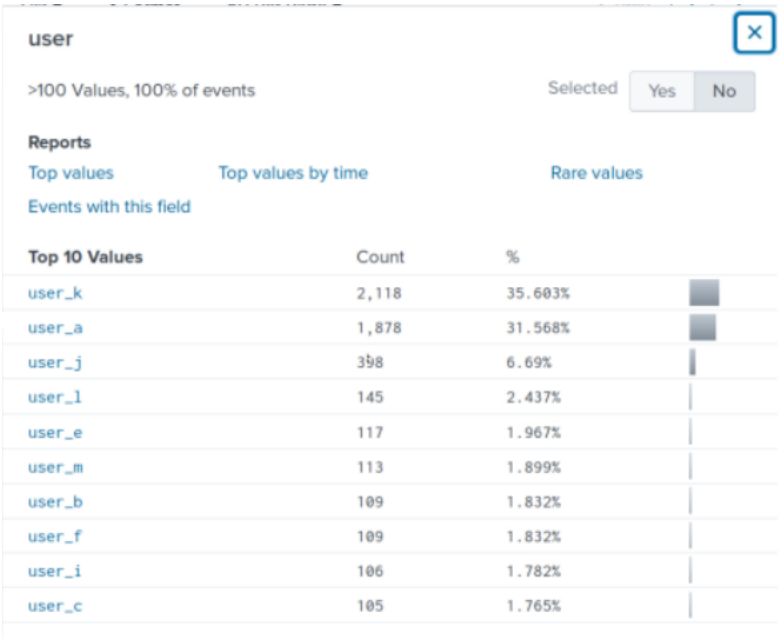


Windows Attack Logs:




New Search
Save As
Create Table View
Close
source="windows_server_attack_logs.csv" | top limit=20 user
All time
5,949 events (before 9/8/22 1:41:27.000 PM)
No Event Sampling
Job
Verbose Mode
Events (5,949)
Patterns
Statistics (20)
Visualization
Column Chart
Format
Trellis
2,500
1,500
1,000
500
count
user: user_k
count: 2,118
count
user
user
count
percent
user_k
2118
35.602622


New Search
Save As
Create Table View
Close
source="windows_server_attack_logs.csv" | top limit=20 user
All time
5,949 events (before 9/8/22 1:41:27.000 PM)
No Event Sampling
Job
Verbose Mode
Events (5,949)
Patterns
Statistics (20)
Visualization
Column Chart
Format
Trellis
2,500
2,000
1,500
1,000
500
count
user: user_a
count: 1,878
count
user

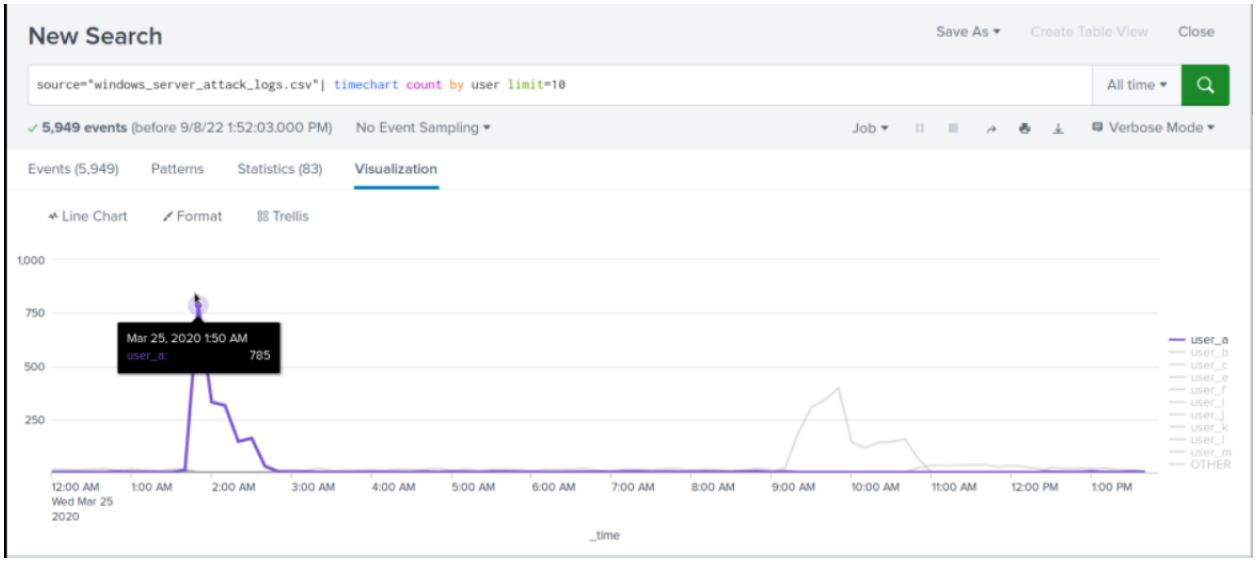


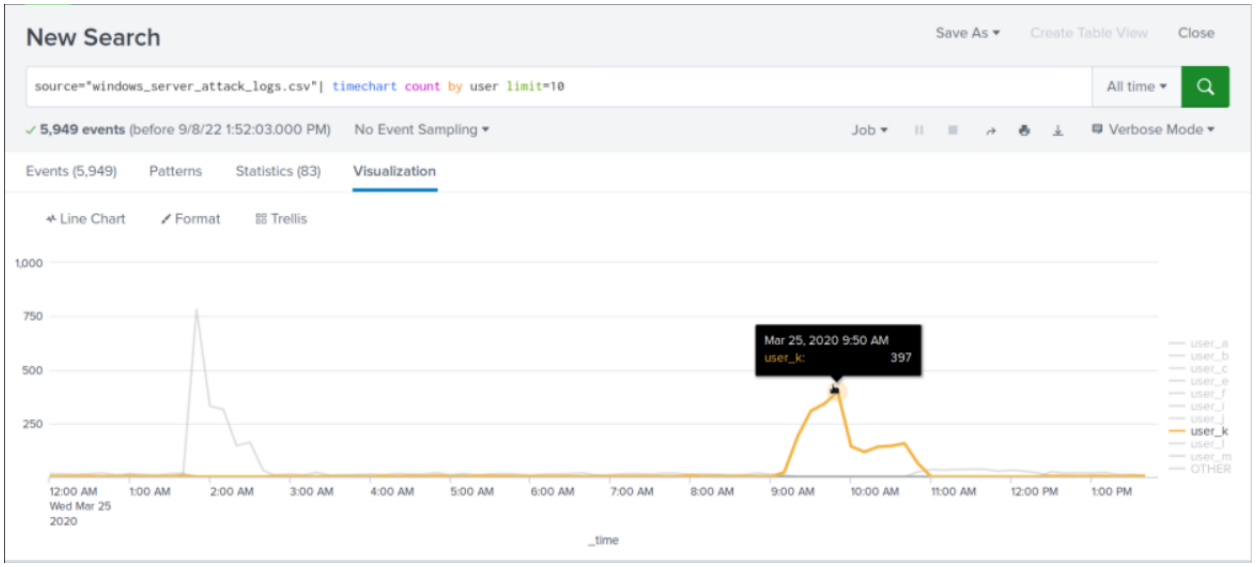
- Does anything stand out as suspicious?

Comparatively speaking,and using the above screenshots, between the window server logs and the attack logs two users appear to be engaged in some malicious activity.

- Which users stand out?

The two users that stand out are User K (user_k) and User A (user_a) with higher event counts than the rest of the user base. Though to be thorough, including User J (user_j) with nearly 2.5x the amount of user activity of the next highest user (user_l)





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

```
For User A: 1AM ending at 3AM
For User K : 9AM ending at 11AM
```

- What is the peak count of the different users?

```
From the above screenshots, the peak counts of user activity is:
User A: 785
User K: 397
```

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

- Does anything stand out as suspicious?

```
Yes, the user profiles match the malicious signature activity.
```

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

```
Yes, in looking at the screenshots there is a correlation in activity with
user profiles.
```

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

- Does anything stand out as suspicious?

```
Yes, the two users (User A and User K) that have increased event activity
count correlate with the malicious signature activity.
```

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

```
Yes, from the previous screenshots of the attack logs reveal that the user
activity uncovered in this section correlates with the malicious signatures
in the previous section.
```

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?

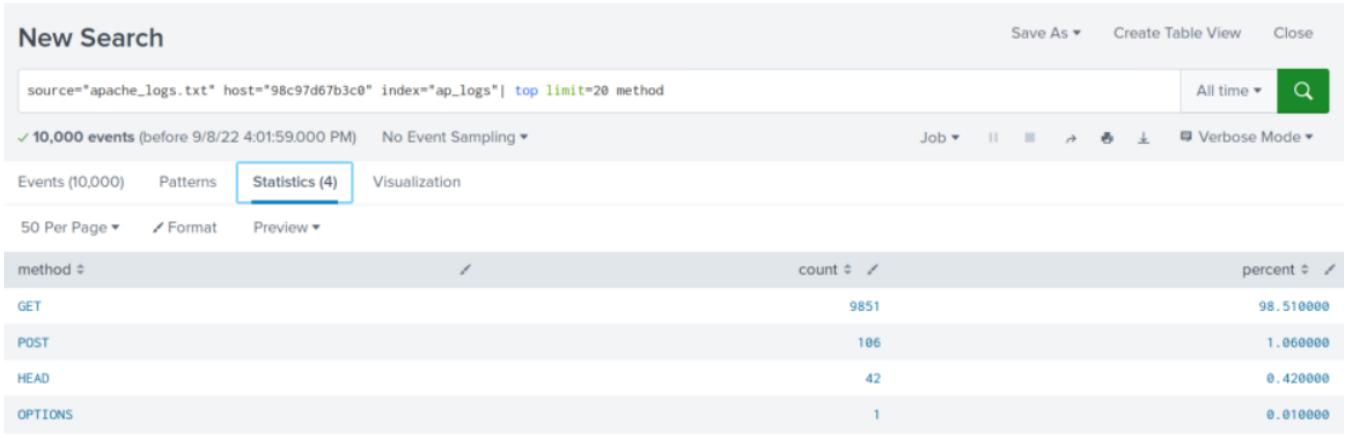
```
Splunk does a great job at organizing and visualizing data. You can easily
keep on drilling down on insights that could allow you to custom tailor
firewall rules for example. For example it is relatively easy looking at the
count of events that User A and K are problematic users within the system.
However, while A and K are noisy user profiles, this does not uncover more
stealthy malicious user activity such as successful logins with stolen
credentials. It would also be prudent to monitor some other signatures such
as a privilege service was called .More stealthy malicious users could be
using something along the lines of a cronjob to escalate their privileges in
```

VSI's environment, along with erasing their trace by modifying or erasing the system logs. It's good to keep an eye on the system as a whole and not just those components with statistical noise.

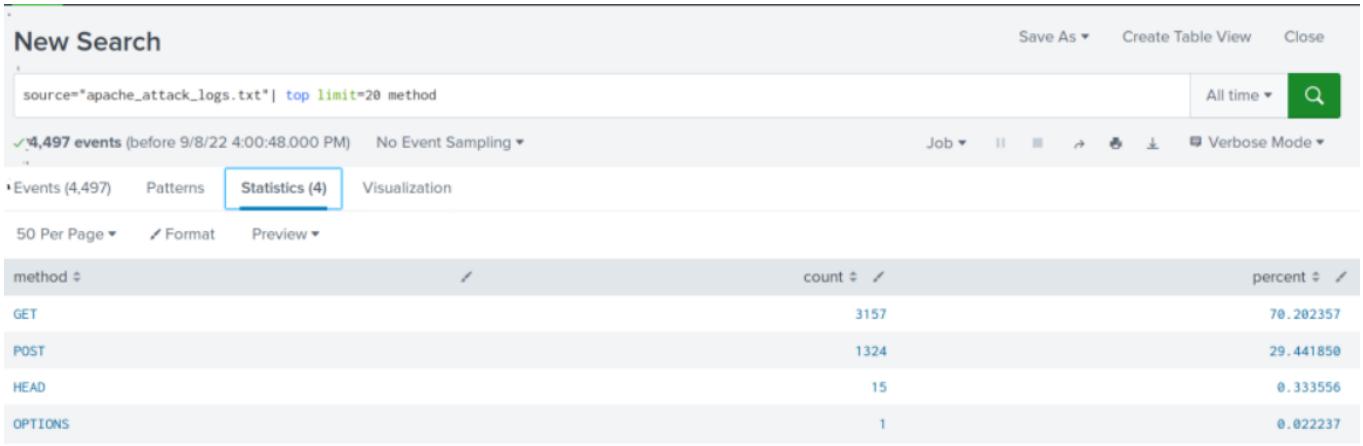
Apache Web Server Log Questions

Report Analysis for Methods:

Apache Logs:



Apache Attack Logs:



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

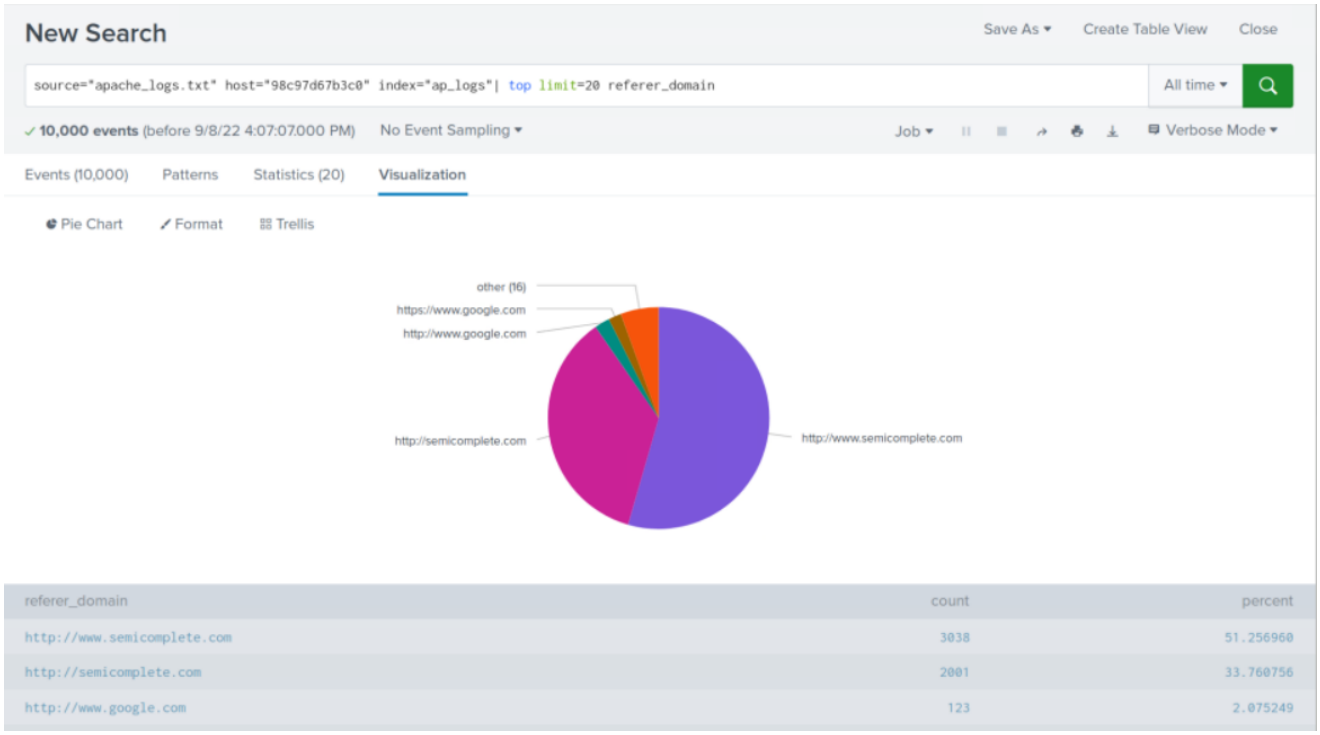
```
Yes, there is a suspicious change in HTTP methods, in particular the POST
method that saw and increase from 106 (1.06%) to 1324 (29.44%)
```

- What is that method used for?

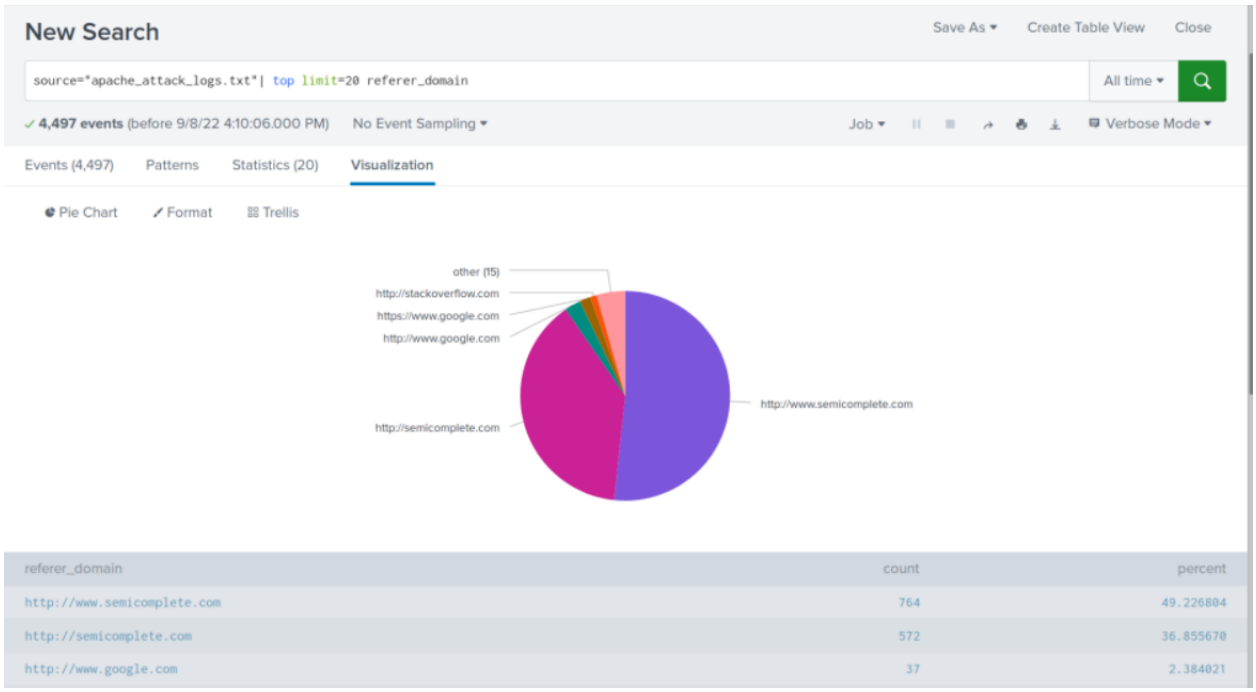
```
The POST method sends data to a server and is then used to create and update
a resource.
```

Report Analysis for Referrer Domains:

Apache Logs:



Apache Attack Logs:

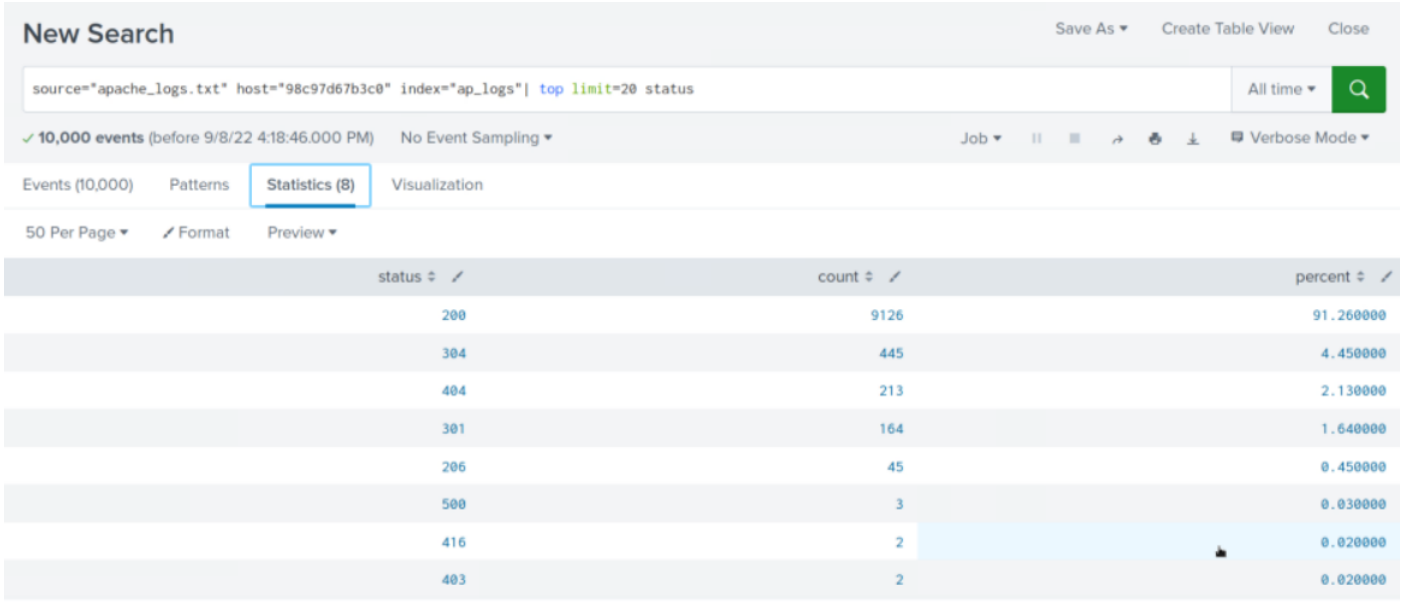


- Did you detect any suspicious changes in referrer domains?

There were no major suspicious changes in referrer domains between the Apache logs and the Apache attack logs. In the Apache logs, www.semicomplete.com accounted for 51.25% of traffic with http://semicomplete.com 33.76% representing the majority of traffic. In the attack logs www.semicomplete.com accounted for 49.22% and http://semicomplete.com 36.65% of all incoming traffic

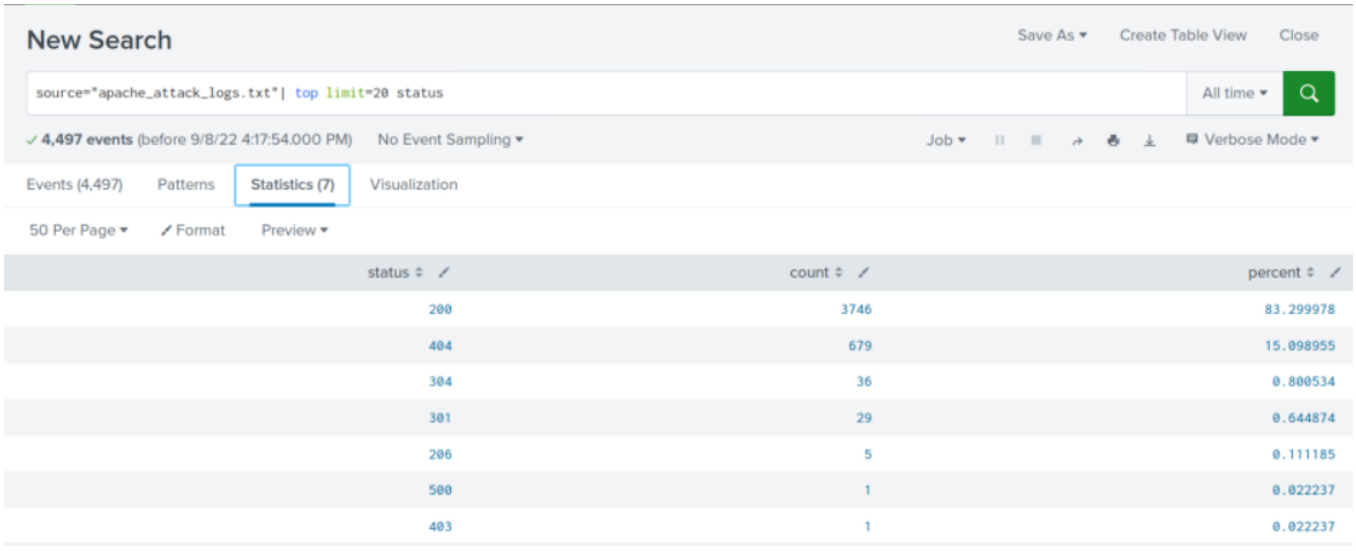
Report Analysis for HTTP Response Codes:

Apache Logs:



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

Apache Attack Logs:



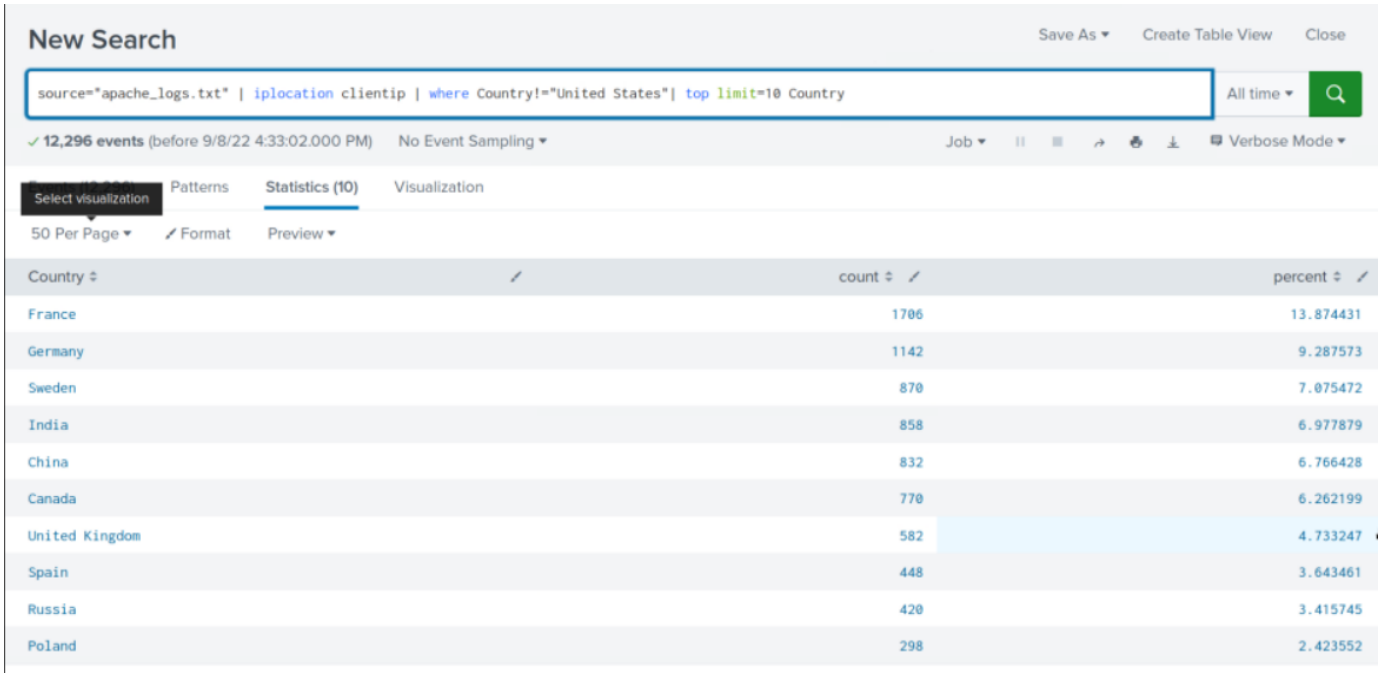
status	count	percent
200	3746	83.299978
404	679	15.098955
304	36	0.800534
301	29	0.644874
206	5	0.111185
500	1	0.022237
403	1	0.022237

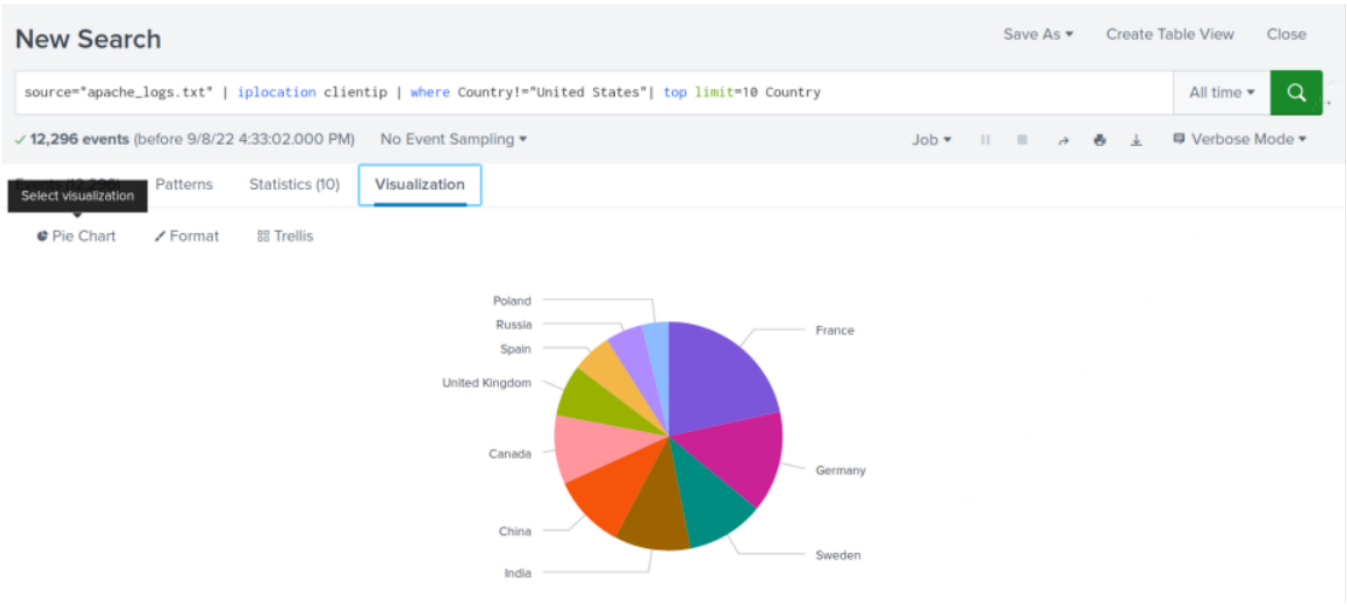
- Did you detect any suspicious changes in HTTP response codes?

The most crucial change in the response codes is the amount of 404, or file/page not found. The amount of 404 response code increased from 2.13% in the Apache logs to 15.09% in the Apache attack logs. Equally, the 200 response code decreased from 91.26% in the Apache logs to 83.29% in the attack logs.

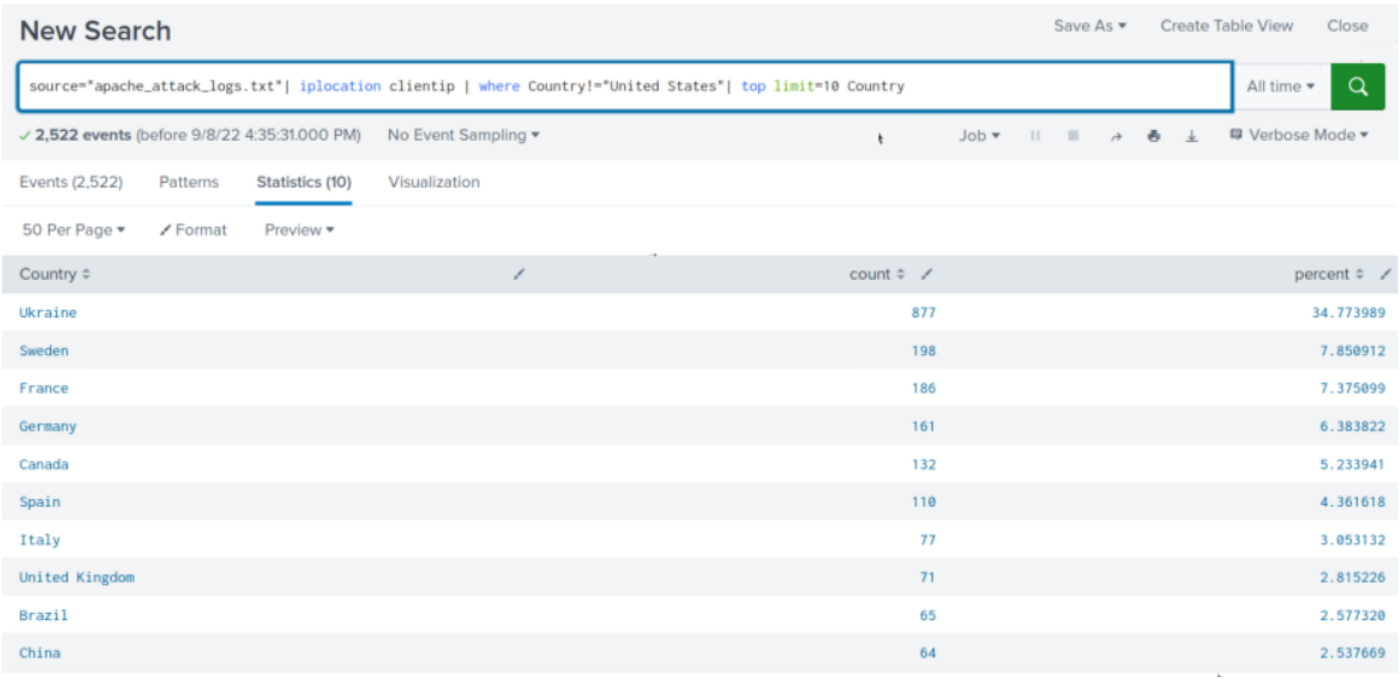
Alert Analysis for International Activity:

Apache Logs:

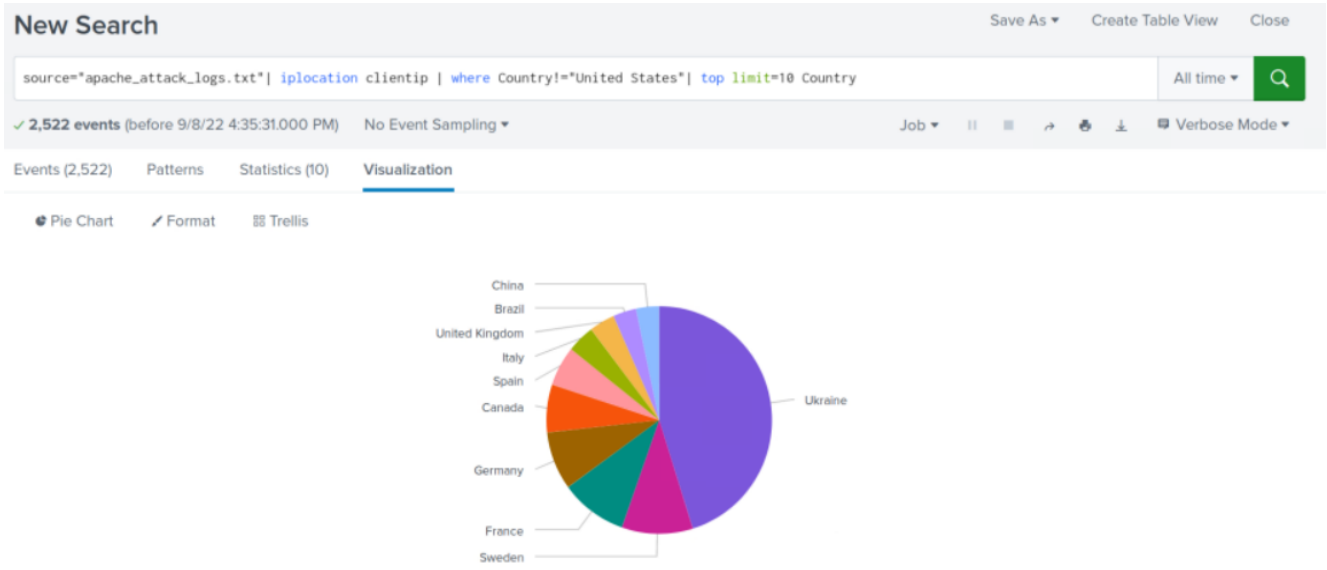




Apache Attack Logs:



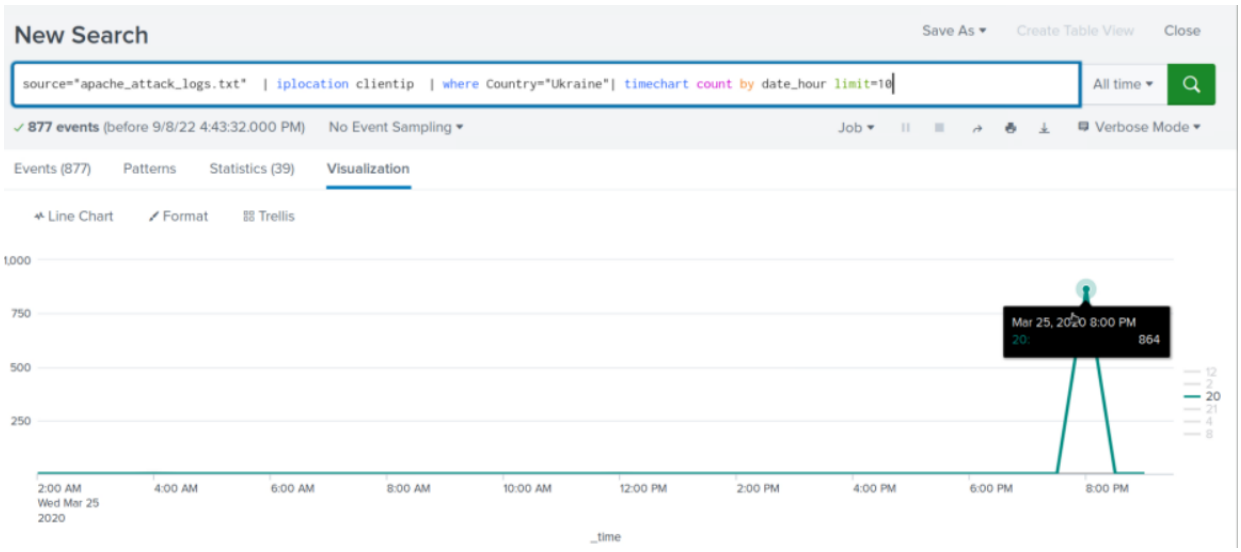
Country	count	percent
Ukraine	877	34.773989
Sweden	198	7.850912
France	186	7.375099
Germany	161	6.383822
Canada	132	5.233941
Spain	110	4.361618
Italy	77	3.053132
United Kingdom	71	2.815226
Brazil	65	2.577320
China	64	2.537669

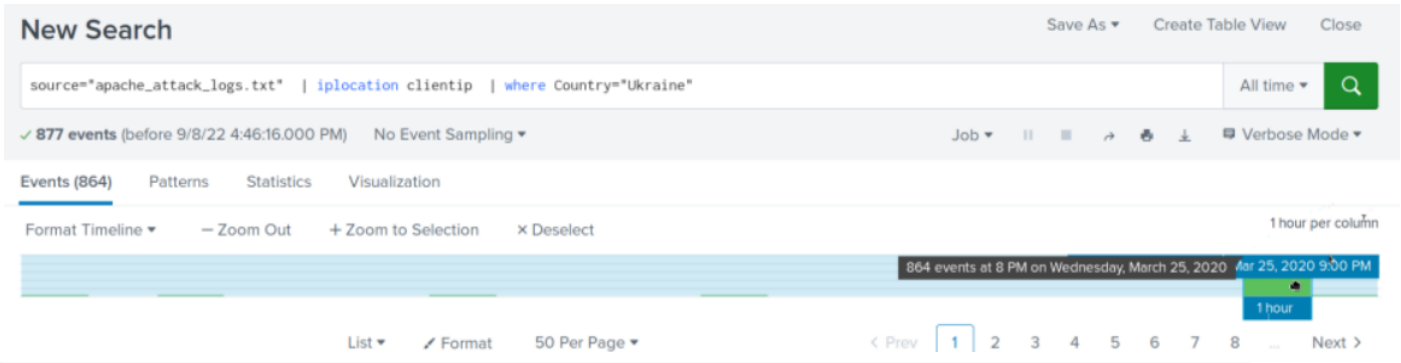


- Did you detect a suspicious volume of international activity?

From the Apache logs to the Apache attack logs there appears to be an increase in activity from the Ukraine.

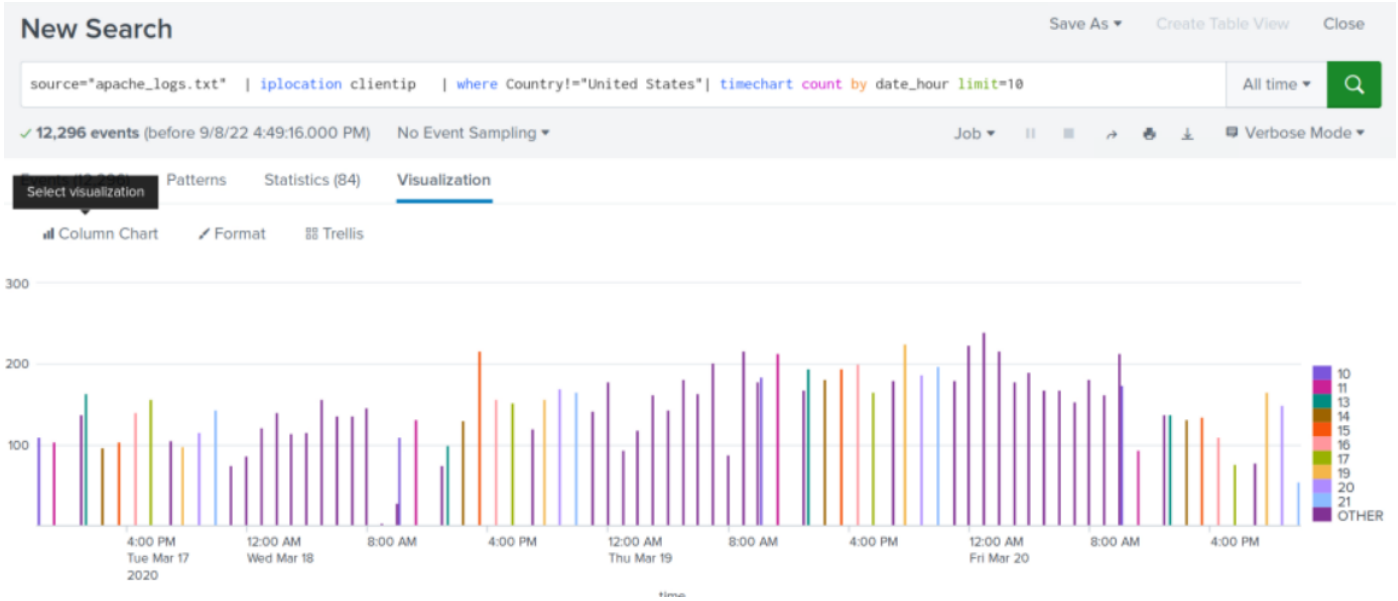
- If so, what was the count of the hour(s) it occurred in?

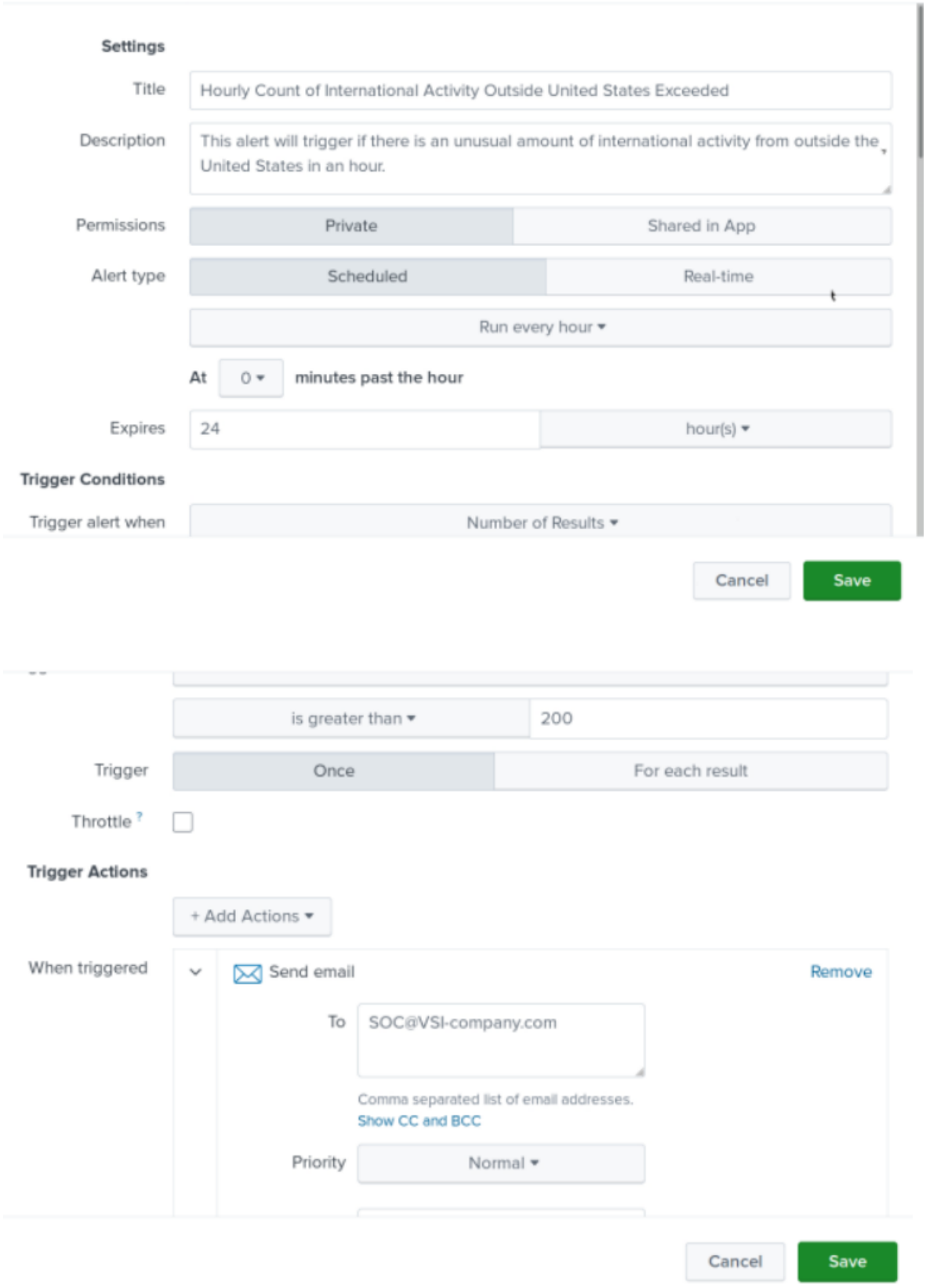




The activity from the Ukraine spikes at 8 PM on Wednesday March 25th,2020 with 864 events.

- Would your alert be triggered for this activity?




Settings
Title
Hourly Count of International Activity Outside United States Exceeded
Description
This alert will trigger if there is an unusual amount of international activity from outside the United States in an hour.
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Run every hour
At
0
minutes past the hour
Expires
24
hour(s)
Trigger Conditions
Trigger alert when
Number of Results
Cancel
Save
is greater than
200
Trigger
Once
For each result
Throttle
Trigger Actions
+ Add Actions
When triggered
Send email
Remove
To
SOC@VSI-company.com
Comma separated list of email addresses.
Show CC and BCC
Priority
Normal
Cancel
Save

```
Yes, as the threshold was set at 200 events/hour.
```

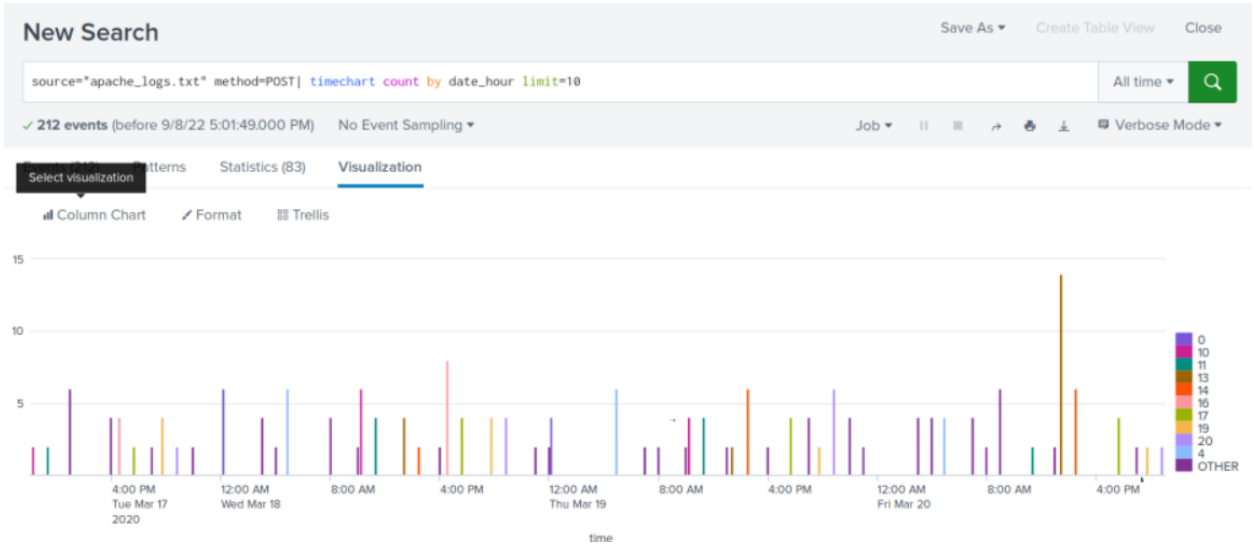
- After reviewing, would you change the threshold that you previously selected?

```
No, as the events for the surge in the increased Ukrainian activity would
have met our threshold of 200 events/hour
```

Alert Analysis for HTTP POST Activity:

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

Apache Logs:



Settings

Title: Unusual Number of POST Requests

Description: This alert will trigger if there are an unusual amount of POST requests made within an hour

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Run every hour

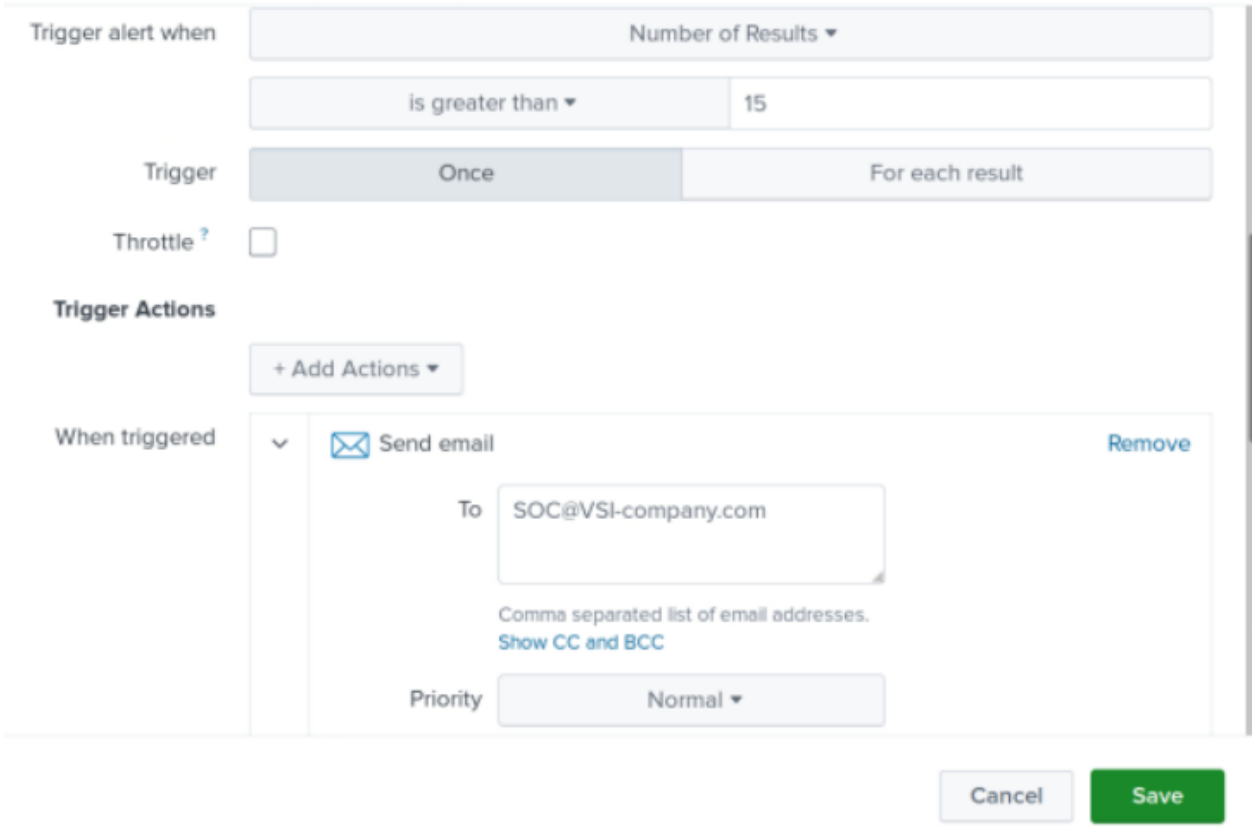
At 0 minutes past the hour

Expires: 24 hour(s)

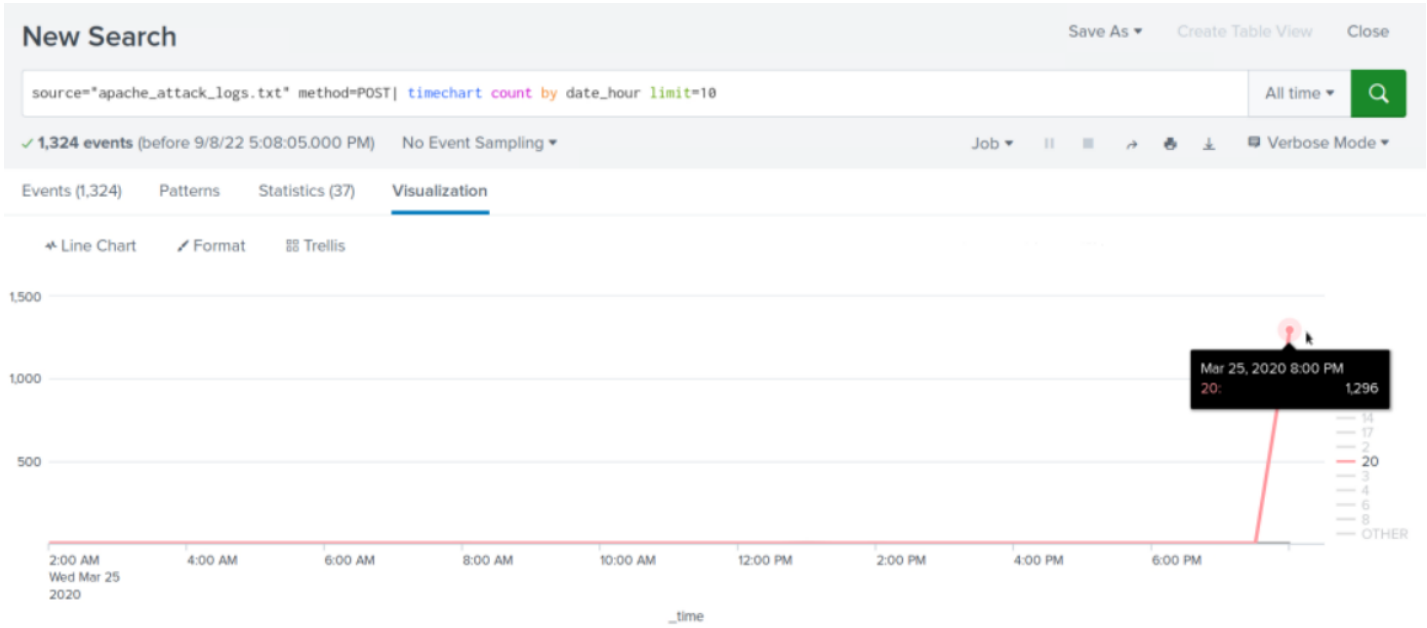
Trigger Conditions

Trigger alert when: Number of Results

Cancel Save



Apache Attack Logs:



From the Apache logs we set the threshold of POST method requests to alert if POST method requests exceeded 15/hour. The alert would trigger as there was a peak of 1296 events.

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

The count of the POST method request was 1296 events.

- When did it occur?

The attack using the POST method occured at 8 PM

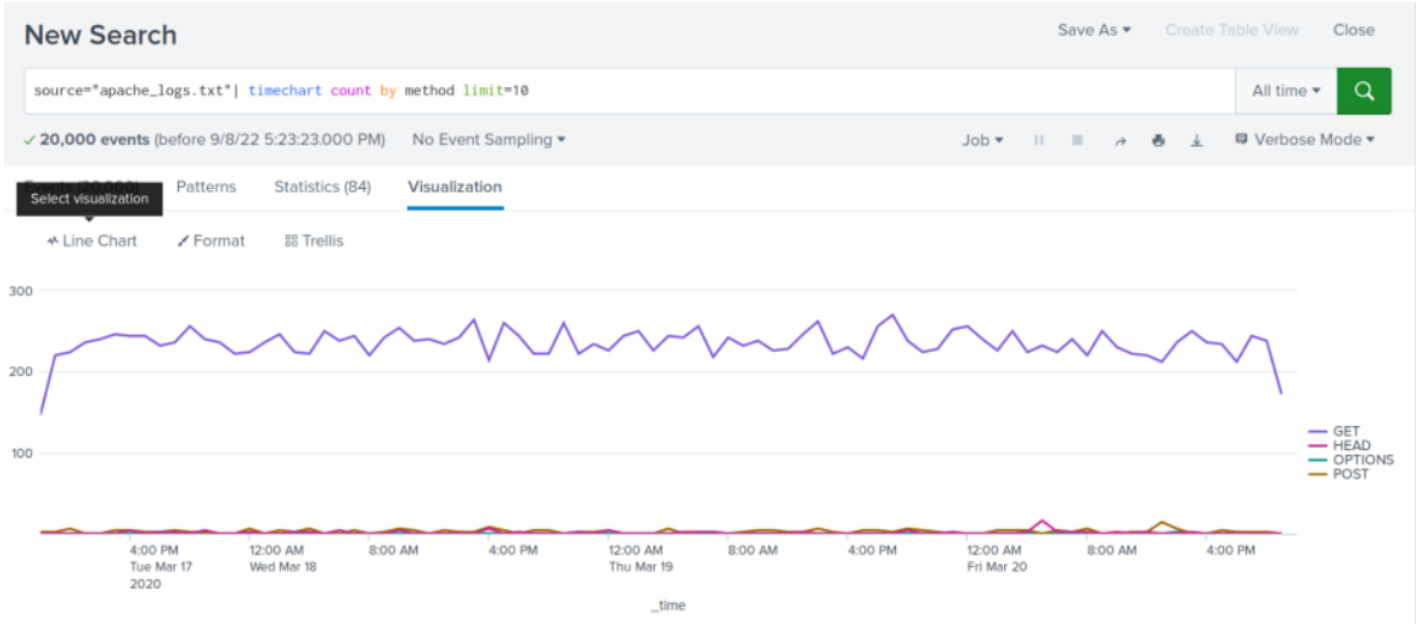
- After reviewing, would you change the threshold that you previously selected?

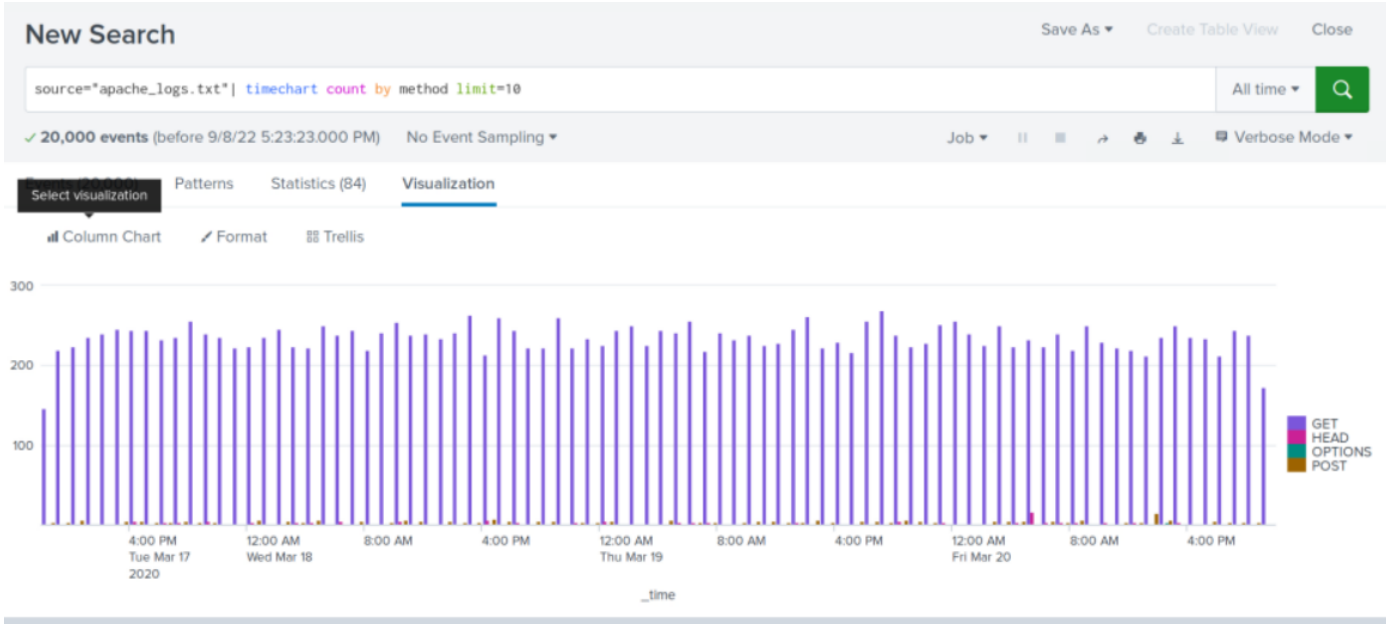
No, as our alert would have triggered with the base of 15/hour.

Dashboard Analysis for Time Chart of HTTP Methods:

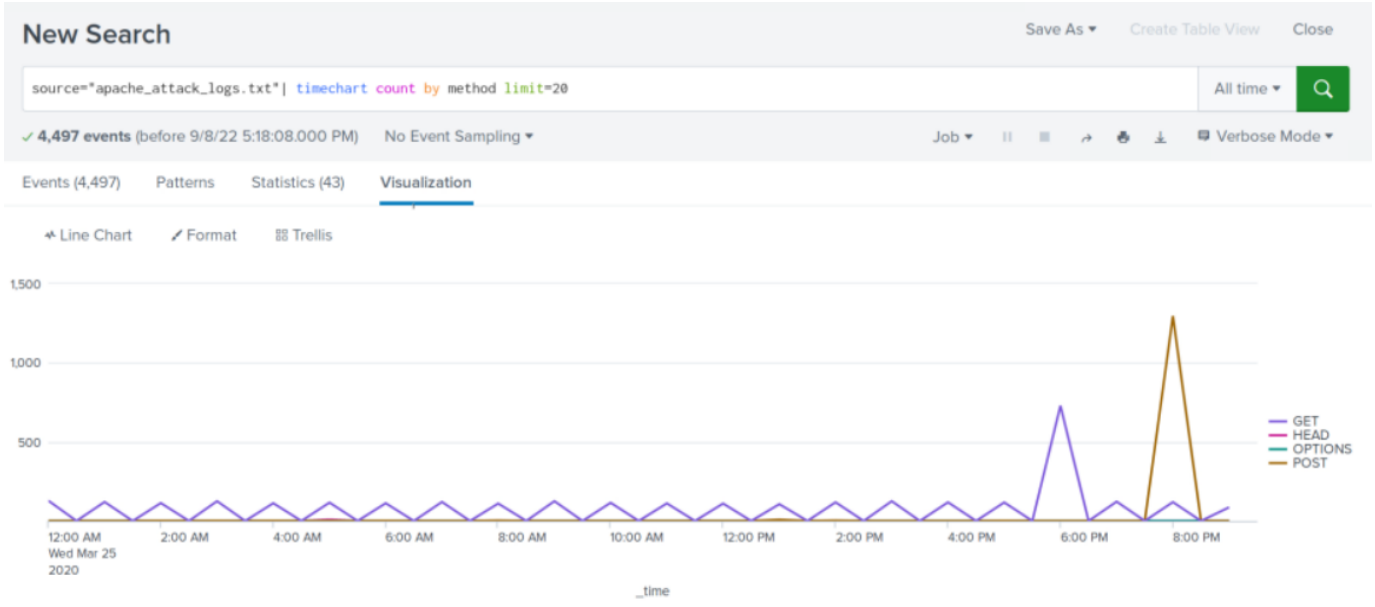
- Does anything stand out as suspicious?

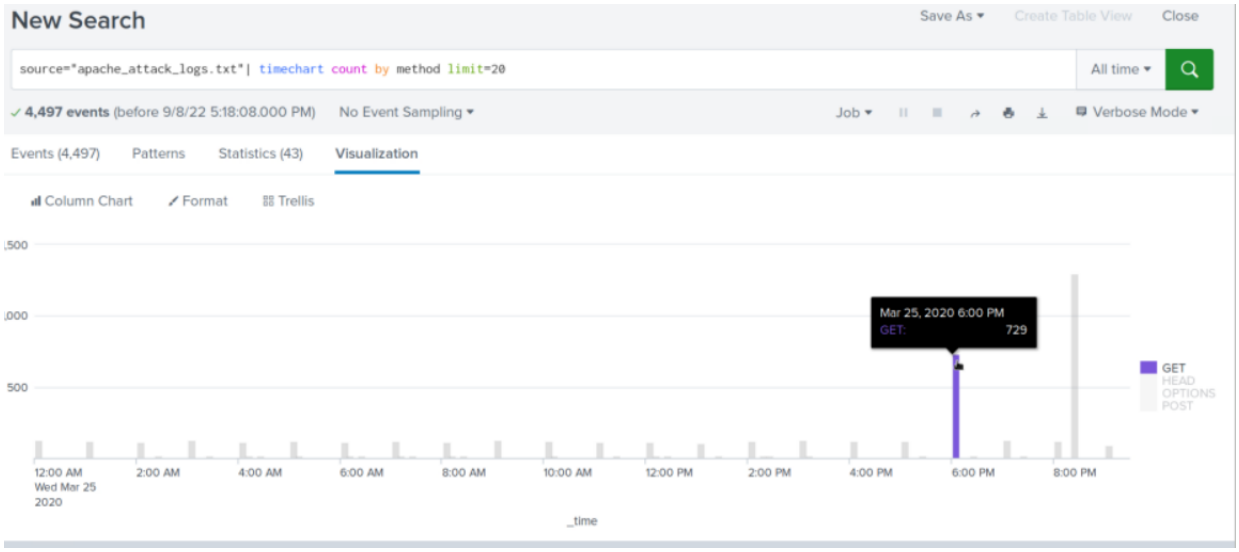
Apache Logs:

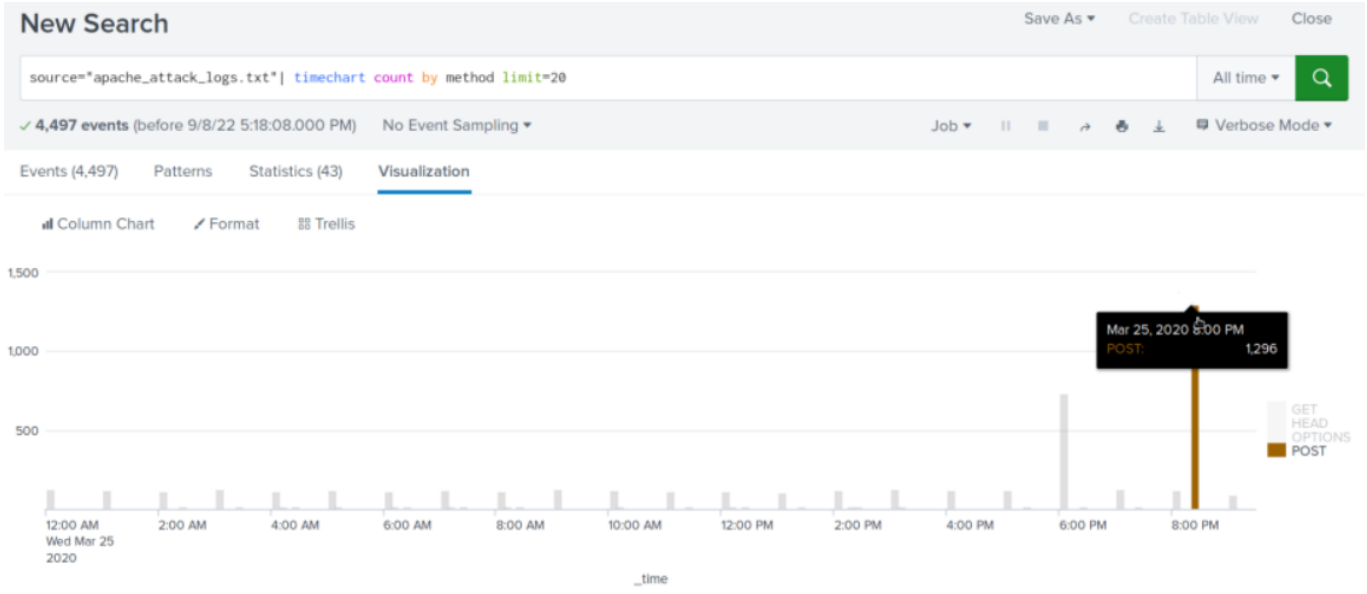




Apache Attack Logs:







Comparatively speaking, in the attack logs, the use of both the GET and POST methods seem suspicious.

- Which method seems to be used in the attack?

The POST method is used for attack.

- At what times did the attack start and stop?

```
The attack started at 8PM and ended at 9PM.
```

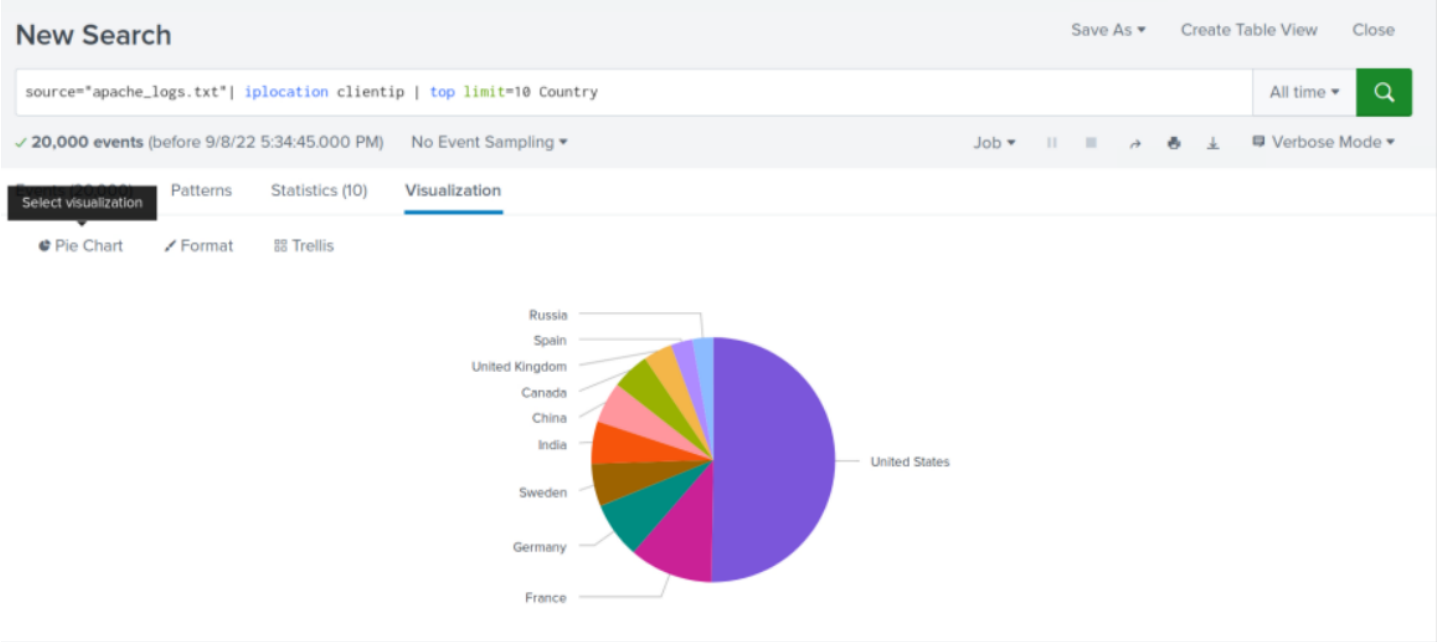
- What is the peak count of the top method during the attack?

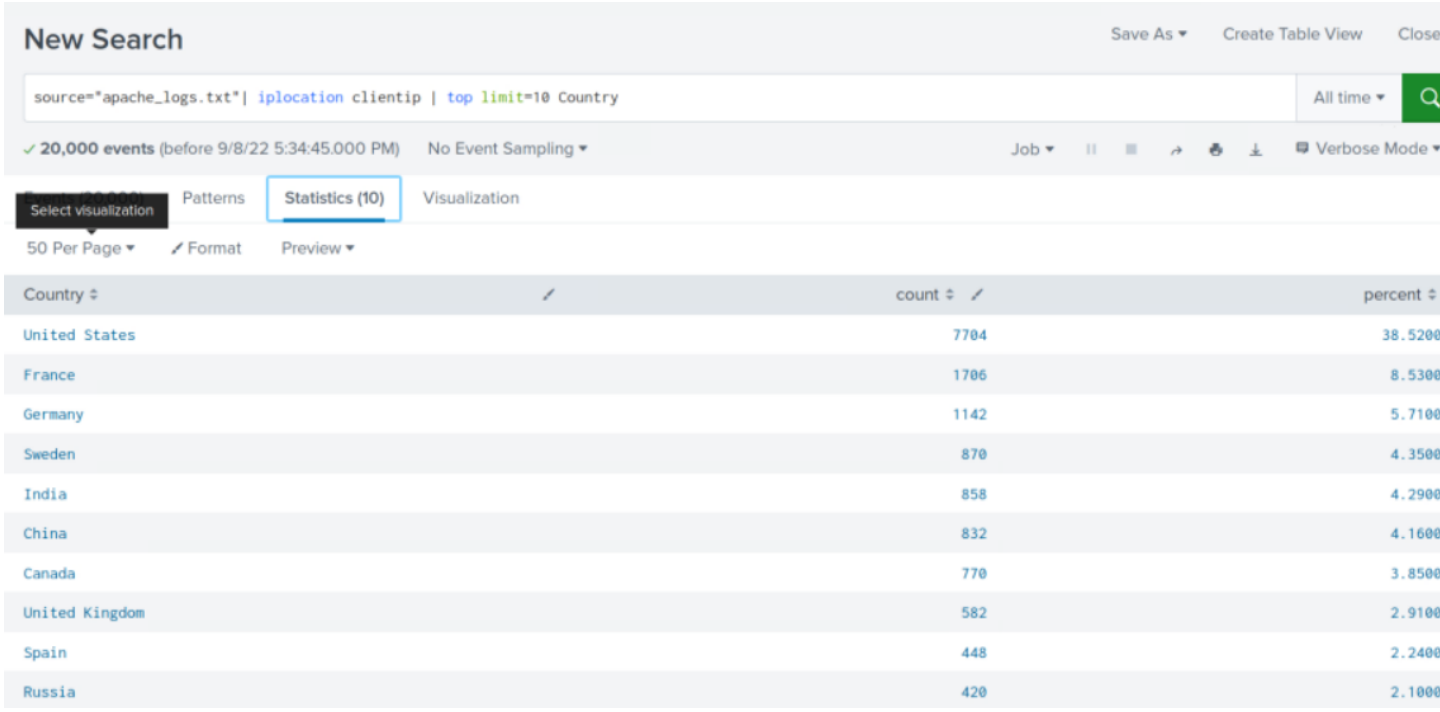
```
The peak count of POST method requests was 1296.
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

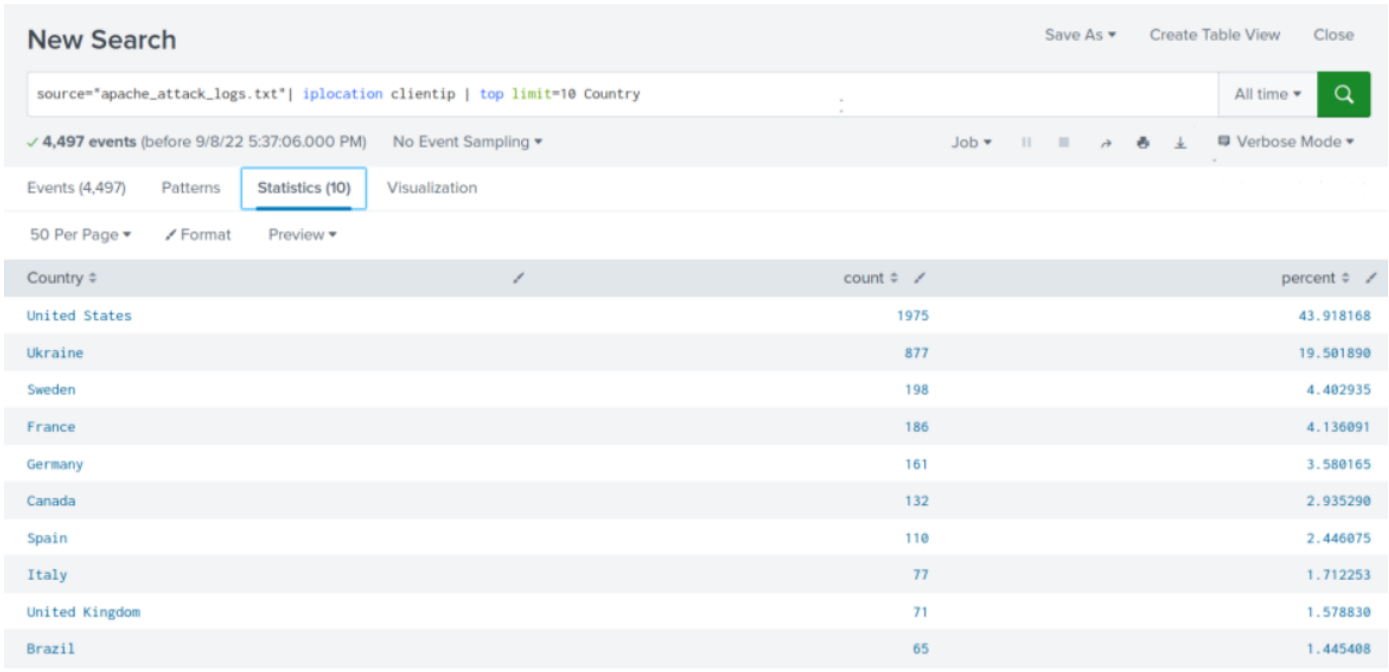
Apache Logs:





Country	count	percent
United States	7704	38.5200
France	1706	8.5300
Germany	1142	5.7100
Sweden	870	4.3500
India	858	4.2900
China	832	4.1600
Canada	770	3.8500
United Kingdom	582	2.9100
Spain	448	2.2400
Russia	420	2.1000

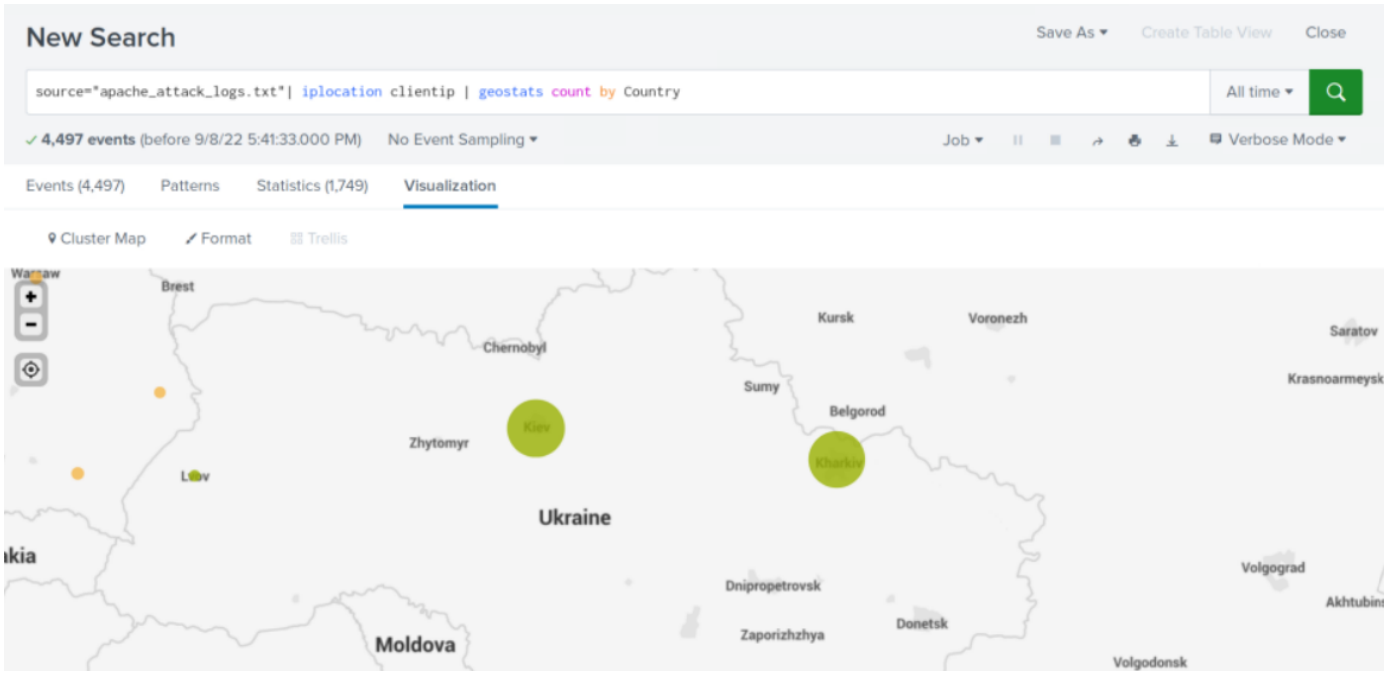
Apache Attack Logs:

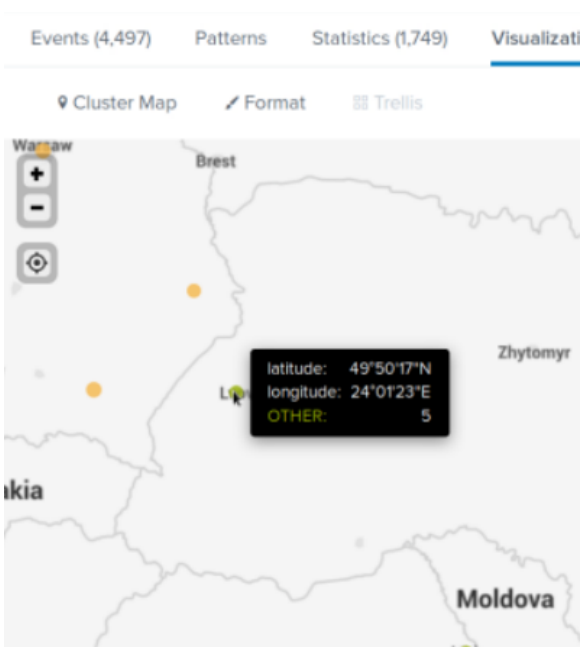


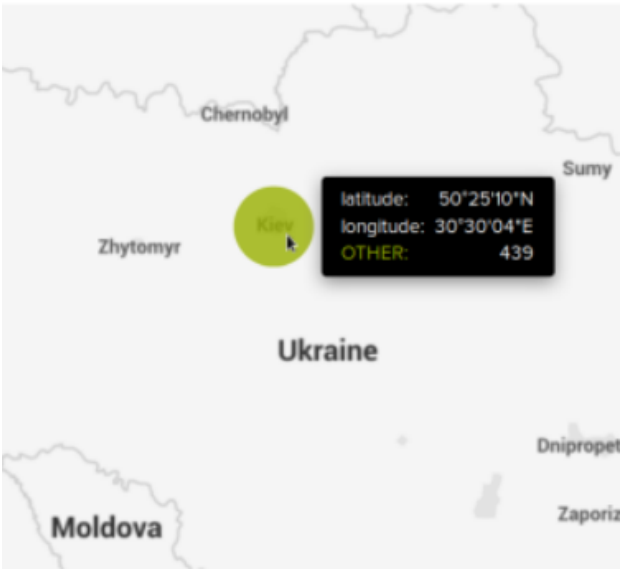
Country	count	percent
United States	1975	43.918168
Ukraine	877	19.501890
Sweden	198	4.402935
France	186	4.136091
Germany	161	3.580165
Canada	132	2.935290
Spain	110	2.446075
Italy	77	1.712253
United Kingdom	71	1.578830
Brazil	65	1.445408

Yes, as mentioned previously, there was a pronounced increase in activity from Ukraine, when it was not even a top 10 country in the Apache logs.

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





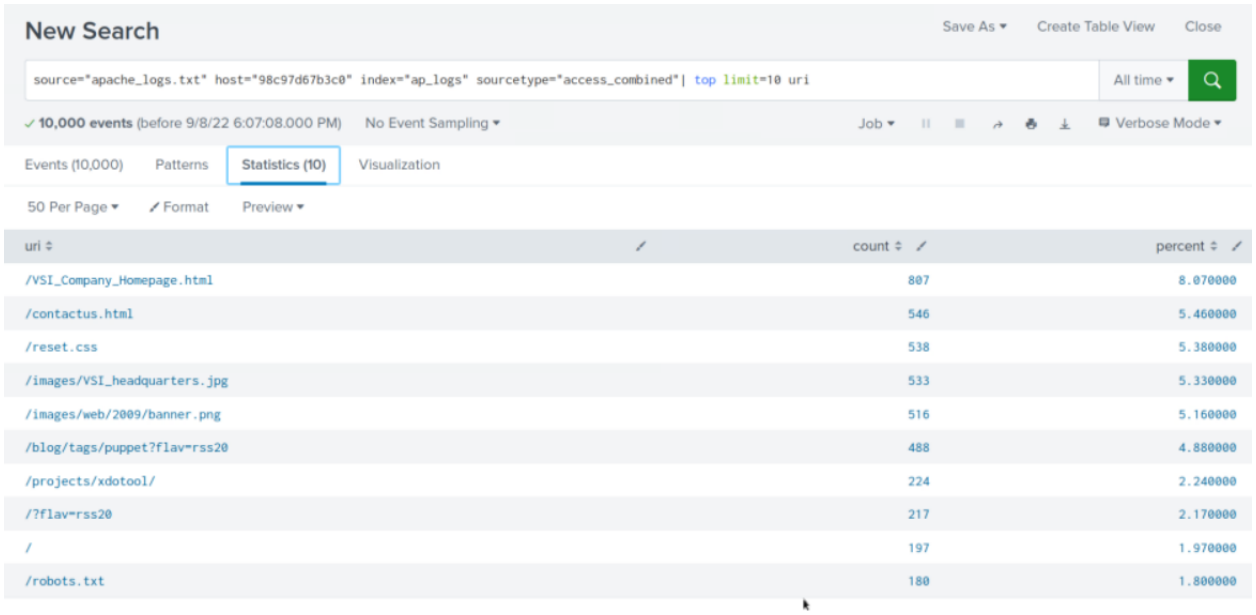


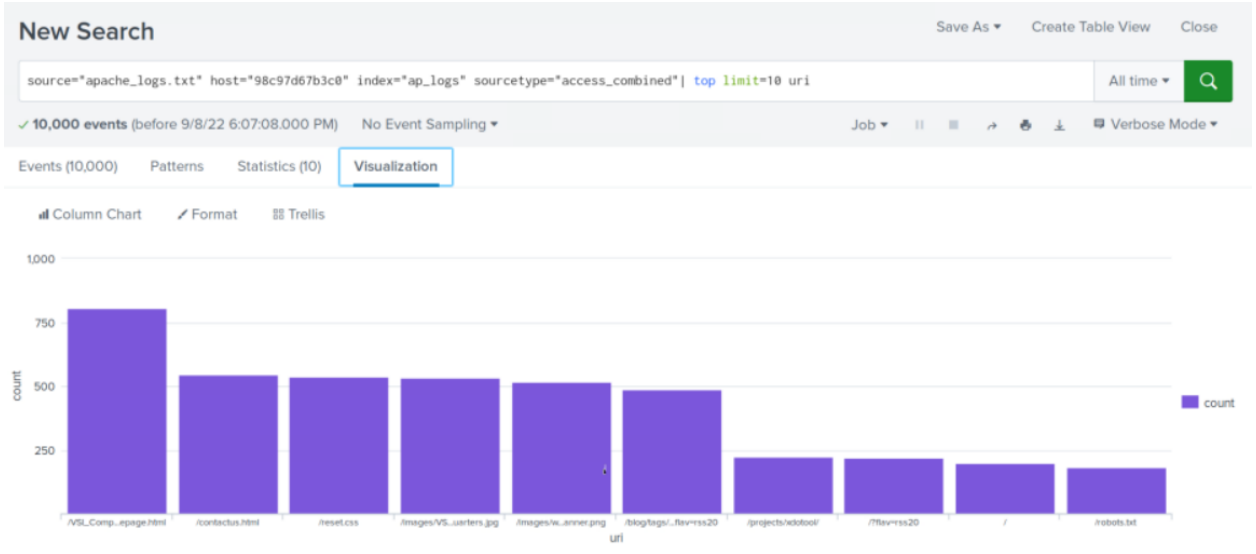
Ukraine is the country with the most suspicious amount of international activity. There are three cities that provide most of the traffic: Kiev with 439, Kharkiv with 433, and lastly Lvov with 5

- What is the count of that city?

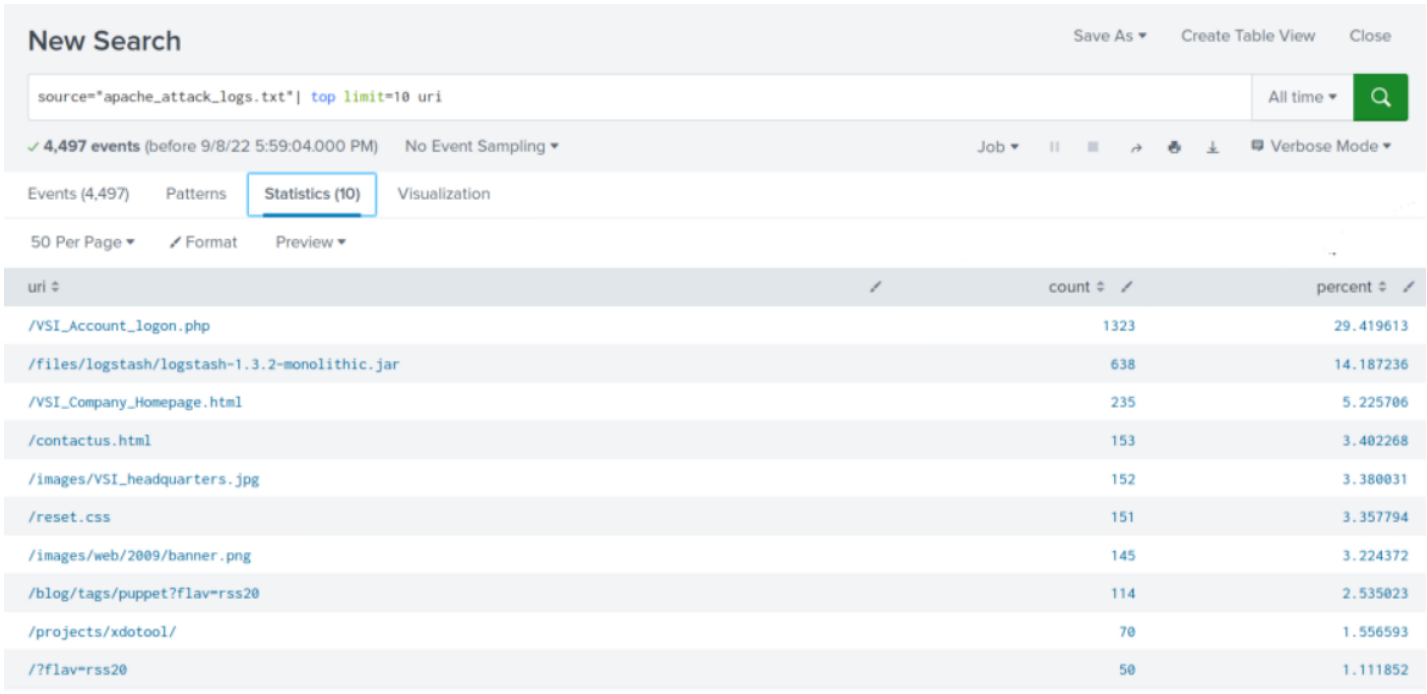
```
The biggest count of activity comes from Kiev with 439 events.
```

Dashboard Analysis for URI Data:
Apache Logs:

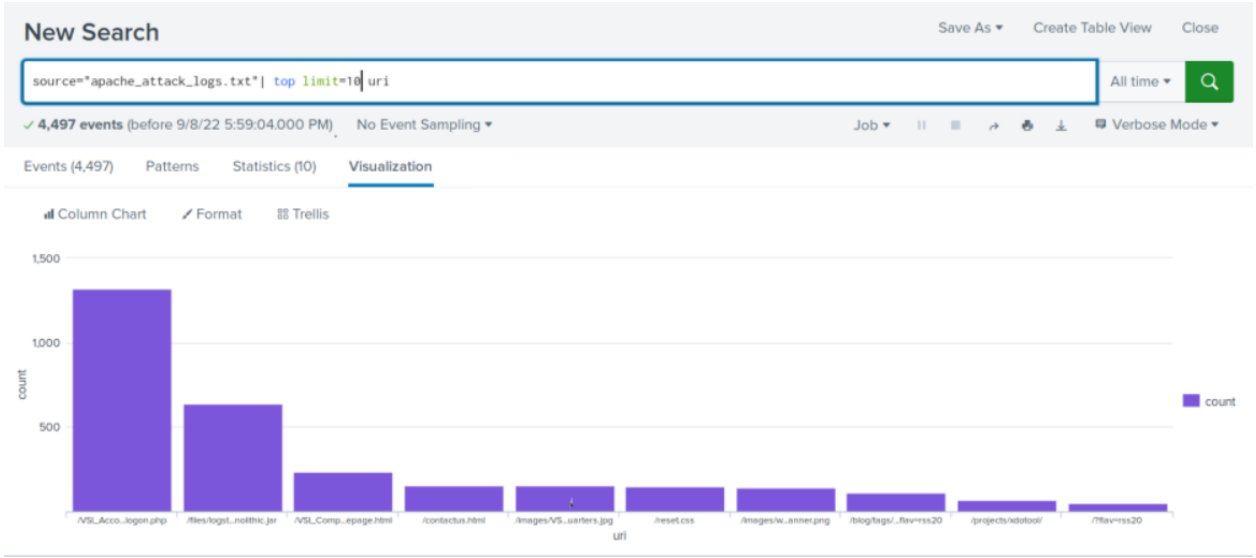




Apache Attack Logs:



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



- Does anything stand out as suspicious?

```
Yes, comparing the Apache logs and the Apache attack logs there is a shift
from /VSI_Company_Homepage.html to /VSI_Account_logon.php.
```

- What URI is hit the most?

```
The URI that is being hit the most is /VSI_Account_logon.php.
```

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

```
Based on the URI being accessed the attacker appears to be mounting a brute
force attack on the VSI logon page.
```