Cybersecurity

Project 3 Review Questions

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

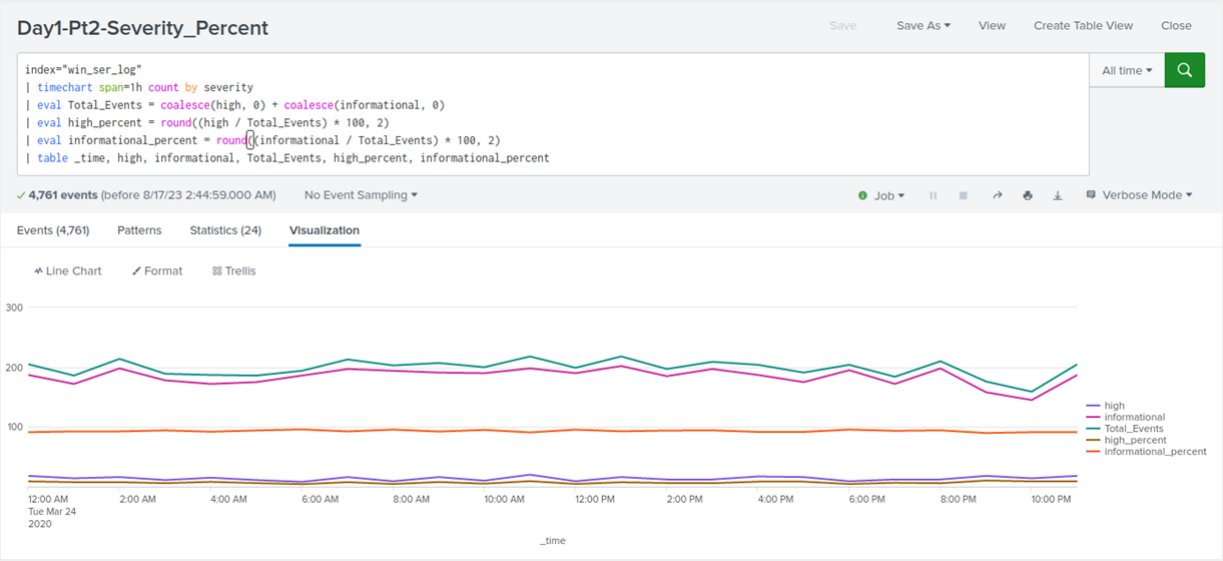
Windows Server Log Questions

Report Analysis for Severity

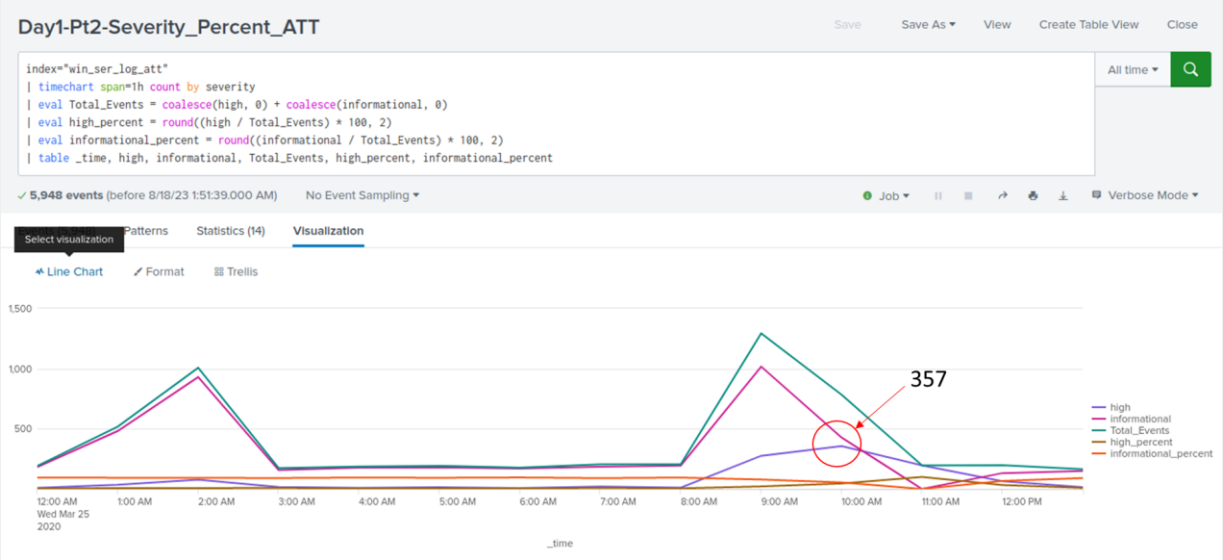
- Did you detect any suspicious changes in severity?

```
Data derived from Windows Server Log dated 3/24/2020 established a baseline
for normal operations. Activity totals held consistent around approximately
200 severity events - informational and high.

On 3/25/2020, the day of the attack, significant spikes in activity occurred
in the early and late morning periods. The spikes occurred at 2:00am and
9:00am. The logs clearly depict two attacks. The first attack began at
12:00am and ended at 3:00am. The second attack began at 8:00am and ended at
11:00am. The spike in activity was predominantly due to the increase in
“informational” activity. It is important to highlight the spike in 357
“high” severity activities that occurred at 10:00am. An alert would have
been triggered by “high” activity alone, barring the already significant
number of “informational” activities triggering the alert.
```



- *Windows Server Log - 3/24/2020*



- *Windows Server Log - 3/25/2020*

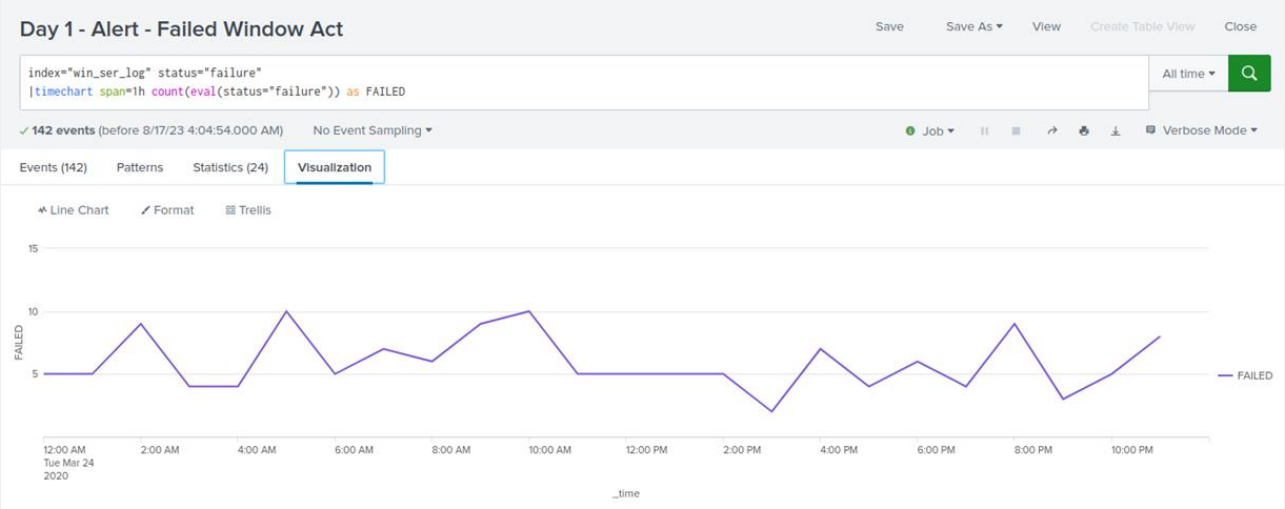
Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

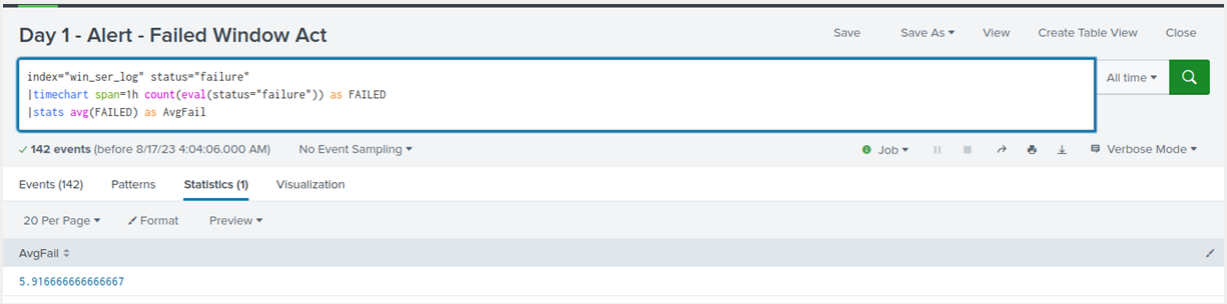
Data derived from Windows Server Log dated 3/24/2020 established a baseline for normal operations. The number of “failed” activities stayed at or below 10.

Subsequently, a threshold of 11 was established. A base line of 6 was established by computing the average amount of “failed” activities using the Splunk function.

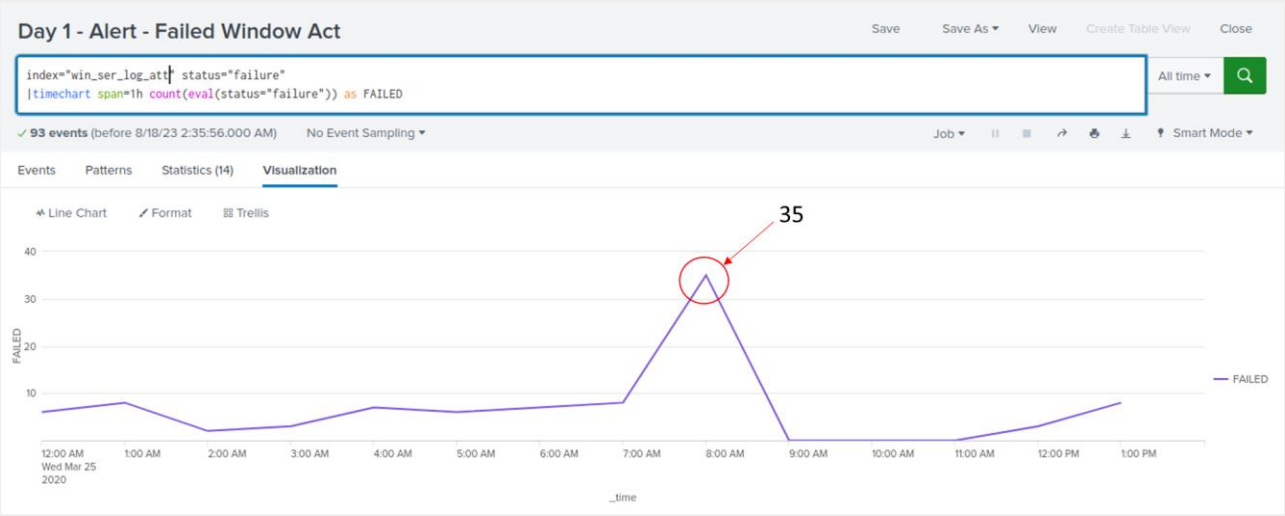
On 3/25/2020, the day of the attack, a significant spike in activity occurred from approximately 7:00am to 8:30am. The spike occurred at 8:00am totaling 35 “failed” activities. With a threshold of 11, the attack would have triggered an alert for the increase in “failed” activities.



- *Windows Server Log - 3/24/2020*



- *Avg Fail Calculation - Windows Server Log - 3/24/2020*

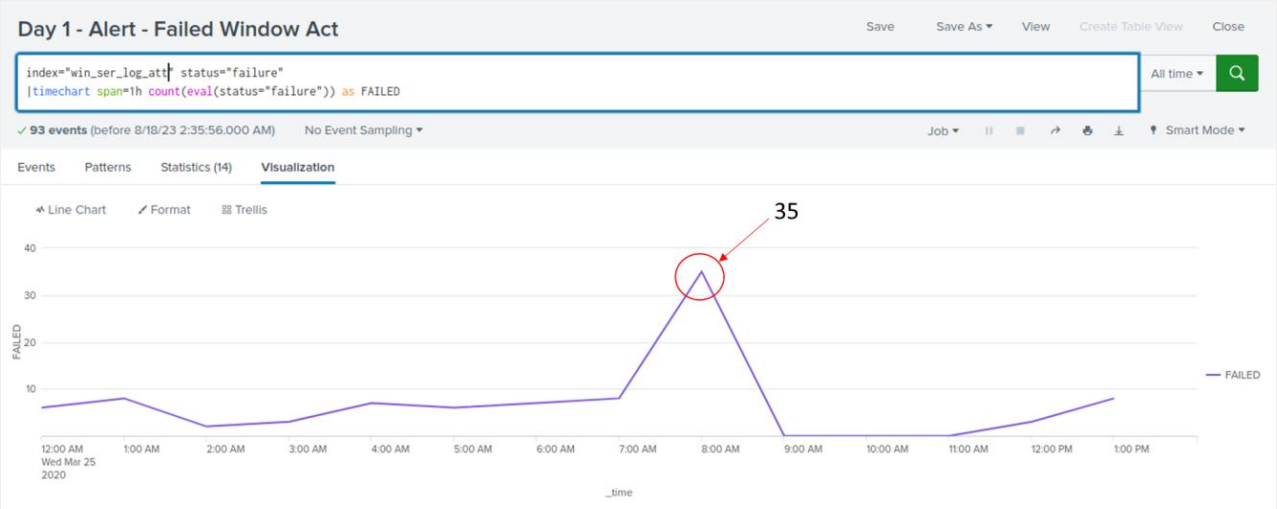


- *Windows Server Log - 3/25/2020*

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

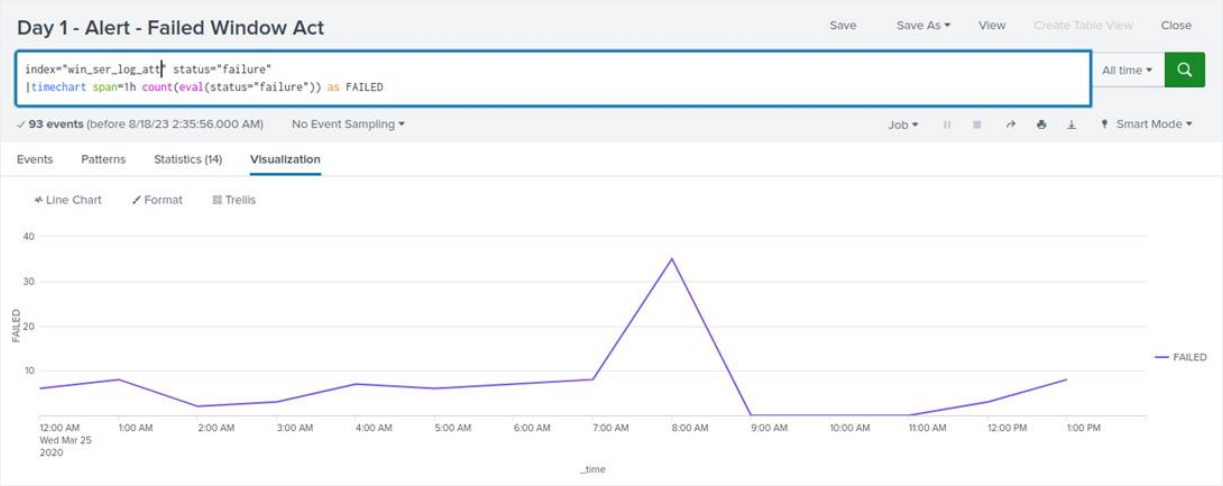
Yes, the average volume of “failed” activities on 3/25/2020 surpassed the threshold of 11 as the highest number of failed activities. An alert would have been triggered as early as 7:15am with the peak occurring at 8:00am.



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

The counts were:

- 12 at approximately 7:15am
- 35 at 8:00am
- 12 at approximately 8:25am



- When did it occur?

It occurred on March 25, 2020 from 7:15am to 8:25am.

- Would your alert be triggered for this activity?

Yes, my alert would have been triggered for this activity.

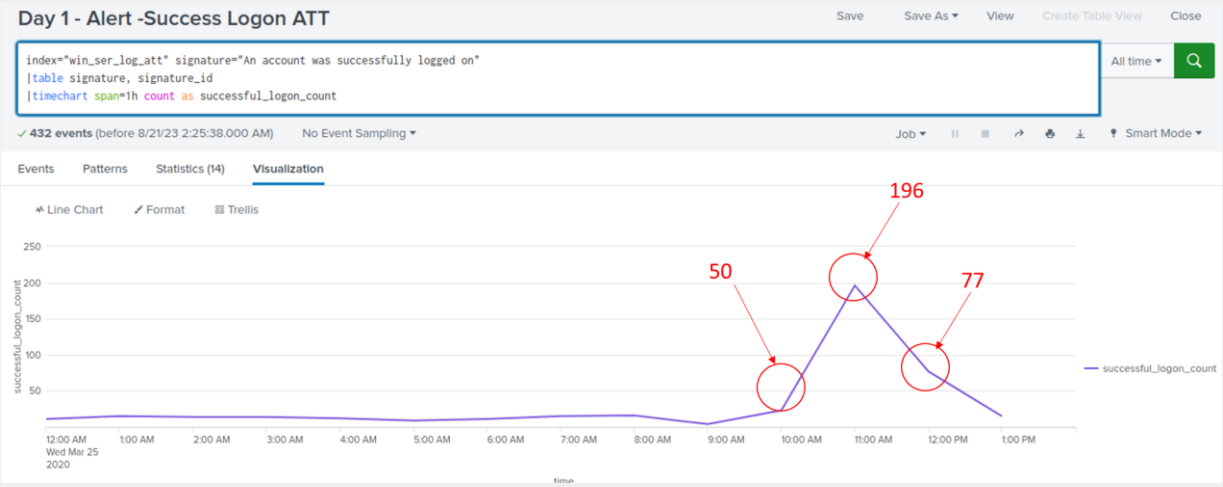
- After reviewing, would you change your threshold from what you previously selected?

No, given the amount of traffic that came into the company platform, which was approximately 10,000 events across two days, isolating the failed activity from 3/25/2020 from 7:15am to 8:25am, the average amount of failed activities still remained at approximately 6, and didn't break 10 failed activities. I would maintain the current threshold of 11. The spike in failed activities would have been clearly observed.

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

Yes, considering the amount of average successful log-ins was calculated at approximately 13, and a threshold at 25, there was a period where the volume of successful logins skyrocketed to 196.



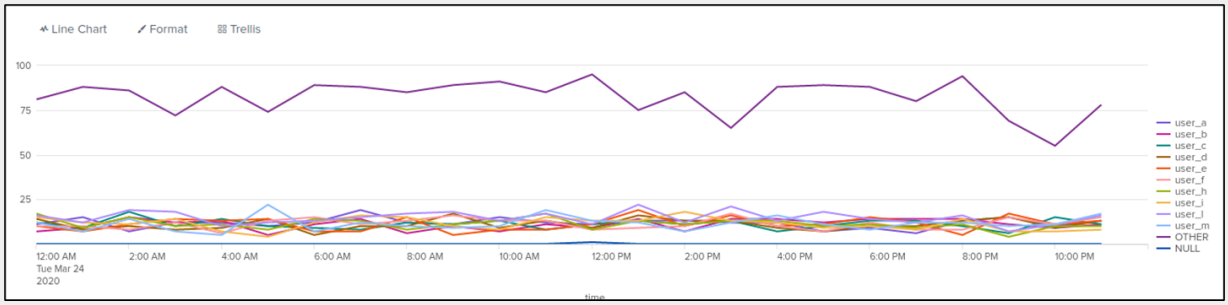
- If so, what was the count of events in the hour(s) it occurred?

The counts were:

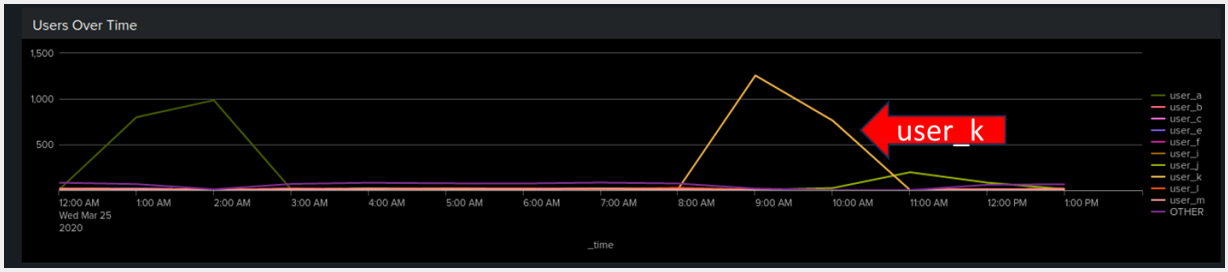
- 50 at approximately10:15am, on 3/25/2020
- 196 at 11:00am, on 3/25/2020
- 77 at 12:00pm, on 3/25/2020

- Who is the primary user logging in?

During the above period of time in questions, Primary User was “user_k”.



- *Windows Server Log - 3/24/2020*



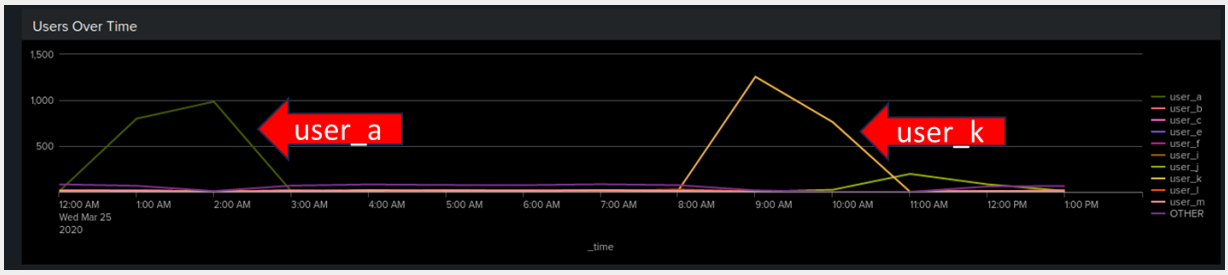
- *Windows Server Log - 3/25/2020*

- When did it occur?

```
This occurred on Mar 25, 2020 from approximately 8:00am to 11:00am.
```

- Would your alert be triggered for this activity?

```
Yes, the Windows Server Log on 3/24/2020 showed user logons never going
above 25, barring the anomaly “OTHER”. During the day of the attack two
alerts would have been triggered. User_a and user_k surpassed the threshold
of 25 logons/hour.
```



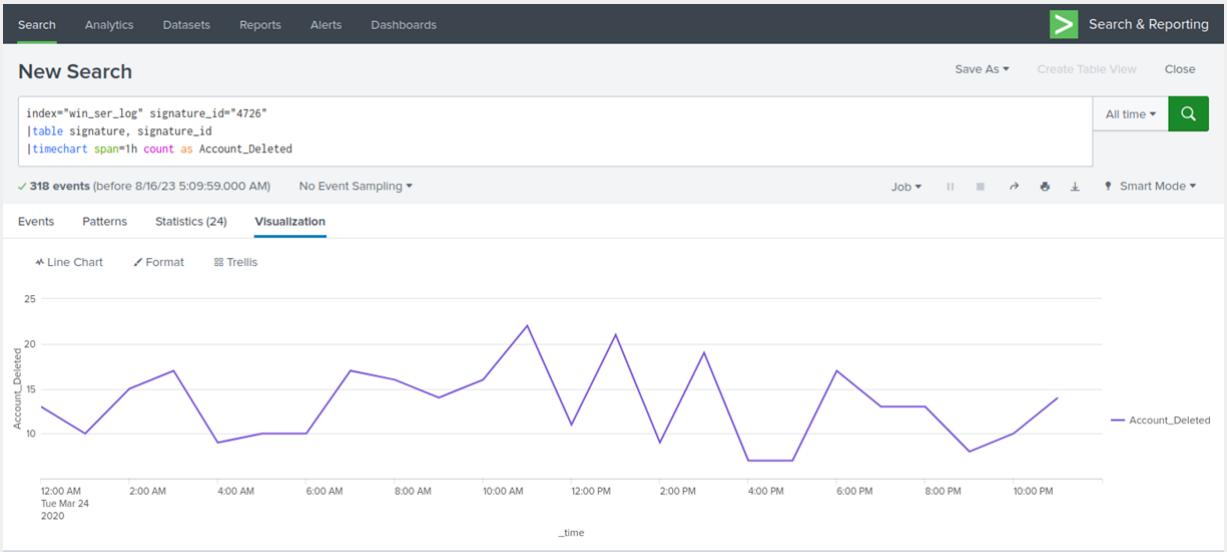
- After reviewing, would you change your threshold from what you previously selected?

```
No, I would maintain the threshold at 25. The amount of logons by user_a and
user_k were too egregious not to notice.
```

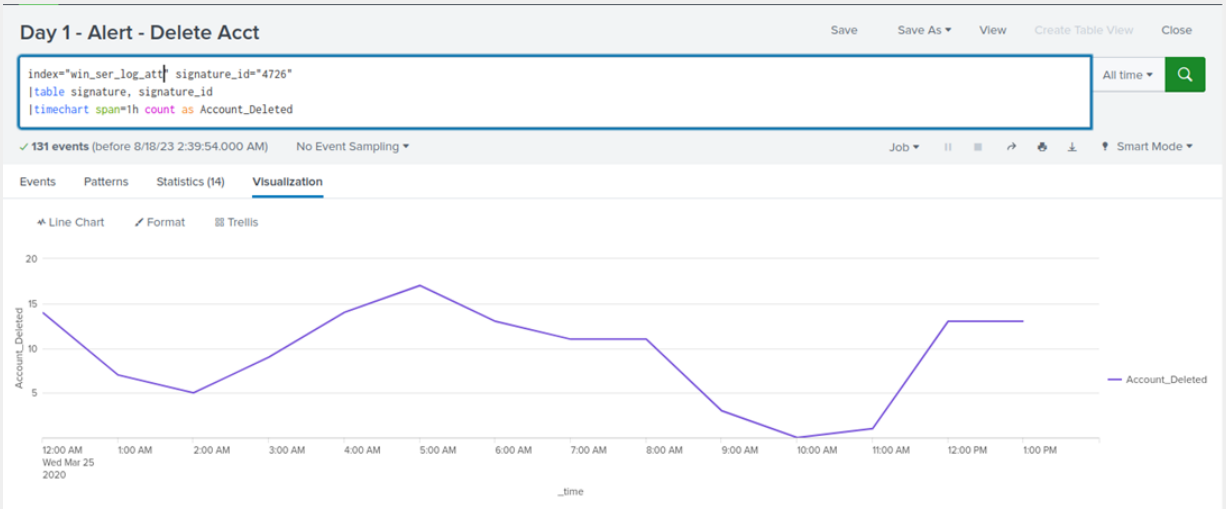
Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

Not particularly, on both 3/24 and 3/25, barring outliers, the number of deleted accounts min/max'ed from 10 to 20. The suspicious activity occurred at 10:00am where NO accounts were deleted.



- *Windows Server Log - 3/24/2020*

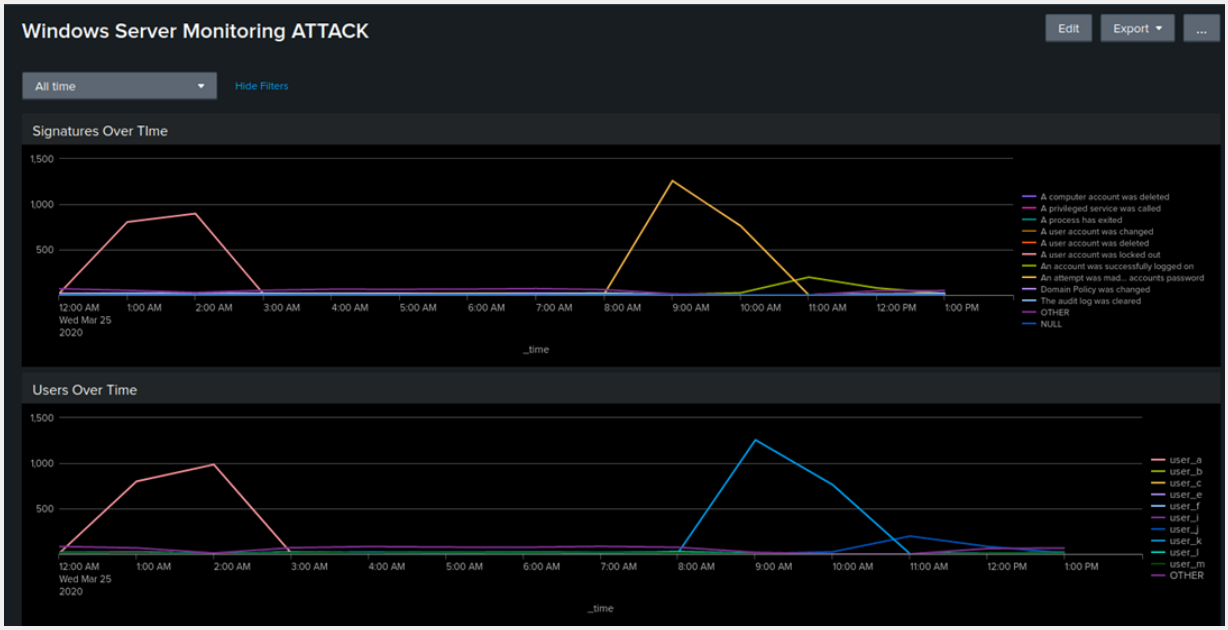


- *Windows Server Log - 3/25/2020*

Dashboard Analysis for Time Chart of Signatures

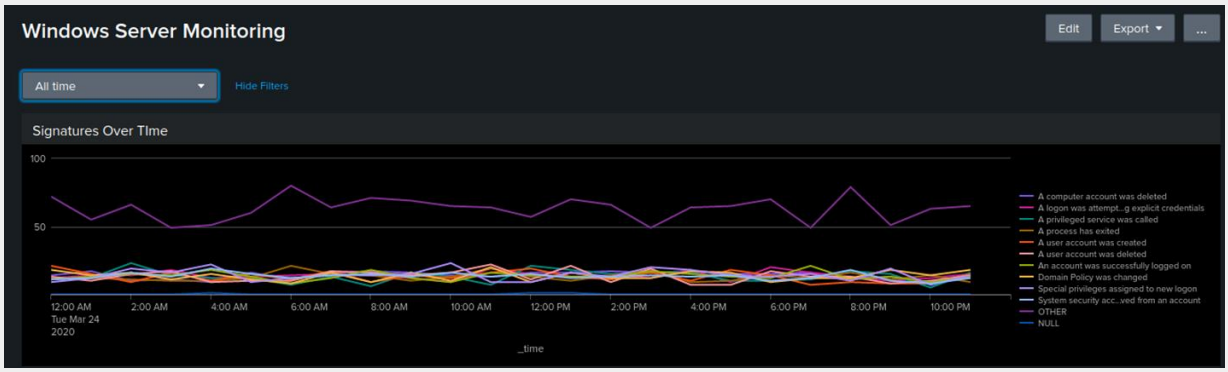
- Does anything stand out as suspicious?

Yes, on 3/25/2020 the spikes in signatures "A user account was locked out" and "An attempt was made to reset an accounts password" directly correlated to the number of logons by user_a and user_k, respectively.

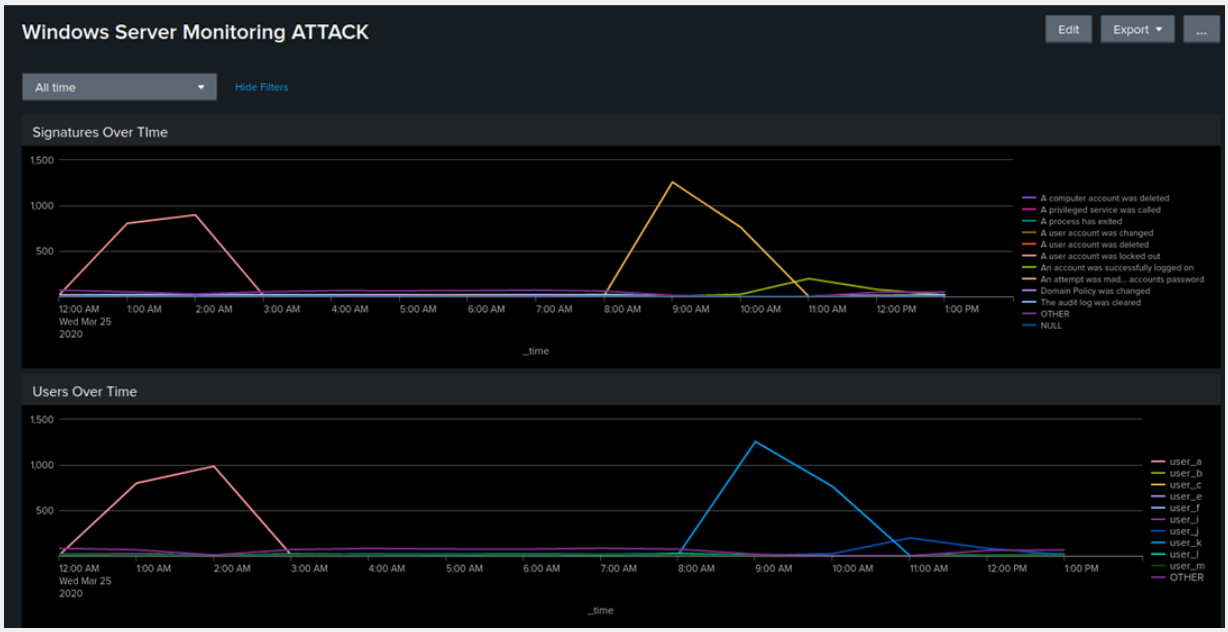


- What signatures stand out?

- “A user account was locked out”
- “An attempt was made to change an accounts password”



- *Normal Operations on 3/24/2020*



- *Surpassed Signature thresholds correlated with Users during attack on 3/25/2020*

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

- "A user account was locked out"
  - Begin 12:00am
  - Ended 3:00am
- "An attempt was made to reset an accounts password"
  - Begin 8:00am
  - Ended 11:00am

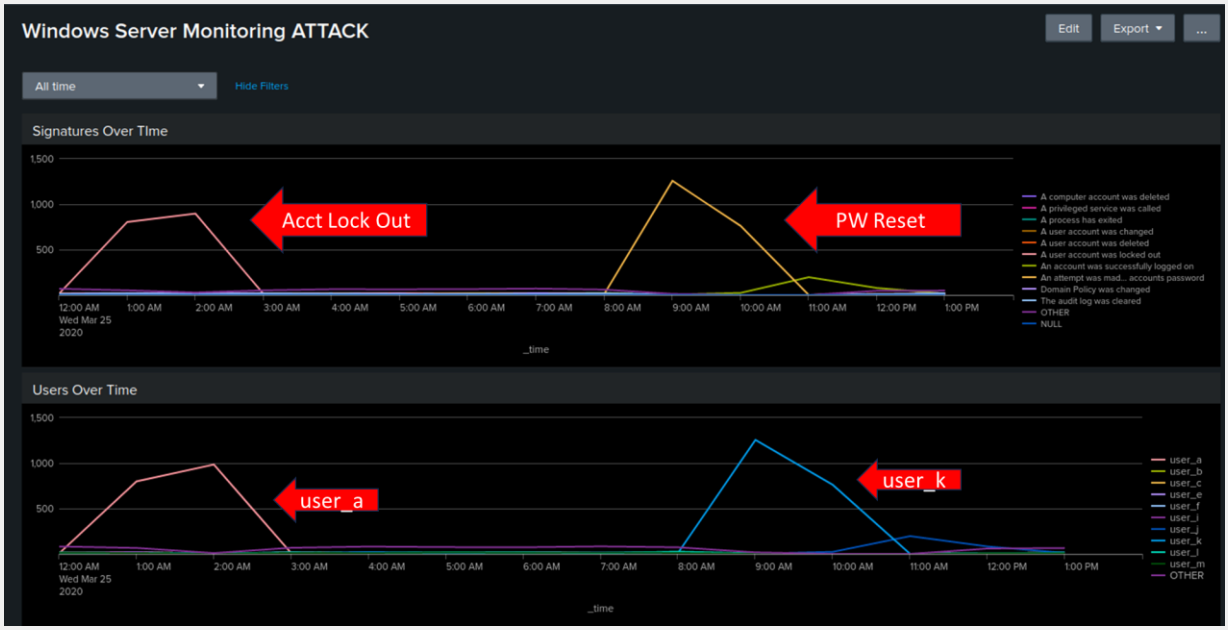
- What is the peak count of the different signatures?

- "A user account was locked out" - 896
- "An attempt was made to reset an accounts password" - 1258

Dashboard Analysis for Users

- Does anything stand out as suspicious?

The Activity of two users, user_a and user_k, tops other users. They also have suspicious peaks that coincide with suspicious signatures.



- Which users stand out?

- user_a
- user_k

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

- user_a: 12:00am-3:00am
- user_k: 8:00am-11:00am

- What is the peak count of the different users?

- user_a: 984
- user_k: 1256

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

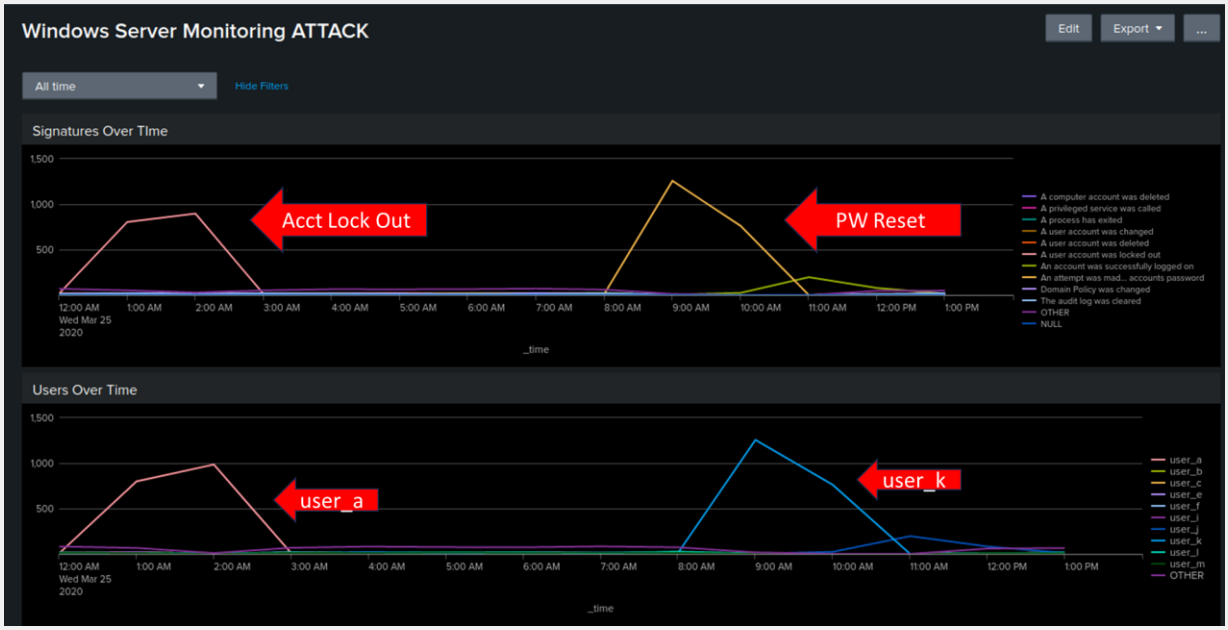
- Does anything stand out as suspicious?

Yes, user_a and user_k's activities correlate to suspicious signatures. User_a seems to have locked out several accounts, subsequently, user_k

performed several password resets. If the users were IT specialists locking accounts and resetting them when the workday began, then it would be too suspicious. Conversely, if user_a and user_k were suspicious users, i.e. JobeCorp pentesters, working in collaboration, the actions may be nefarious in nature.

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

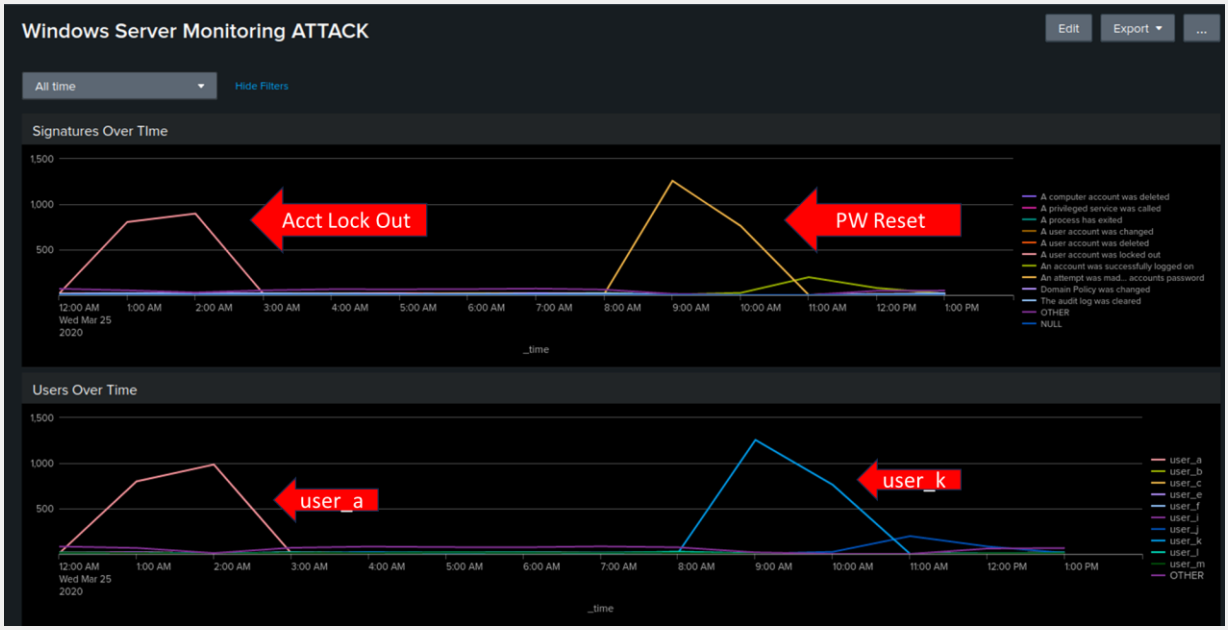
Yes, with respect to Signatures, two related processes and activities spiked. Signatures “A user account was locked out” and “An attempt was made to reset an accounts password”. These are related tasks - locking one’s account and subsequently resetting the password. Both activities would have triggered alerts. Moreover, the spikes in these activities correlate directly to the logon activities for two users.



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

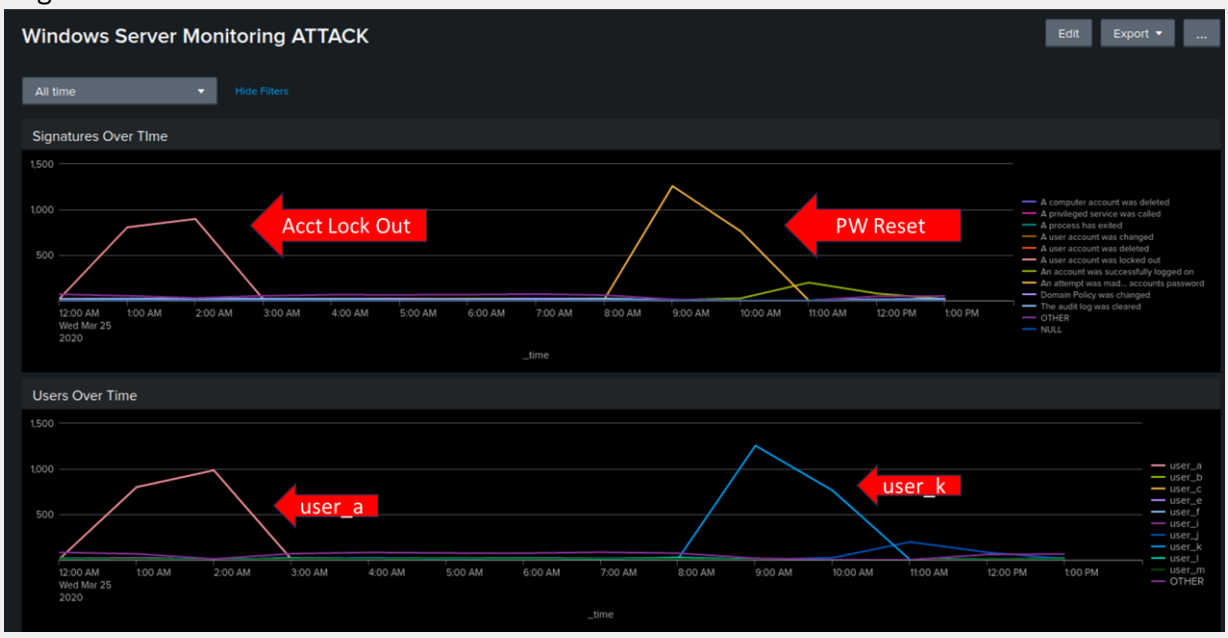
- Does anything stand out as suspicious?

Yes, with respect to Users, user_a and user_k’s activities correlate directly to suspicious spikes in Signature activity.



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

Yes, the activities placed side-by-side on the Dashboard perfectly depict impact from one dashboard to the other. Specific users to specific signatures.



Dashboard Analysis for Users with Statistical Charts

- What are the advantages and disadvantages of using this report, compared to the other user panels that you created?

```
The advantage of the dashboard analysis is correlations between two items can easily be analyzed. Conversely, the disadvantage is that it isn't granular enough, and detailed analysis is needed to discuss where the discrepancies lie.

Statistical charts are great at depicting the detailed information and trends showing clear deviation from baselines and thresholds that can also be calculated from the statistical chart. Conversely, the disadvantage is, it is difficult to compare the information side-by-side. Constant going back-and-forth from charts is needed to develop trends.

The use of this report walks the reader exactly through the problem and issues. Specific information pertaining to the threat is easily collated. The disadvantage is TL:DR, it is a long report. Also, the time required to draft the report, quality check, get senior leadership approval requires a significant amount of time.
```

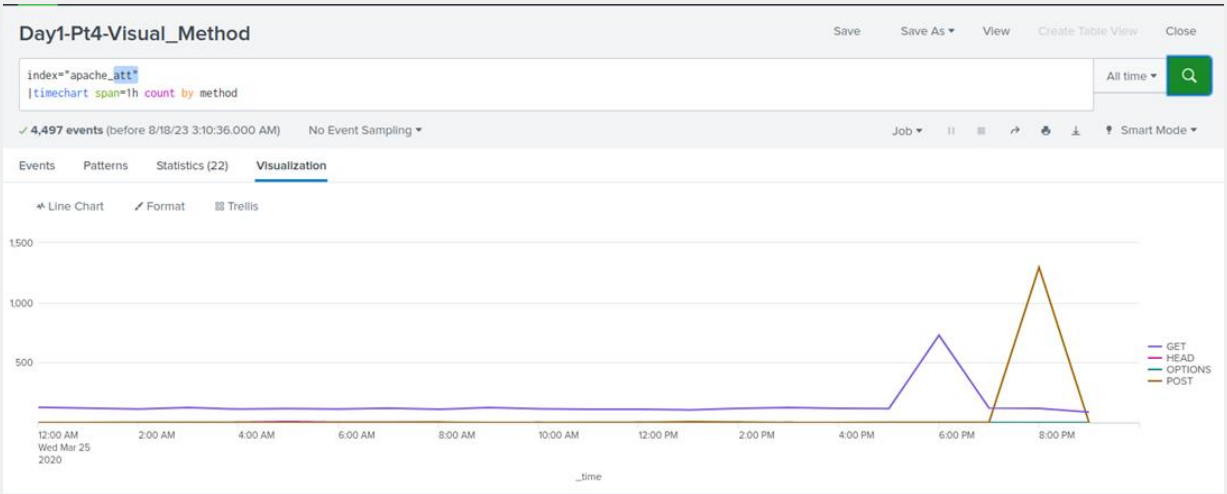
Apache Web Server Log Questions

Report Analysis for Methods

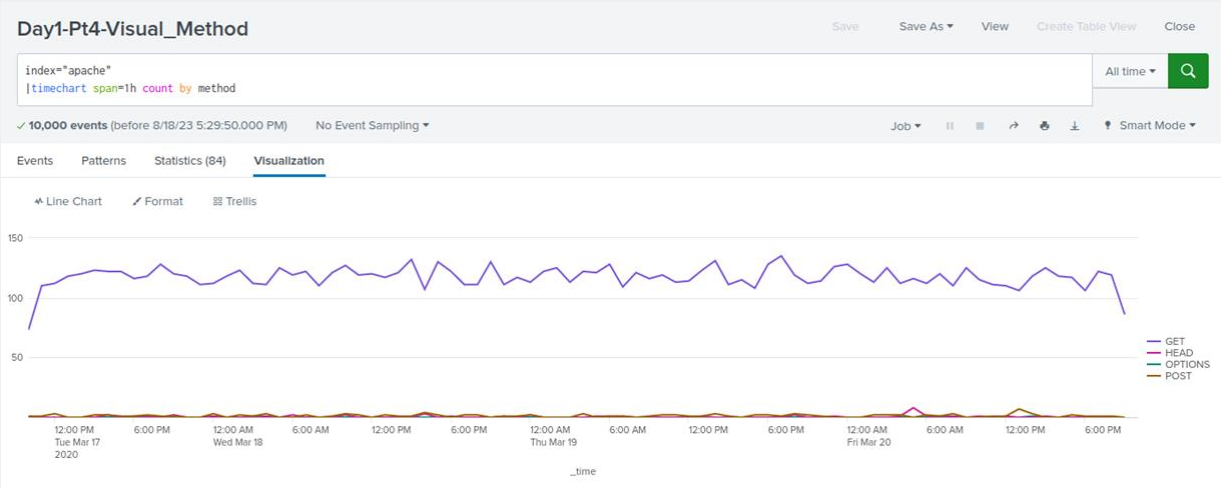
- Did you detect any suspicious changes in HTTP methods? If so, which one?

```
Yes, on 3/25/2020, a significant spike in HTTP method POST spiked to 1296. During normal operations, POST requests typically account for approximately 1% of HTTP methods, 1-3 requests per hour. On the day of the attack, POST requests accounted for 29% of the HTTP methods received. The POST requests occurred at 8:00pm.

It is also notable that GET requests spiked to a count of 729, normal operations typically sees 100-150 GET requests per hour.
```



- Apache Attack Logs on 3/25/2020



- Normal Apache operations

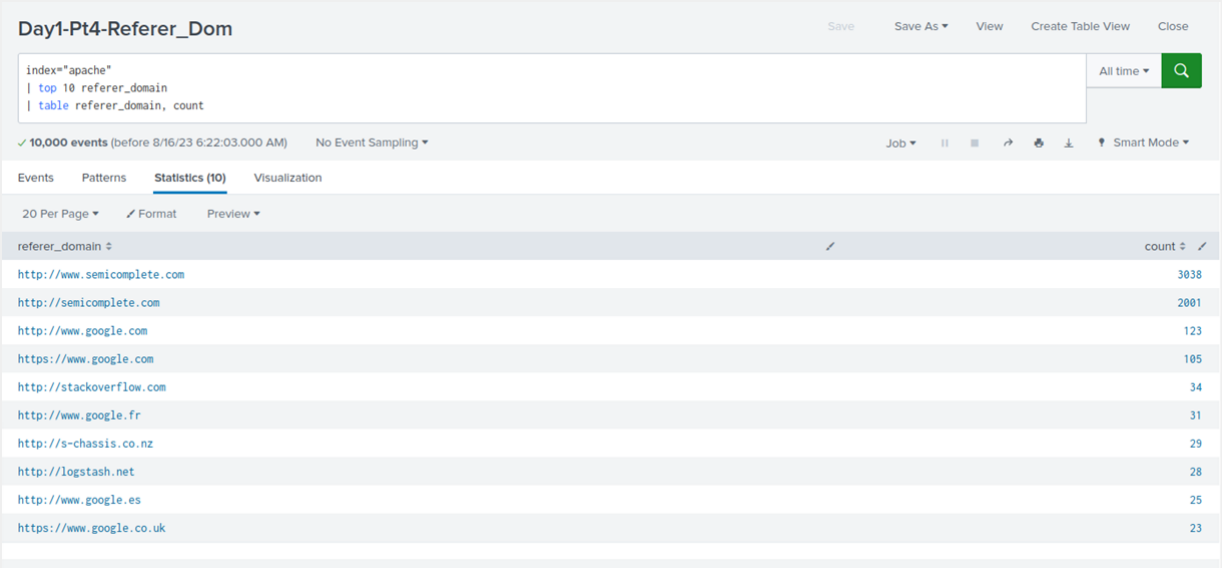
- What is that method used for?

The POST request is used to submit data to be processed to a resource on a server. When a POST is sent, it sends data in the request and the server actions that request. POST is typically used when you're creating or updating data on the server.

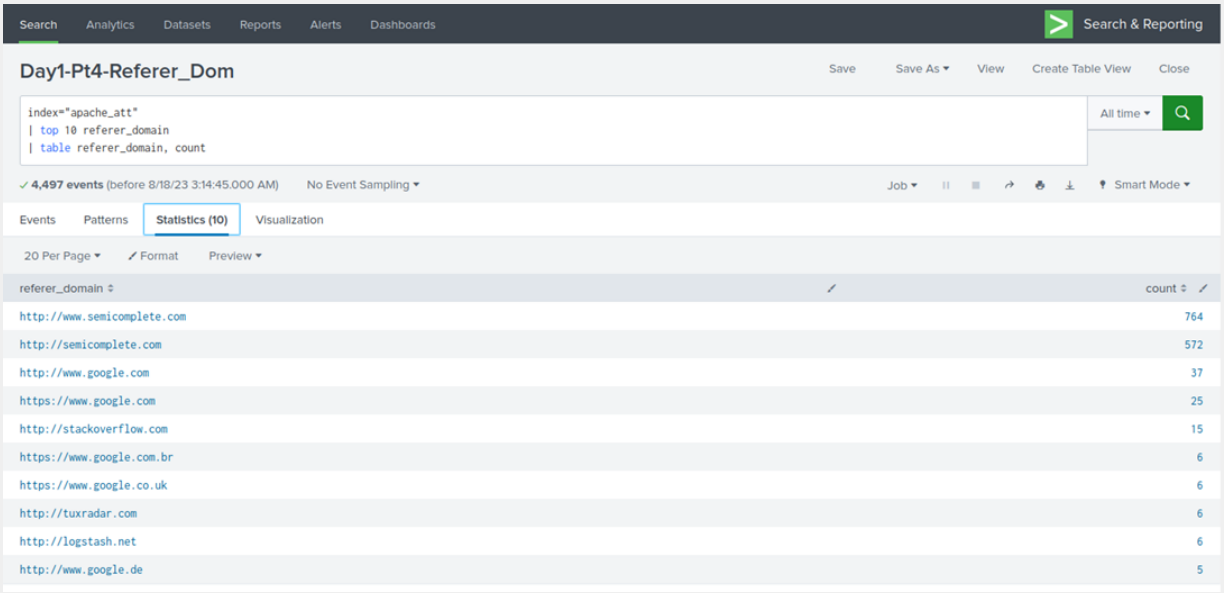
Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

There was no suspicious change in referrer domains.



- *Normal Apache Logs*

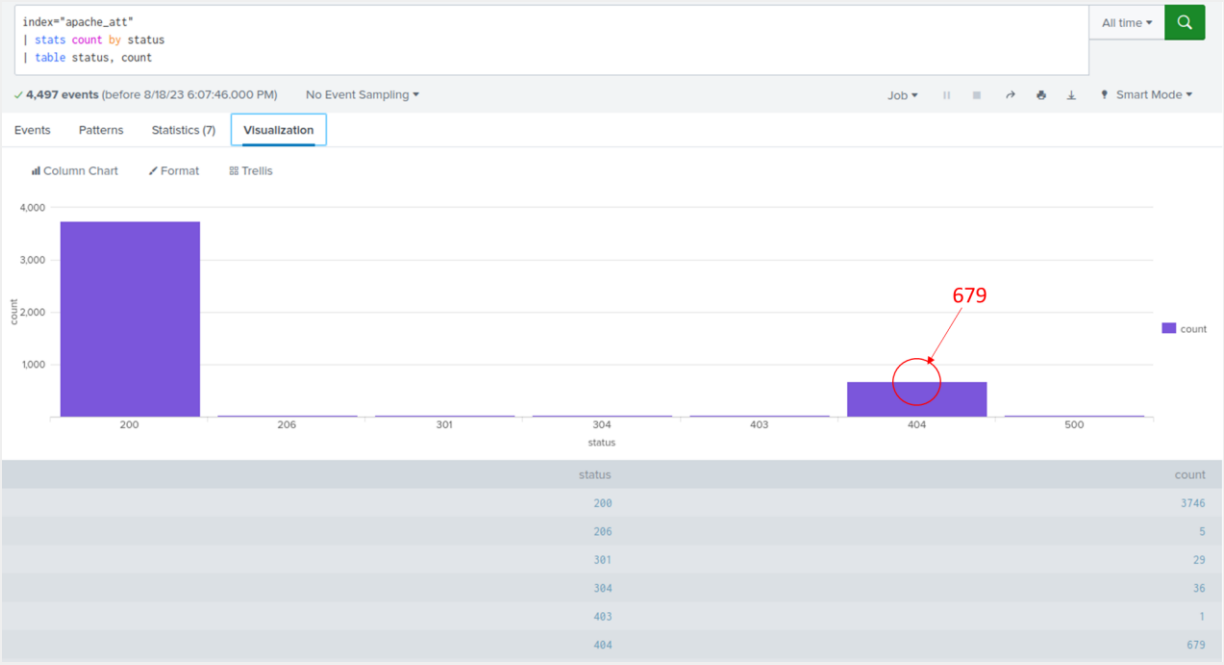


- *Apache Logs during the attack*

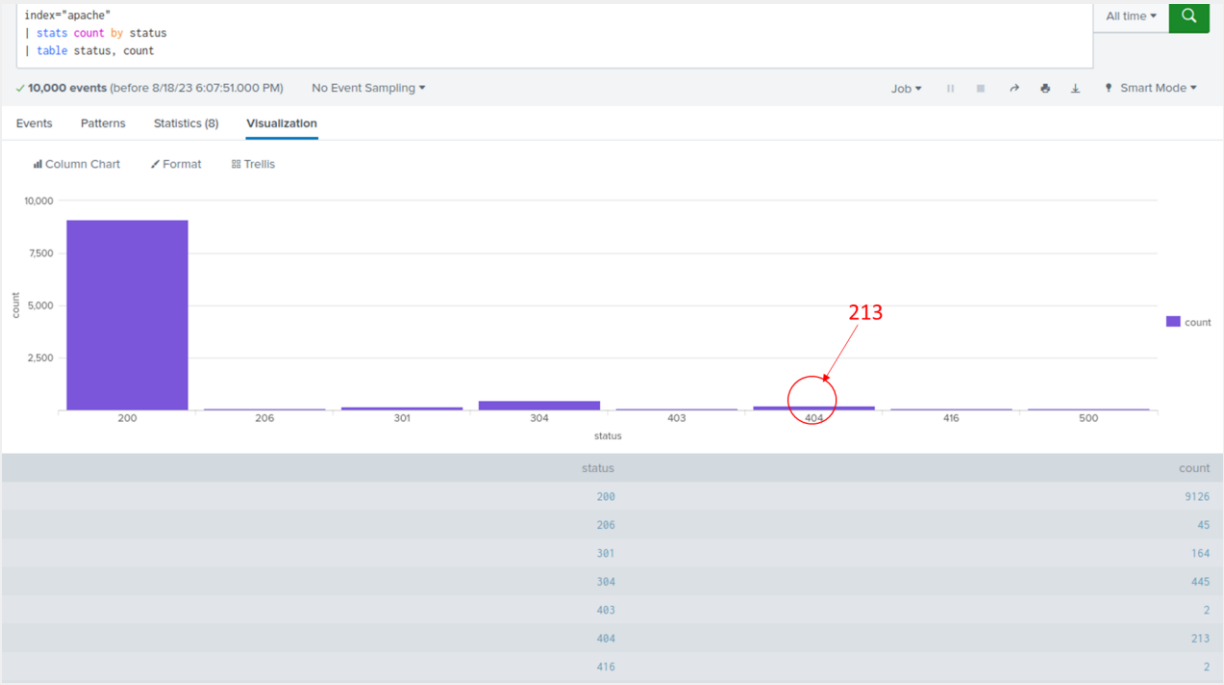
Report Analysis for HTTP Response Codes

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

Yes, HTTP response code 404, “Not Found” error, spiked to 679. Typical operations averaged 200 “404” codes. The spike in “404” codes in the Apache log during the attack was an increase of over 300%.



- *Apache Attack Log - HTTP Response Codes*

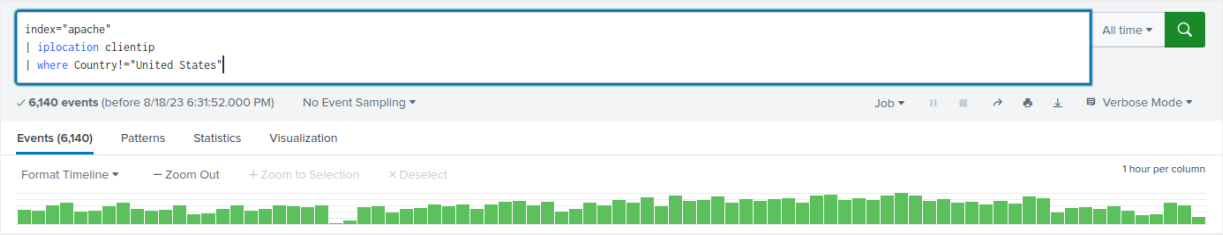


- *Apache Log - Normal Operations - HTTP Response Codes*

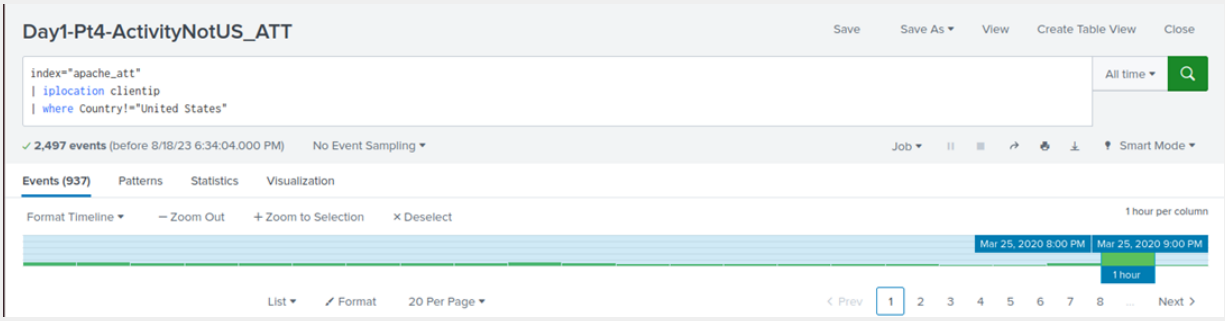
Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

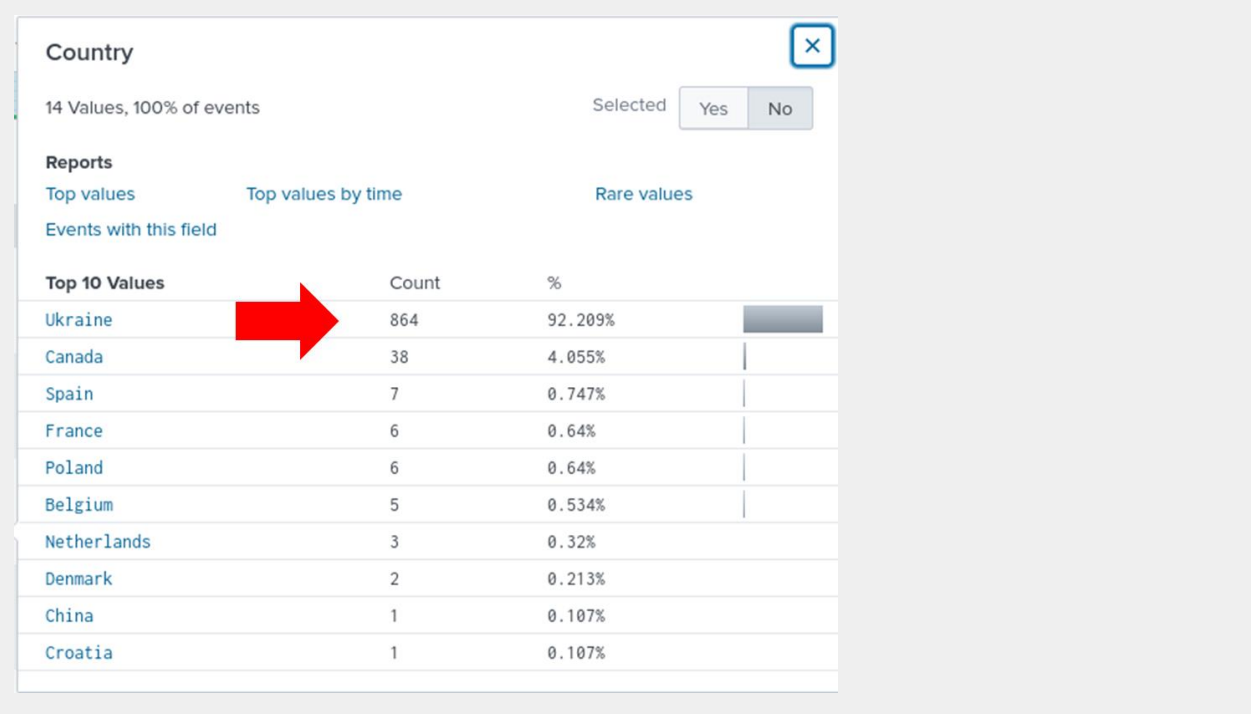
Yes. There was a significant increase in volume from the Ukraine. During normal operations an equally distributed amount of traffic occurs. But on 3/25/2020 at Ukraine suspiciously increases traffic, while other countries decrease.



- *Apache Normal Operations Logs*



- *Apache Attack Logs*



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

```
864 events occurred from 8:00pm to 9:00pm on 3/25/2020.
```

- Would your alert be triggered for this activity?

```
Yes, an alert would have been triggered. On average approximately 120 events
occur an hour. A threshold of 130 was set. The significant jump in events in
the Ukraine to 864 in a single hour would have triggered the alert.
```

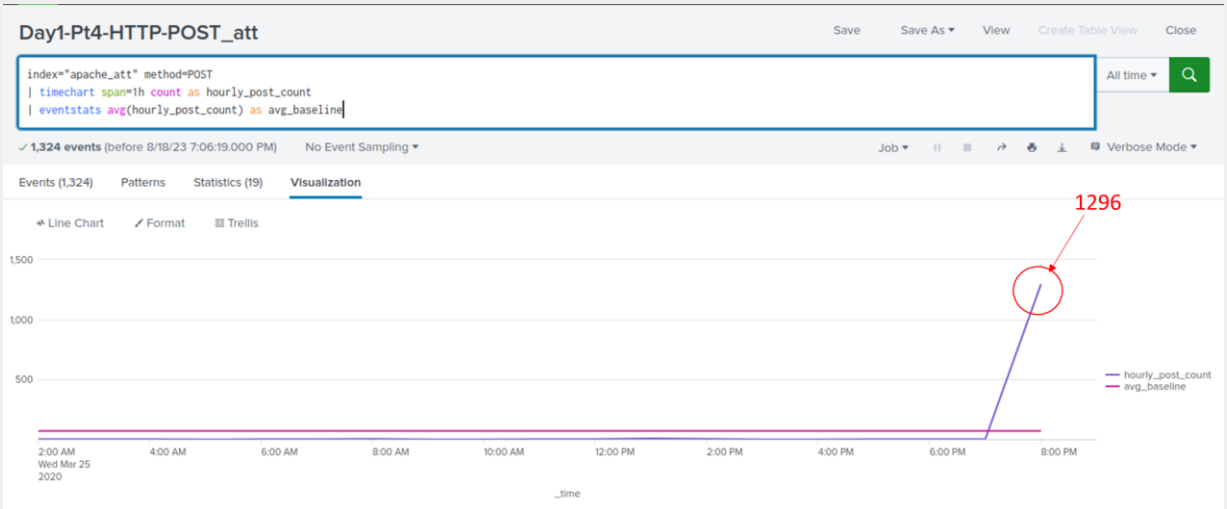
- After reviewing, would you change the threshold that you previously selected?

```
No, I would maintain the threshold at 150.
```

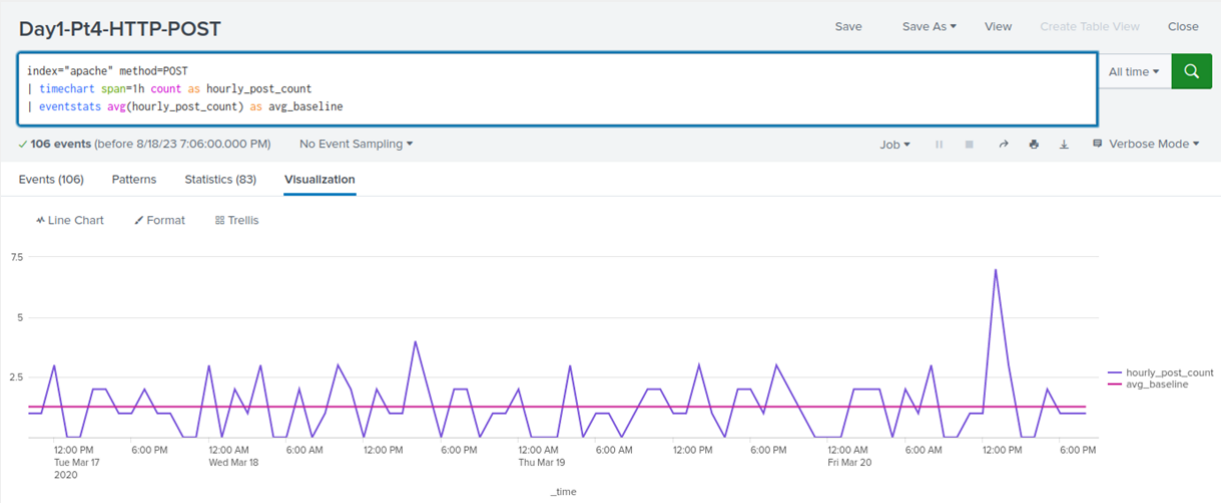
Alert Analysis for HTTP POST Activity

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

Yes, a significant increase in HTTP POST requests occurred on 3/25/2020



- *POST the day of the attack, 3/25/2020*



- *POST during normal operations*

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

The count peaked at 1296

- When did it occur?

It occurred at 8:00pm on 3/25/2020

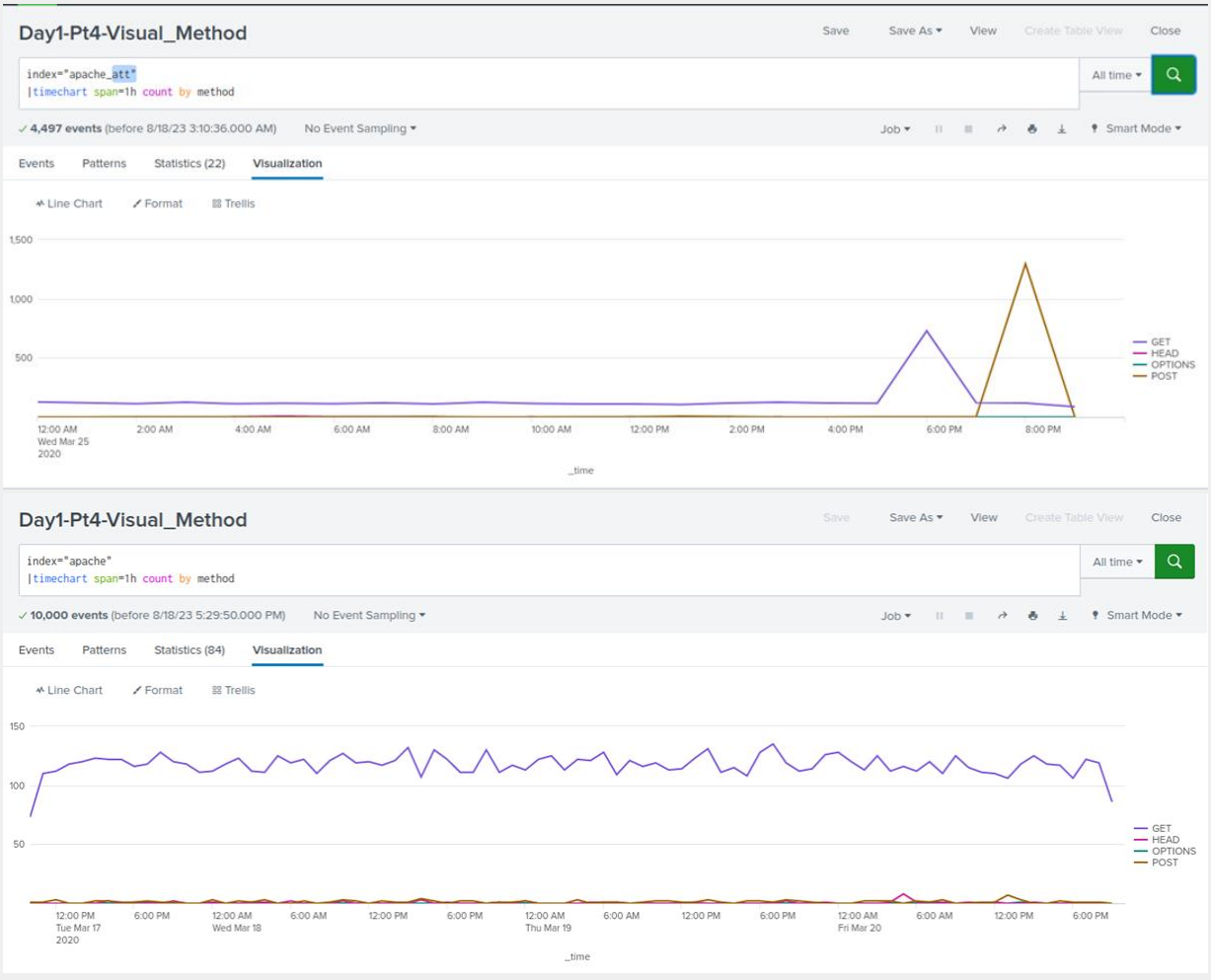
- After reviewing, would you change the threshold that you previously selected?

No, normal operations logged normal POST requests at approximately 5 requests an hour. The jump to 1296 during the attack was an inordinate amount of POST requests.

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

Yes, during the day of the attack, a significant increase in the GET & POST requests spiked at approximately 6:00pm to 8:00pm. The number of counts for GETs increased by approximately 500%, while POST requests increased several magnitudes from normal operations.



- Which method seems to be used in the attack?

```
Initially an influx of GET requests occurred at 6:00pm followed by  POST requests at 8:00pm
```

- At what times did the attack start and stop?

```
The attack began at 5:00pm and stopped at 9:00pm on 3/25/2020.
   ● GET requests started at 5:00pm and stopped at 7:00pm
   ● POST requests started at 7:00pm and stopped at 9:00pm
```

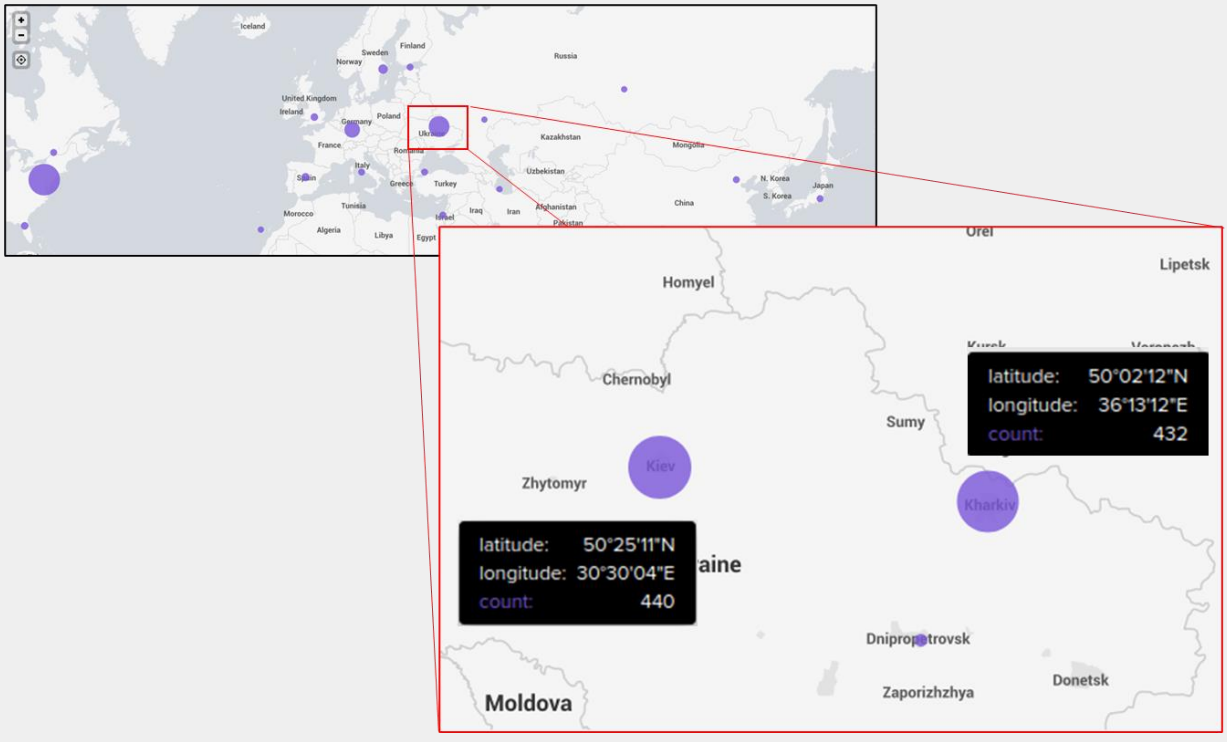
- What is the peak count of the top method during the attack?

```
GET = 729
POST = 1296
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

```
Yes, Ukraine stands out in the cluster maps. The heat map of activity grows
from a normal operational day to the day of the attack on 3/25/2020.
```



- *Apache Attack - 3/25/2020*

- *Normal Operations*

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

```
The cities of Kiev and Kharkiv saw an increase in the volume of activity.
```

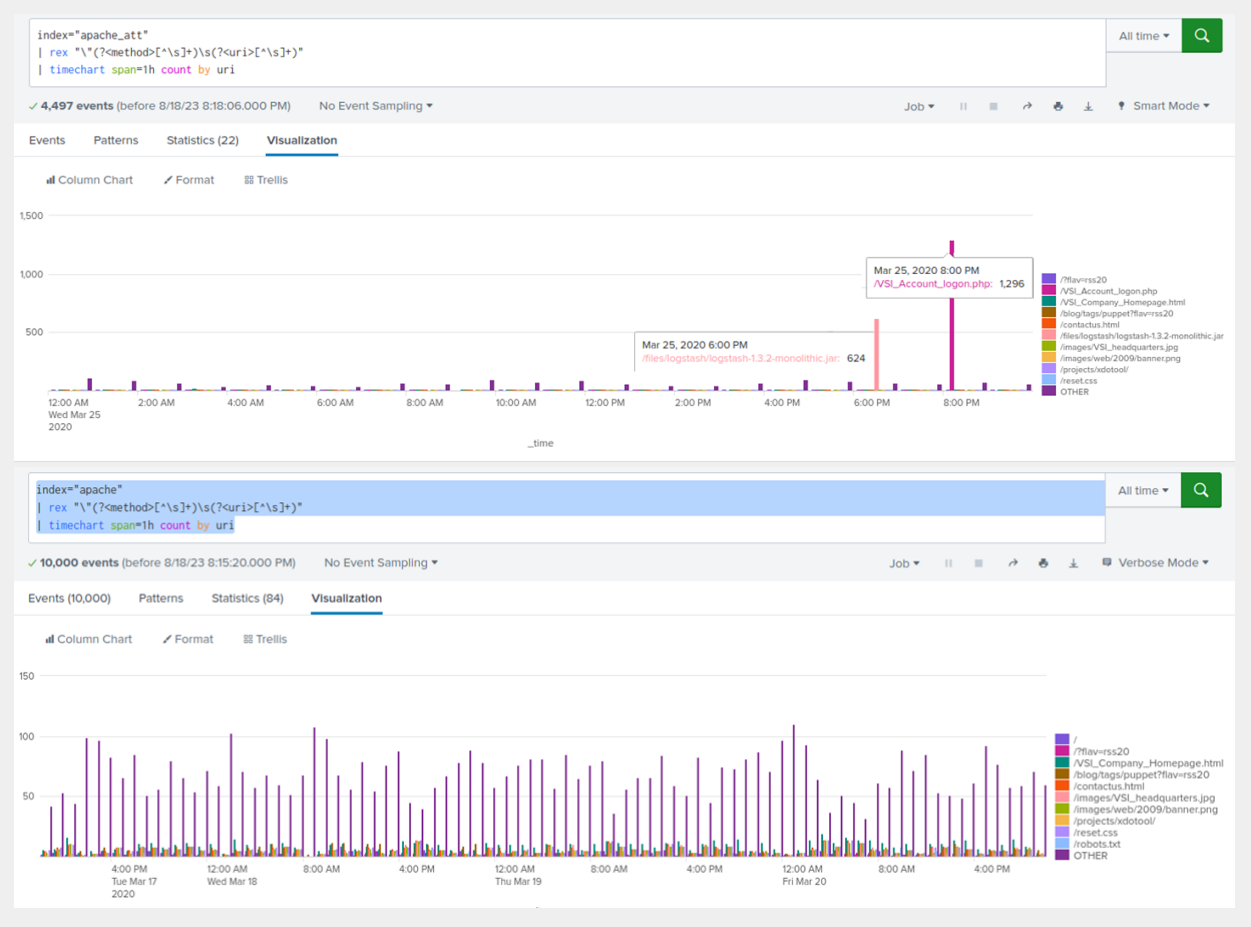
- What is the count of that city?

- The count in Kiev = 440
- The count in Kharkiv = 432

Dashboard Analysis for URI Data

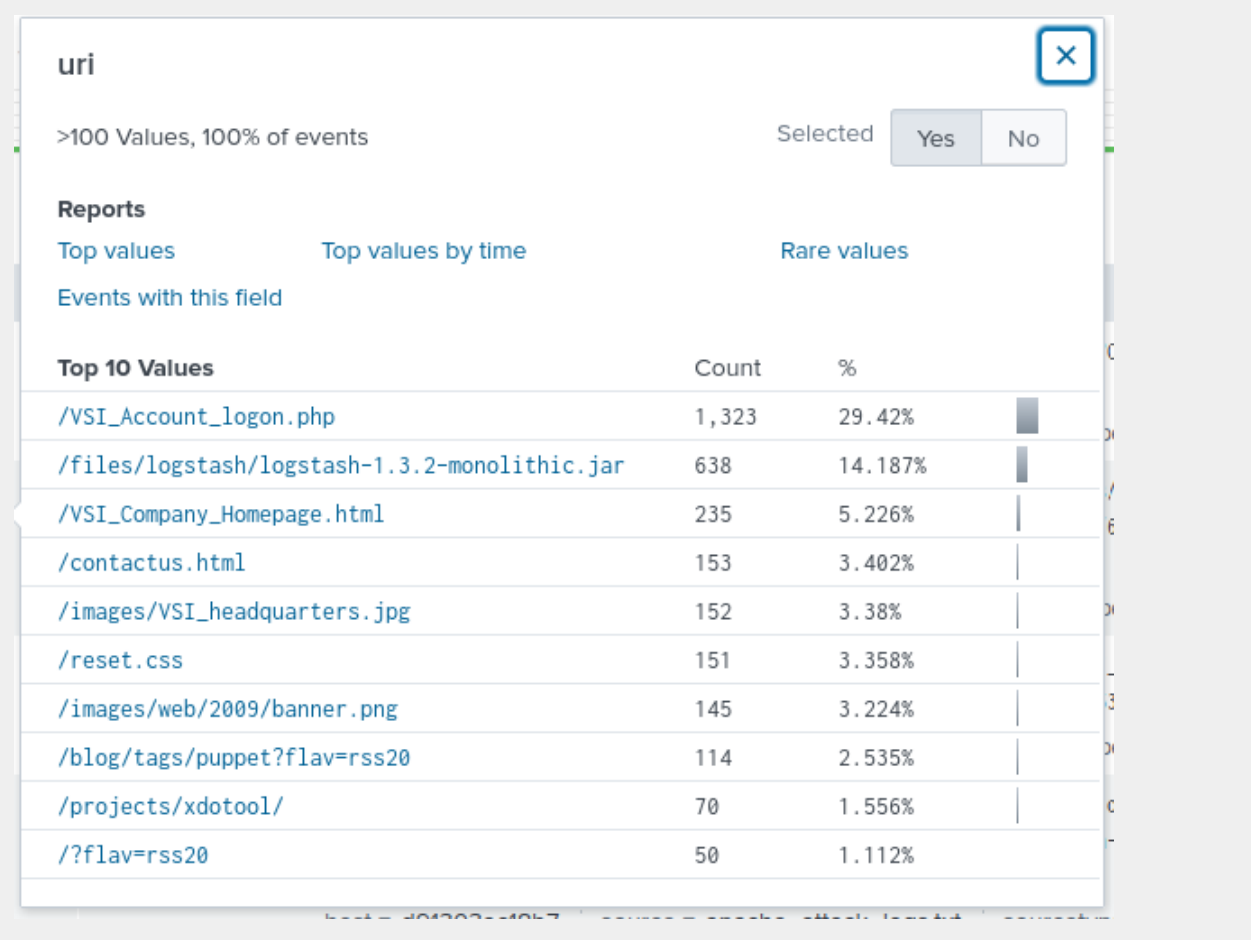
- Does anything stand out as suspicious?

```
Yes, the URI “/VSI_Account_logon.php” is
```



- What URI is hit the most?

The URI hit the most was “**/VSI_Account_logon.php**”. This URI was hit 1323 times.



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

Given the number of hits to /VSI_Account_logon.php it could possibly be a denial of service attack by brute forcing the VSI logon page. Given that the URI “/files/logstash/logstash-1.3.2-monolithic.jar” was also hit with more than normal activity, maybe the attacker was trying to break in access the “.jar” file to hide a virus, reconfigure a system under, then hide their tracks a brute force on the “.php” file.