Cybersecurity

Project 3 Review Questions

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

Windows Server Log Questions

Note:

- Some screenshots have been included in this report. Please refer to the Presentation for further screenshots of our reports, alerts and dashboards.

Report Analysis for Severity

- Did you detect any suspicious changes in severity?

After analyzing the logs, we detected an increase in High ‘severity’, which increased to 1,111 from 329.

Report Analysis for Failed Activities

- Did you detect any suspicious changes in failed activities?

Wed March 25th 20202, 8.30am there was a small spike of failed activity. The rest of the day there were only small incidents.

Alert Analysis for Failed Windows Activity

- Did you detect a suspicious volume of failed activity?

Wed March 25th 2020, 8.30am there was a small spike of failed activity. The rest of the day there were only small incidents.

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

35

- When did it occur?

Failed activities began on an upward trend from 11:00 pm March 24th 2020. Full recovery at 2:00 pm on the 25th of March 2020.

The actual attack is most likely at 8:00 am on Wed March 25th 2020.

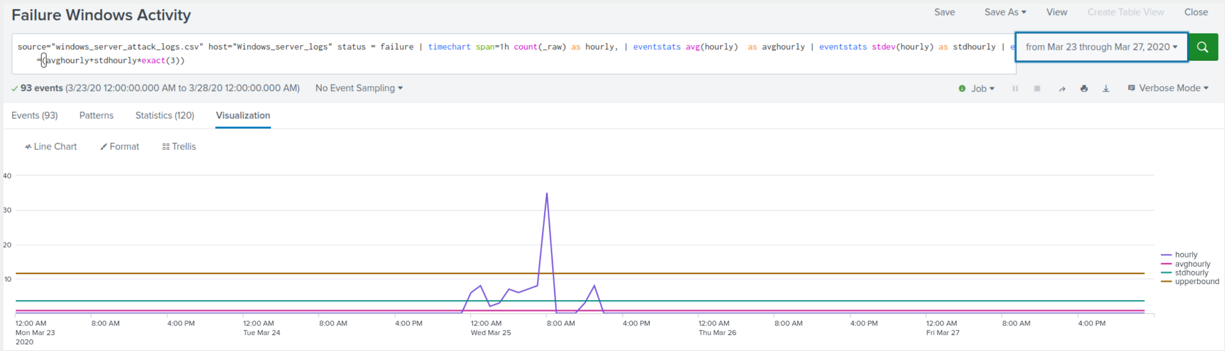
- Would your alert be triggered for this activity?

The trigger threshold was 12 and would have captured this activity in an alert.

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

No, we would not change our threshold in this situation.

It's possible some of the failures could have been early attempts at an attack. However, they were still in the vicinity of normal activity and changing the threshold could create alert fatigue.



Failure Windows Activity

```
source="windows_server_attack_logs.csv" host="Windows_server_logs" status = failure | timechart span=1h count(_raw) as hourly, | eventstats avg(hourly)  as avghourly | eventstats stdev(hourly) as stdhourly | e
    =(avghourly+stdhourly*exact(3))
```

✓ 93 events (3/23/20 12:00:00.000 AM to 3/28/20 12:00:00.000 AM)

Alert Analysis for Successful Logins

- Did you detect a suspicious volume of successful logins?

Yes, there was a suspicious number of successful logins for ‘user_j’ between 11:00 am and 12:00 pm.

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

196 successful logins at 11:00 am
75 successful logins at 12:00 pm

- Who is the primary user logging in?

‘User_j’

- When did it occur?

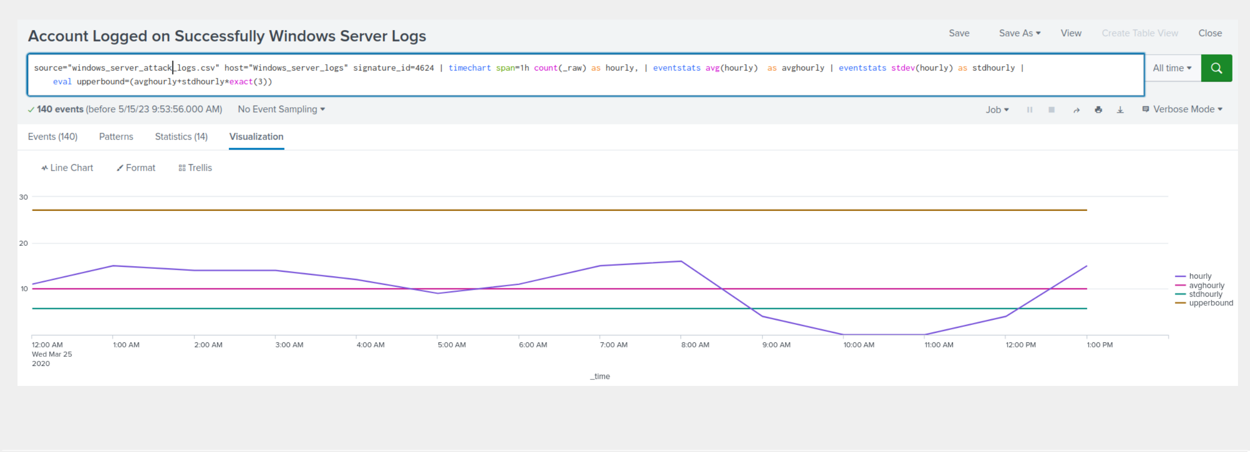
11:00 am and 12:00 pm Wed, March 25 2020

- Would your alert be triggered for this activity?

Alert threshold of ‘greater than 21’ would have detected this suspicious event if we had used the signature name rather than ID.
Interestly these login attempts were not captured when using the alert with the signature id as the source. The 196 successful login attempts were only captured when using the signature name.

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

We would keep the threshold the same at greater than 21 however we would rethink the alert creation. Knowing now that signature id did not pick up user_k’s log in activity after the attack.



```
source="windows_server_attack_logs.csv" host="Windows_server_logs" signature_id=4624 | timechart span=1h count(_raw) as hourly, | eventstats avg(hourly)  as avghourly | eventstats stdev(hourly) as stdhourly |
    eval upperbound=(avghourly+stdhourly*exact(3))
```

✓ 140 events (before 5/15/23 9:53:56.000 AM) No Event Sampling ▾

Alert Analysis for Deleted Accounts

- Did you detect a suspicious volume of deleted accounts?

```
No, a suspicious volume of deleted accounts were not detected.
```

Dashboard Analysis for Time Chart of Signatures

- Does anything stand out as suspicious?

```
In the ‘business as usual’ data, all of the Signatures are within the 10-20
events per hour range. After ingesting the attack logs and analyzing, it is
clear that there is a significant increase in 3 signature types. Refer to
the below for further information.
```

- What signatures stand out?

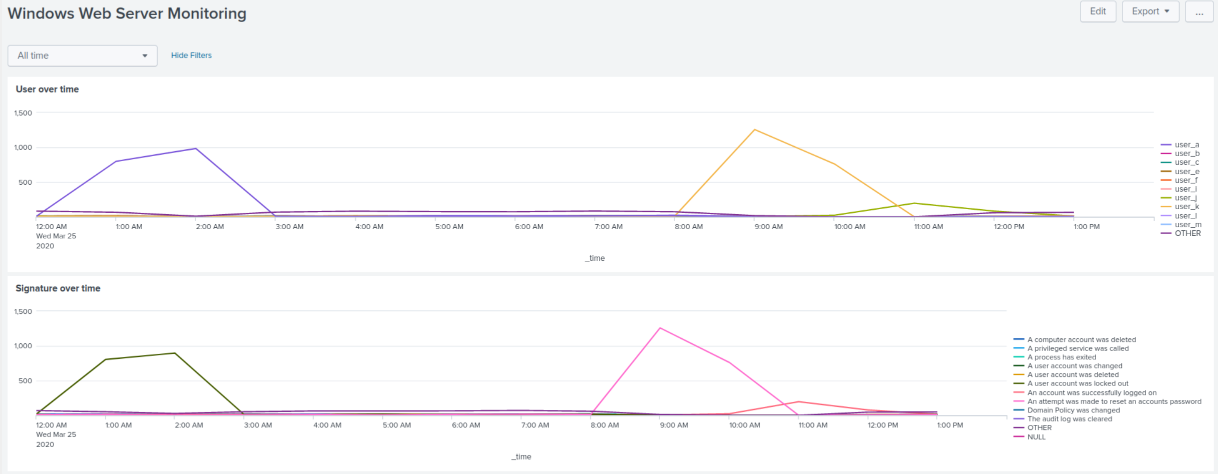
```
● A user account was locked out
● An attempt was made to reset an accounts password
● An account was successfully logged on
```

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

```
● Account Lockouts: 1:00 am to 2:00 am. Recovery at 3:00 am.
● Account password resets: 9:00 am to 10:00 am. Recovery at 11:00 am.
● Successful log on: 11:00 am to 12:00 pm.Recovery at 1:00 pm.
```

- What is the peak count of the different signatures?

```
Account Lockout Peak: 896
Account Password Reset: 1258
```



Dashboard Analysis for Users

- Does anything stand out as suspicious?

```
There is a large volume of activity from ‘User_a’, ‘User_k’ and ‘user_j’ at
various hours on March 25 2020.
```

- Which users stand out?

```
‘User_a’, ‘User_k’ and ‘user_j’
```

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

```
User_a: from 1:00 am to 2:00 am
User_k: from 9:00 am to 10:00 am
User_j: from 11:00 am to 12:00 pm
```

- What is the peak count of the different users?

```
User_a: 984
```

User_k: 1,256
User_j: 271

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

- Does anything stand out as suspicious?

Lockout, Password Reset and Successful Login Events stand out as suspicious when compared to the ‘business as usual’ data:

- Lockout: 1,811
- Password Reset: 2,128
- Successful Login: 273

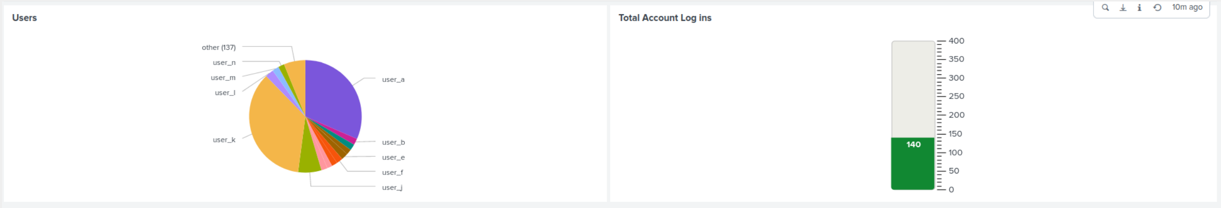
- Do the results match your findings in your time chart for signatures?

Yes the increases do match up. The signature bar grabs all of the counts so it is higher than the single peaks.

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

- Does anything stand out as suspicious?

The users with the largest login attempts are clear from the ‘pie graph’ visualization; ‘user_a’ and ‘user_k’ have the most activity.



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

The results from signature dashboard analysis verify the findings from the users timecharts.

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?

If the above question is in regards to using reports over inline analytics then the advantage of a report is it is essentially a saved search, they are bespoke and don't take up more of your apps namespace while the advantage of inline is that you can convert and reuse it for other common inputs.

Furthermore, reports are useful for viewing small amounts of data, but cannot provide useful insights for large amounts of data and comparisons to other data types (in this case, comparison to other users and events). Using the visualization panels created in the dashboard, it is easy to see abnormalities when compared with other users/events.

Apache Web Server Log Questions

Report Analysis for Methods

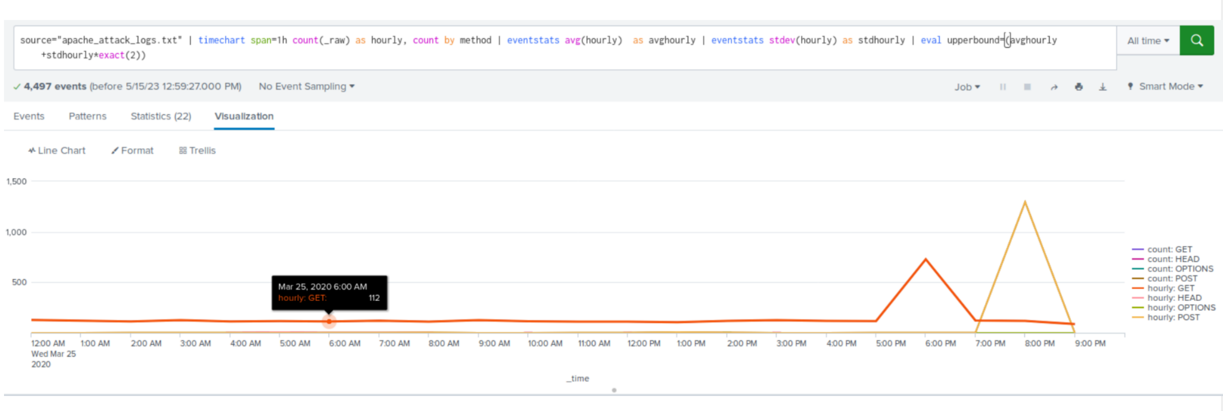
- Did you detect any suspicious changes in HTTP methods? If so, which one?

GET and POST requests increased dramatically. GET requests went from an average of roughly 120 per hour to 729 and POST requests increased from a rough average of 2 per hour to 1,296. Both of these increases occurred at similar times, starting with GET requests beginning at 5:00 pm, reaching its apex at 6:00 pm and returning to normal by 7:00 pm. POST requests begin climbing at 7:00 pm, peaking at 8:00 pm and returning to normal by 9:00 pm.

- What is that method used for?

GET requests are to retrieve information from a web server and do not affect the server state, however if done maliciously can result in sensitive data being leaked.

POST requests are essentially when a client is sending data to the web server and can result in the server state being affected. This method can be used to infiltrate and compromise a web server if done maliciously.



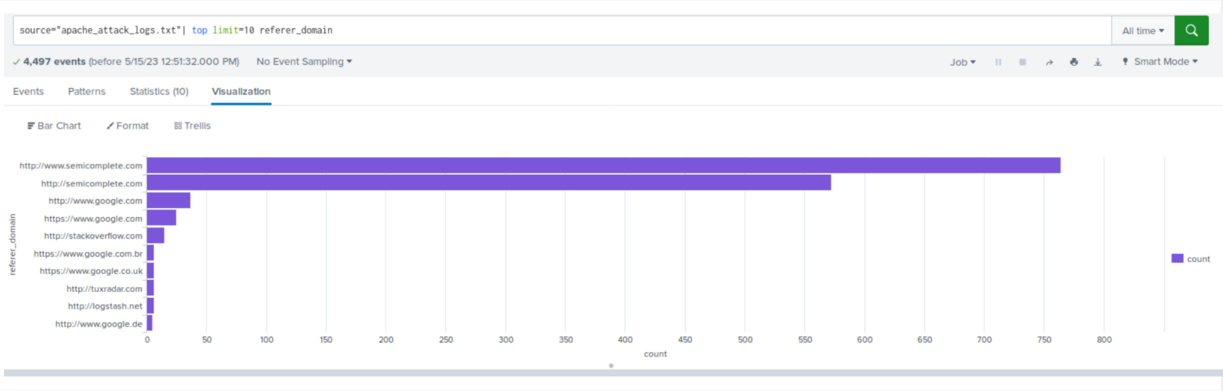
```
source="apache_attack_logs.txt" | timechart span=1h count(_raw) as hourly, count by method | eventstats avg(hourly)  as avghourly | eventstats stdev(hourly) as stdhourly | eval upperbound=(avghourly
    +stdhourly*exact(2))
```

✓ 4,497 events (before 5/15/23 12:59:27.000 PM)

Report Analysis for Referrer Domains

- Did you detect any suspicious changes in referrer domains?

There was a significant reduction in the count of referrer domains with the results being almost a quarter of when compared with typical results. The actual sources of the domains remained similar if not the same.



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

✓ 4,497 events (before 5/15/23 12:51:32.000 PM)

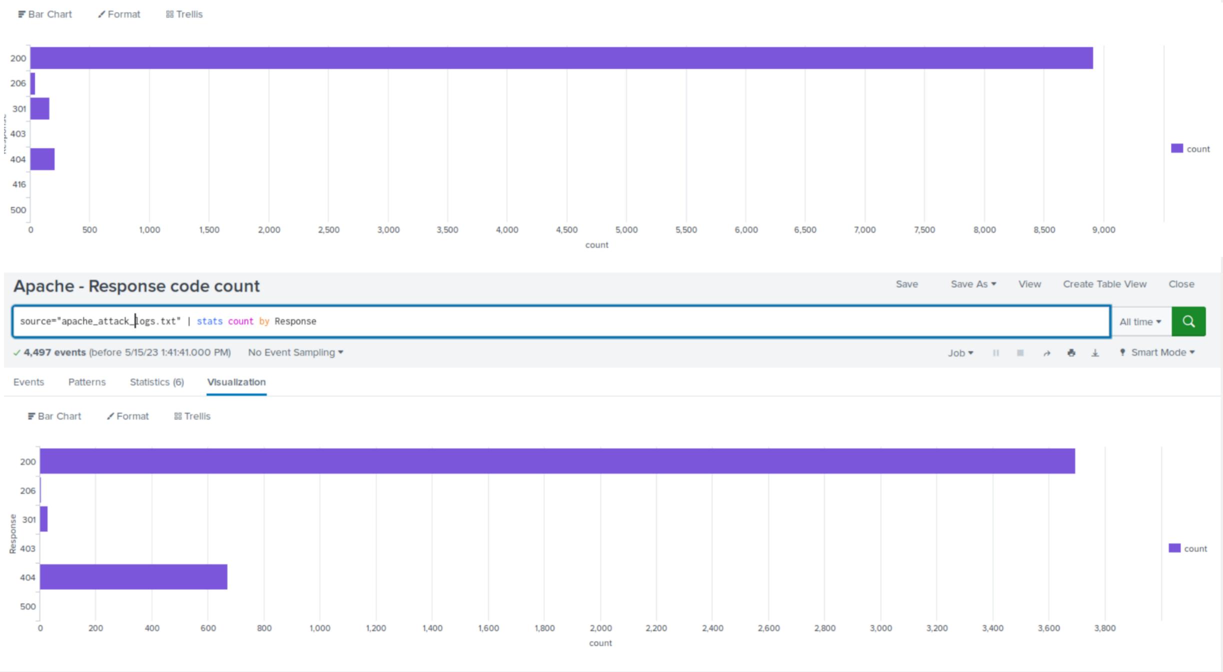
Report Analysis for HTTP Response Codes

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

```
Attack response codes:            200, 206, 301, 403, 404, 500
Typical Traffic response codes:   200, 206, 301, 403, 404, 416, 500
```

```
The response codes seemed typical except for the absence of a couple of 416
responses, what was noticeable was the significant relative increase in
‘404’ responses:

  ● 4,497 events with 671 of those events represented by ‘404’ responses;
  ● 10,000 events with 205 of those events represented by 404 responses).
```



Apache - Response code count

```
source="apache_attack_logs.txt" | stats count by Response
```

✓ 4,497 events (before 5/15/23 1:41:41.000 PM) No Event Sampling

Alert Analysis for International Activity

- Did you detect a suspicious volume of international activity?

```
Yes, the alert would have triggered at between 7pm and 8pm on the 25th of
March 2020. The alert was set to trigger when the count per hour exceeded
125 and at 8pm the number of results peaked at 939 within the hour.
```

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

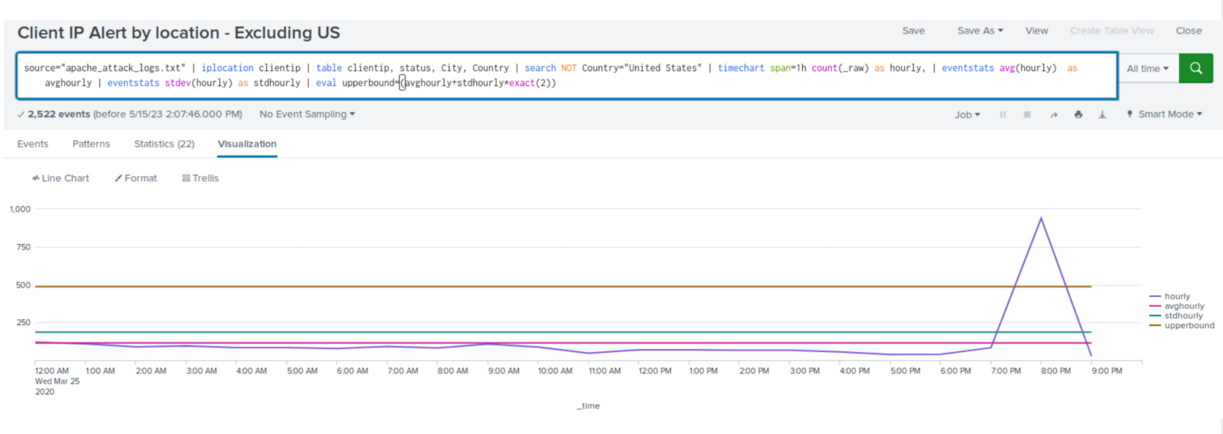
```
939
```

- Would your alert be triggered for this activity?

```
Yes
```

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

```
No, the pre-configured alert would have detected this activity.
```



Client IP Alert by location - Excluding US

```
source="apache_attack_logs.txt" | iplocation clientip | table clientip, status, City, Country | search NOT Country="United States" | timechart span=1h count(_raw) as hourly, | eventstats avg(hourly)  as
    avghourly | eventstats stdev(hourly) as stdhourly | eval upperbound=(avghourly+stdhourly*exact(2))
```

✓ 2,522 events (before 5/15/23 2:07:46.000 PM) No Event Sampling ▾

Alert Analysis for HTTP POST Activity

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

```
Yes. There was a dramatic increase in POST requests that would have well
exceeded the alert threshold of 4. The peak of POST requests occurred at
8:00 pm with a count of 1,296.
```

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

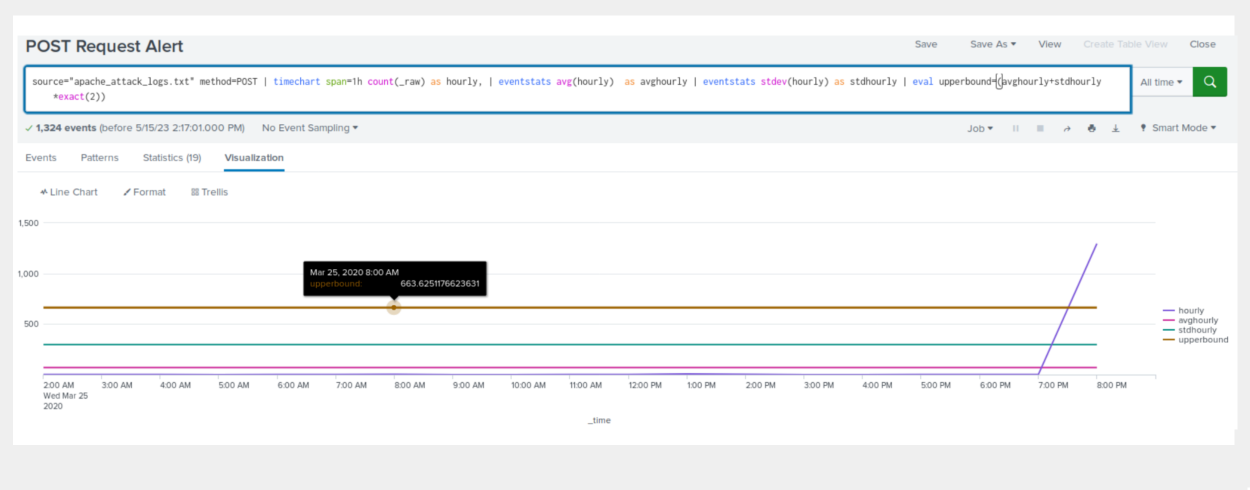
```
1,296
```

- When did it occur?

```
Between 7:00 pm and 8:00 pm.
```

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

```
No, the alert captured the suspicious increase in requests.
```


POST Request Alert

```
source="apache_attack_logs.txt" method=POST | timechart span=1h count(_raw) as hourly, | eventstats avg(hourly)  as avghourly | eventstats stdev(hourly) as stdhourly | eval upperbound=(avghourly+stdhourly
    *exact(2))
```

✓ 1,324 events (before 5/15/23 2:17:01.000 PM)

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious?

```
The GET and POST requests methods are particularly high at 6:00 pm and 8:00
pm respectively.
```

- Which method seems to be used in the attack?

```
GET and POST. The POST requests are concerning with 1,296 requests at 8:00
pm.
```

- At what times did the attack start and stop?

```
The increase in GET requests began between 5:00 pm and 6:00 pm recovering by
7:00 pm.

The increase in POST requests began between 7:00 pm and 8:00 pm and
recovered by 9:00 pm.
```

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

```
1,296 POST requests.
```

Dashboard Analysis for Cluster Map

- Does anything stand out as suspicious?

New activity in odd locations compared to the original baseline; further information below.

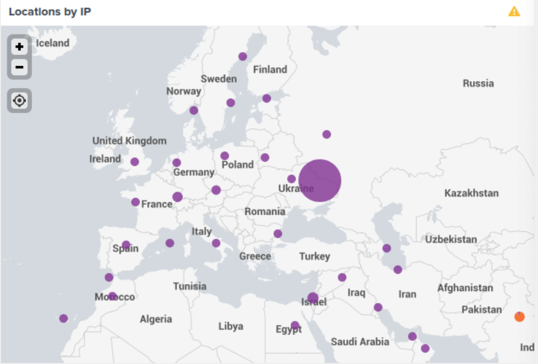
- Which new location (city, country) on the map has a high volume of activity? (**Hint**: Zoom in on the map.)

The following cities/countries have a high volume of activity:

- Osaka, Japan
- Bangalore/New Delhi, India
- Tel Aviv, Israel
- Kharkiv, Ukraine [Kharkiv is noted as having the largest growth in activity]

- What is the count of that city?

Kharkiv, Ukraine: 432



Dashboard Analysis for URI Data

- Does anything stand out as suspicious?

Yes, ‘logon page’ activity coming from Ukraine. It is noted that New York also has a high level of activity but is less concerning given that the customer base is majority US.

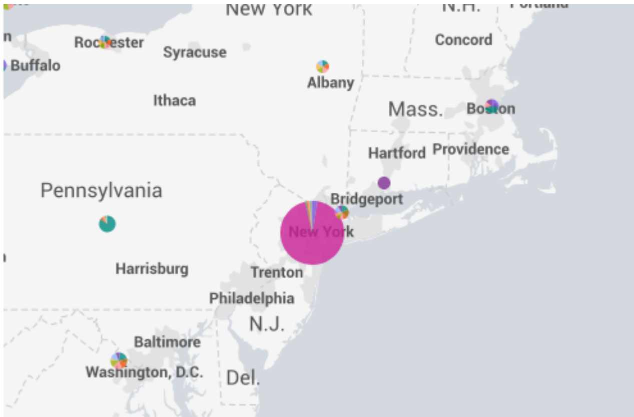
- What URI is hit the most?

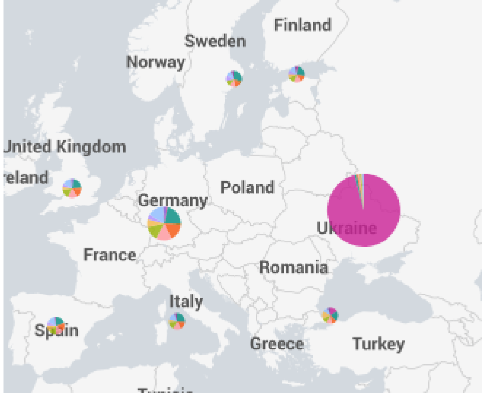
‘Logon Page’ has been hit the most; further stats noted below:

- New York, USA has 432 hits on the ‘logon page’
- Ukraine has 864 hits on the ‘logon page’.

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

Based on the login page URI being targeted, a brute force attack is most likely.


New York
N.H.
Rochester
Syracuse
Buffalo
Concord
Albany
Ithaca
Mass.
Boston
Hartford
Providence
Pennsylvania
Bridgeport
New York
Harrisburg
Trenton
Philadelphia
N.J.
Baltimore
Washington, D.C.
Del.


Finland
Sweden
Norway
United Kingdom
Ireland
Poland
Germany
Ukraine
France
Romania
Italy
Spain
Greece
Turkey