Day 1

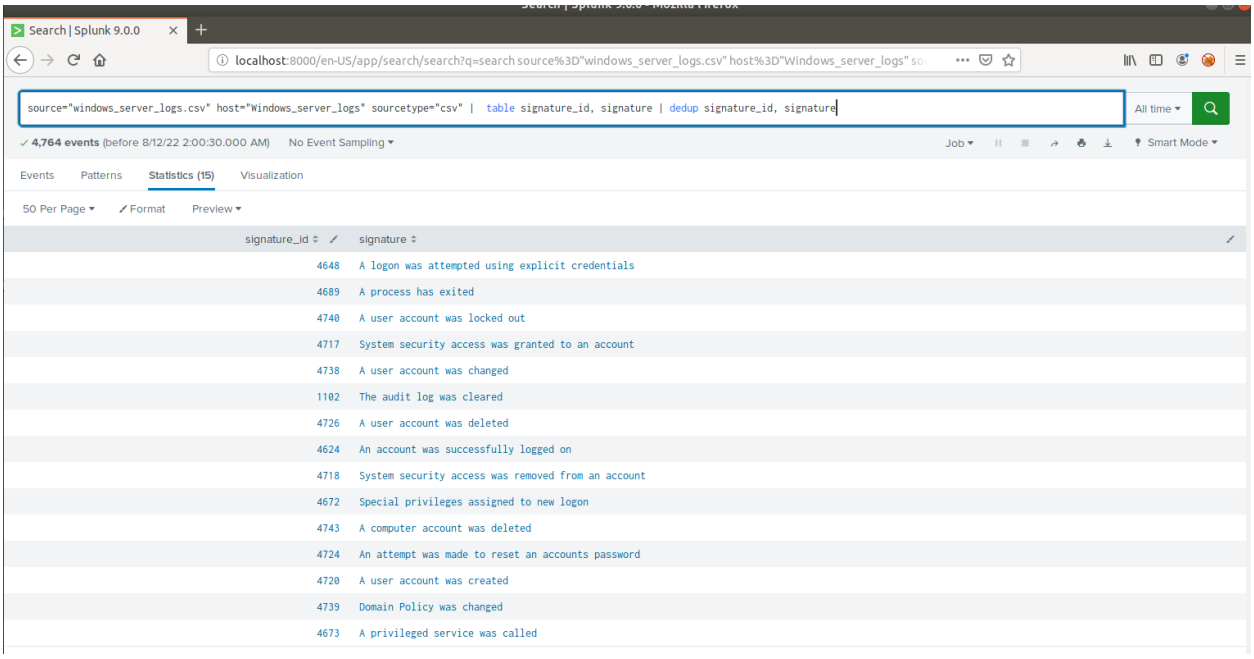
Part 2: Create Reports, Alerts, and Dashboards for the Windows Logs

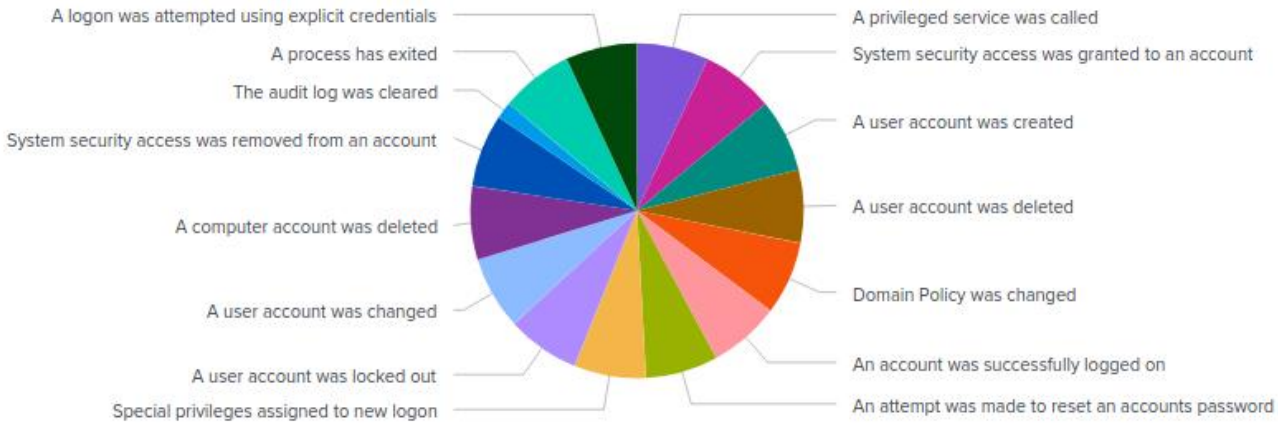
Design the following deliverables to protect VSI from potential attacks by JobeCorp:

Reports: Design the following reports to assist VSI in quickly identifying specific information (be sure to grab screenshots of each report!):

1. A report with a table of signatures and associated signature IDs.

```
source="windows_server_logs.csv" |  table signature, signature_id
| dedup signature, signature_id
```

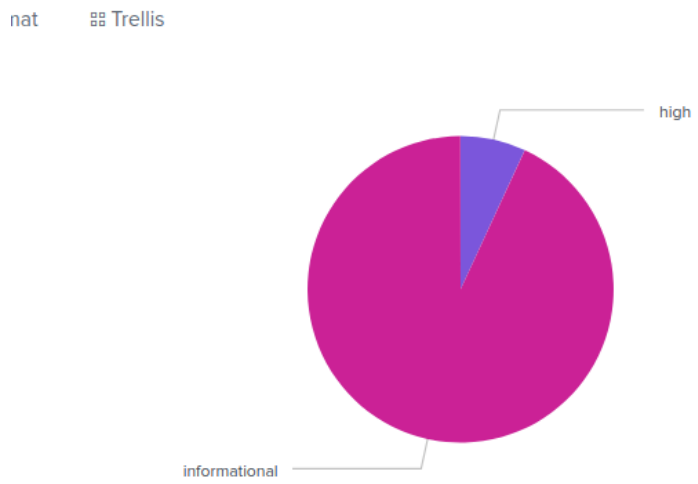


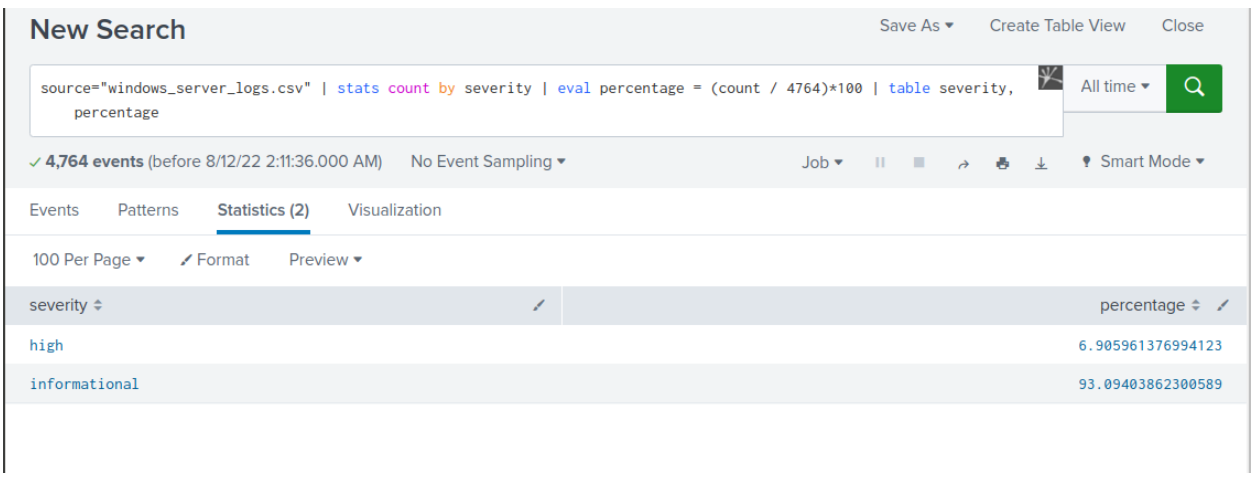


2. A report that displays the severity levels, and the count and percentage of each.

```
source="windows_server_logs.csv" | top limit=20 severity
```

view as pie chart to view as %

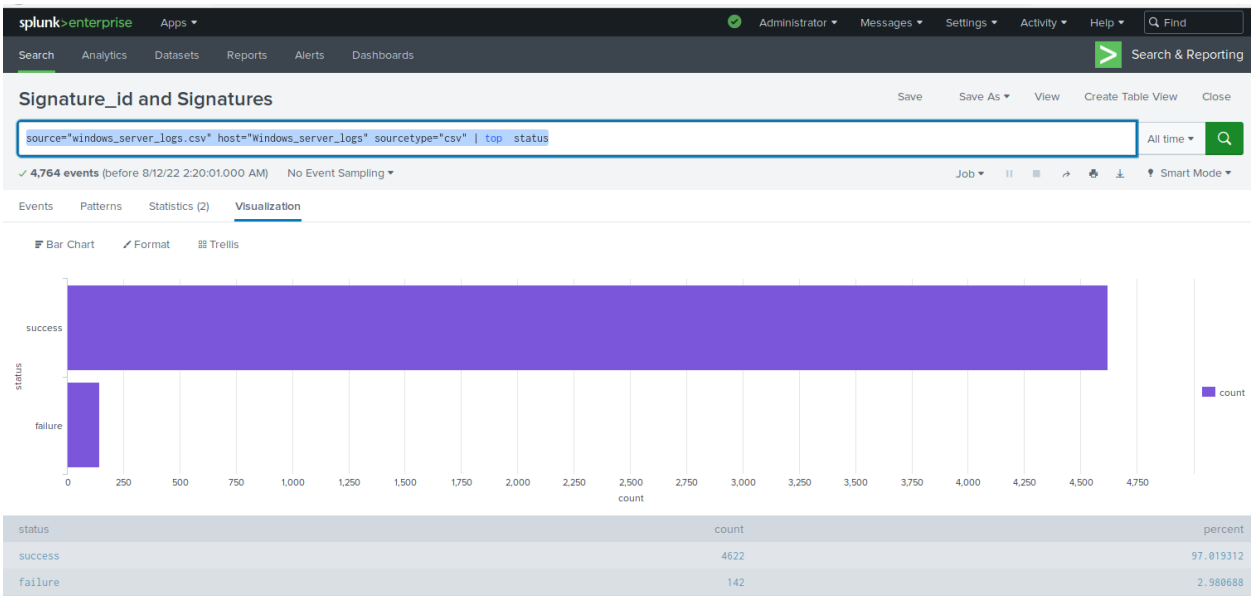


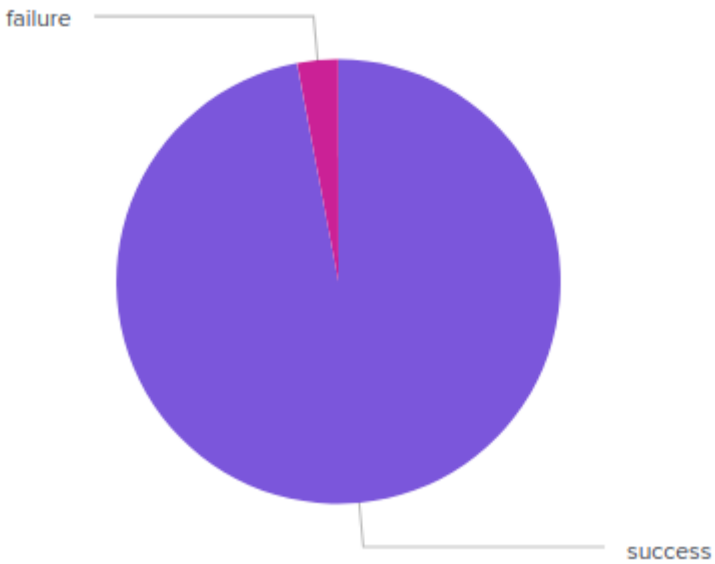


3. A report that provides a comparison between the success and failure of Windows activities.

```
source="windows_server_logs.csv" | top  status
```

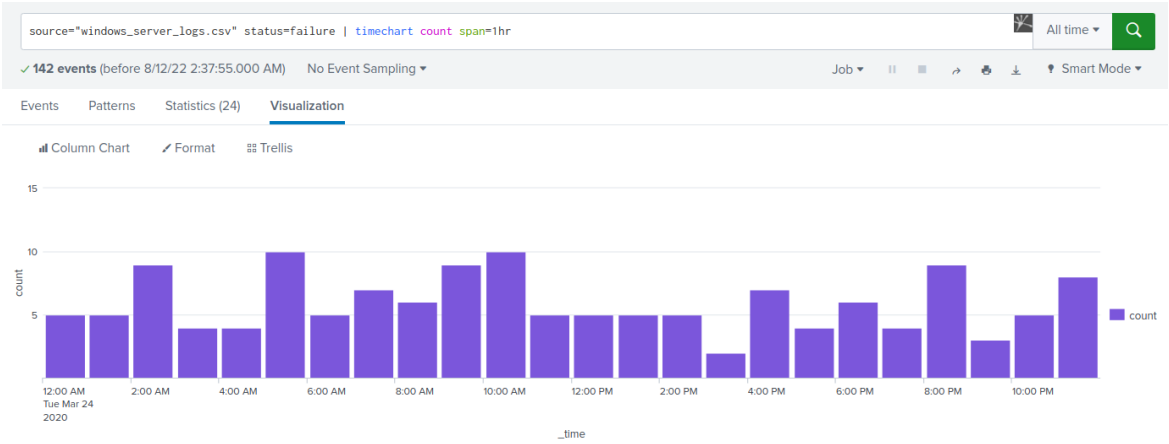
   a. -visualization bar chart





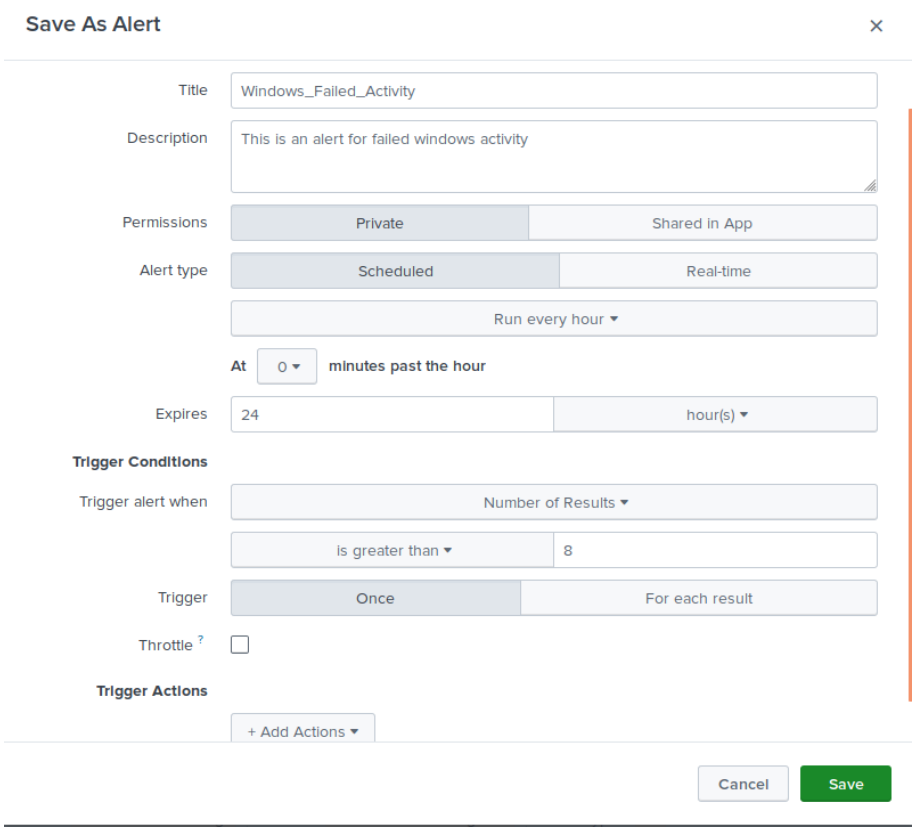
Alerts: Design the following alerts to notify VSI of suspicious activity:

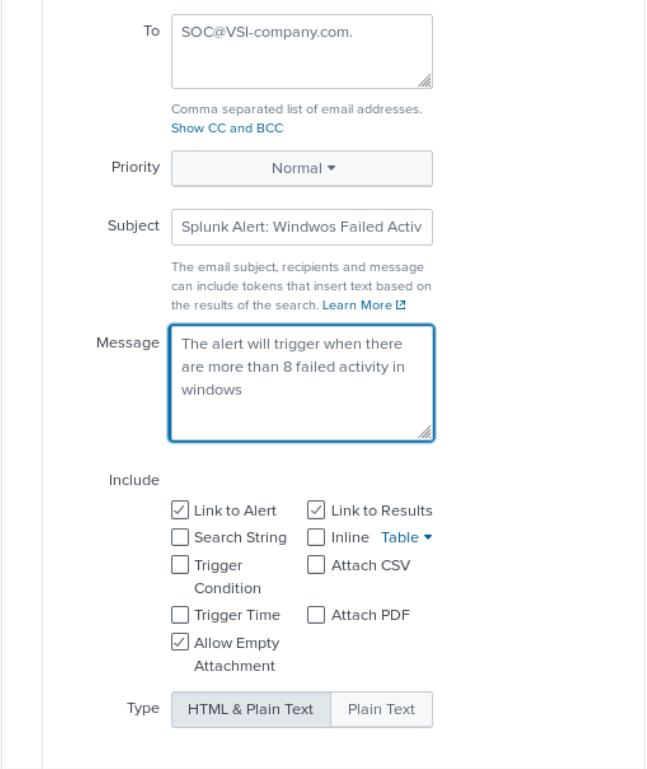
1. Determine a baseline and threshold for the hourly level of failed Windows activity.



Baseline - 6 failed windows activity per hour

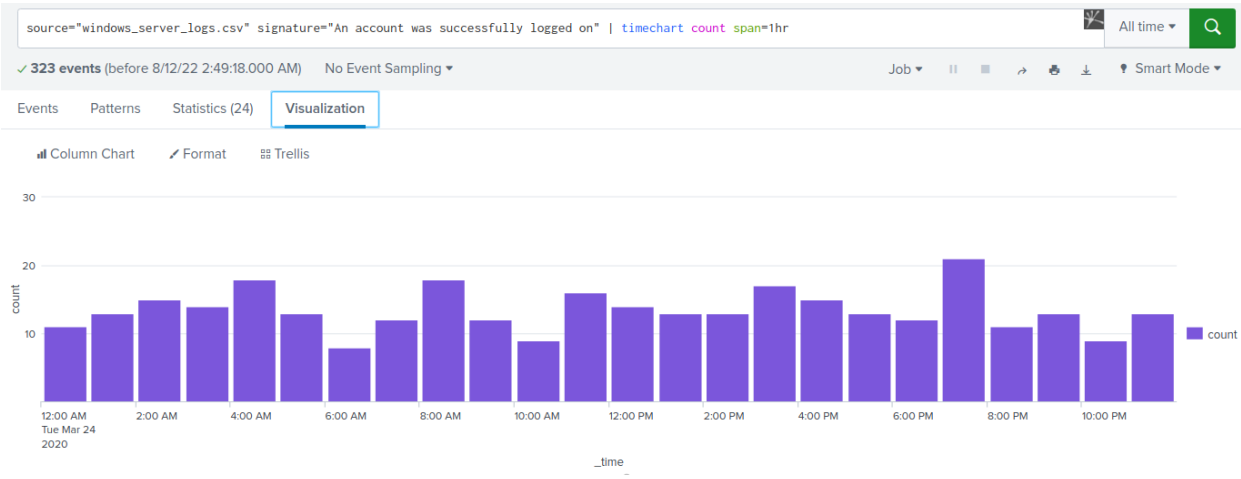
Threshold - 8 failed windows activity per hour





2. Determine a baseline and threshold for the hourly count of the signature "an account was successfully logged on."

```
source="windows_server_logs.csv" signature="An account was successfully logged on" OR signature_id=4624 | timechart count span=1hr
```



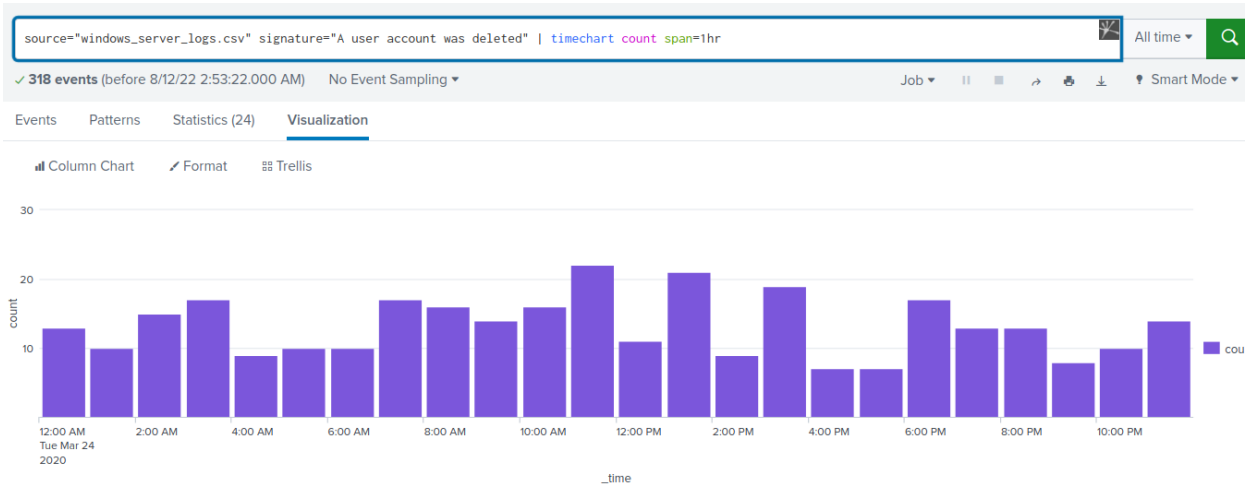
Baseline - 13

Threshold - 16

3. Determine a baseline and threshold for the hourly count of the signature "a user account was deleted."

   Based on signature_id:

```
source="windows_server_logs.csv" signature="A user account was deleted" OR signature_id=4726 | timechart count span=1hr
```



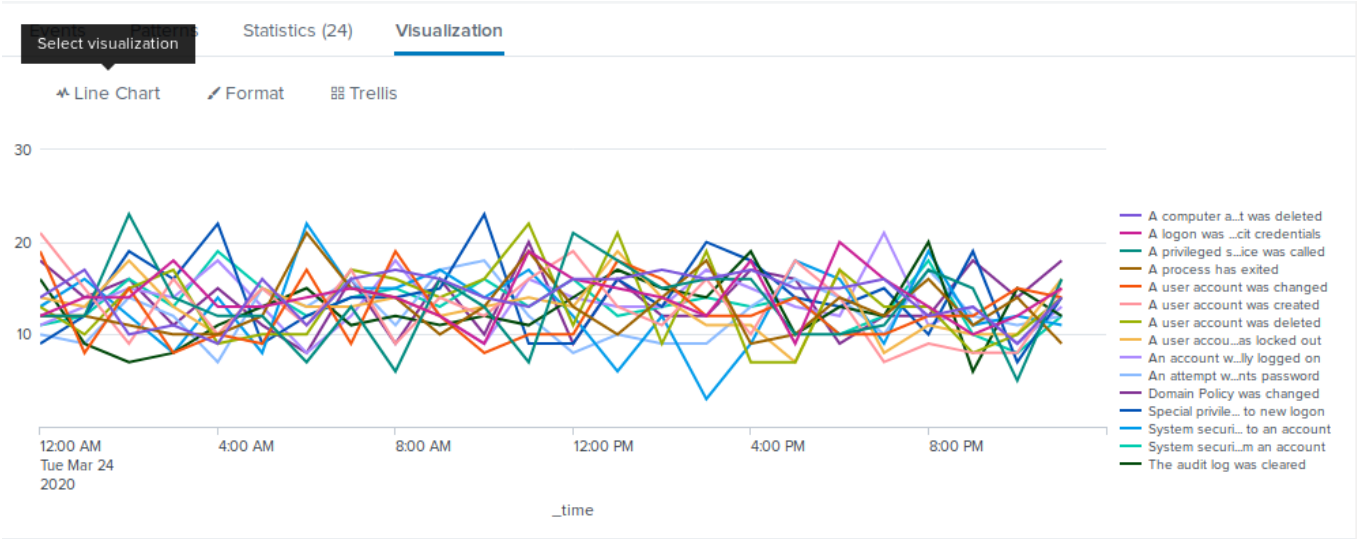
Baseline: 13

Threshold 16

Visualizations and dashboards: Design the following visualizations, and add them to a dashboard called "Windows Server Monitoring" (be creative with your visualizations, and make sure to grab screenshots of each!):

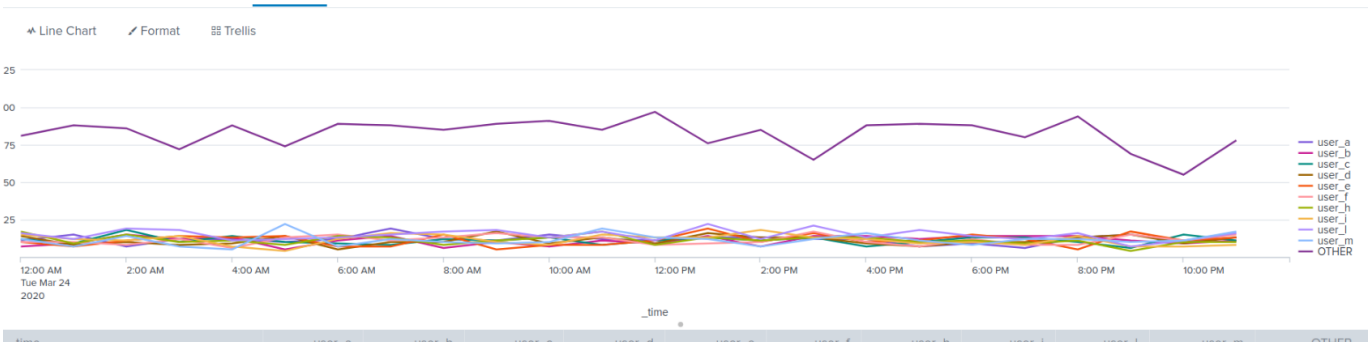
1. A line chart that displays the different "signature" field values over time.

```
source="windows_server_logs.csv" host="Windows_server_logs3"
sourcetype="csv" | timechart span=1hr count by signature limit=15
```



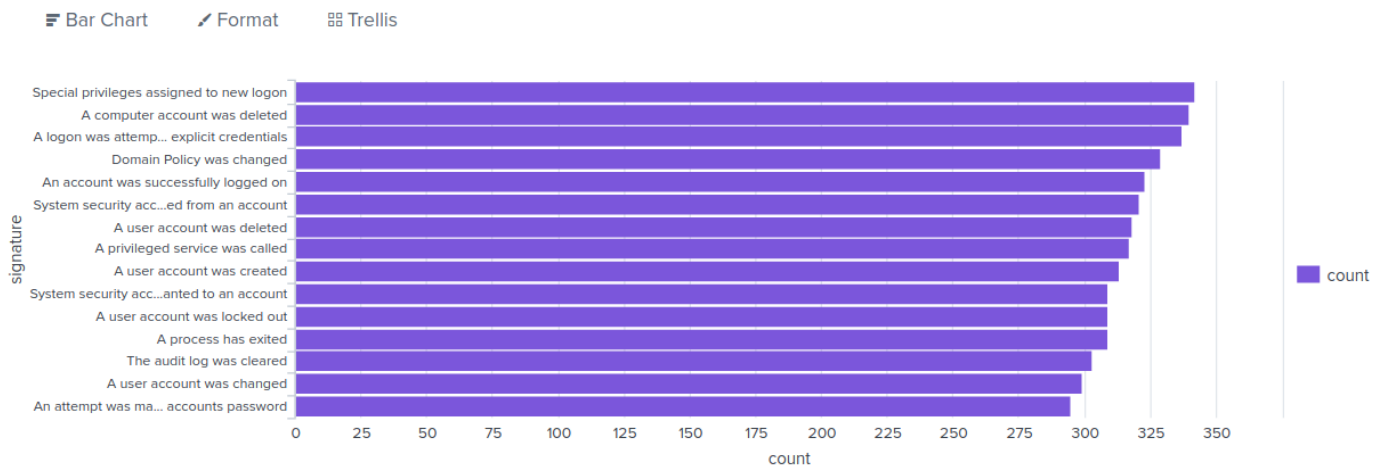
2. A line chart that displays the different "user" field values over time.

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



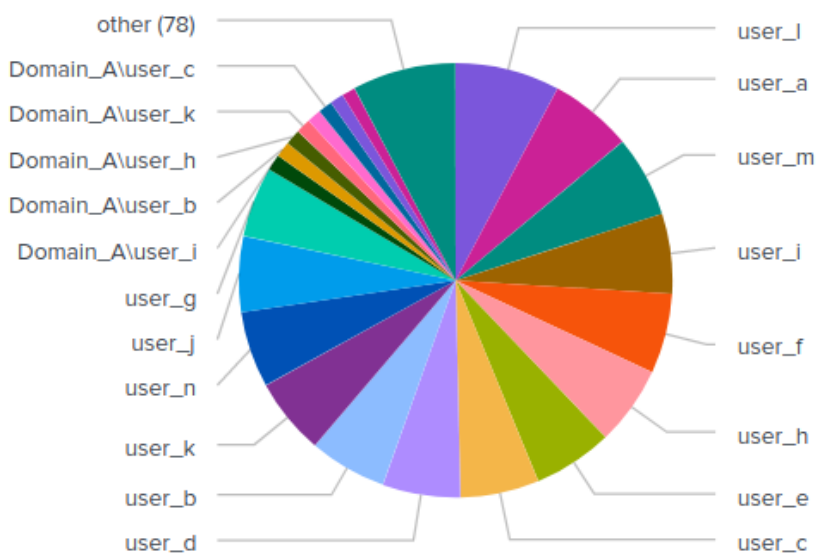
3. Any visualization that illustrates the count of different signatures.

```
source="windows_server_logs.csv" host="Windows_server_logs3"
sourcetype="csv" | top limit=20 signature
```



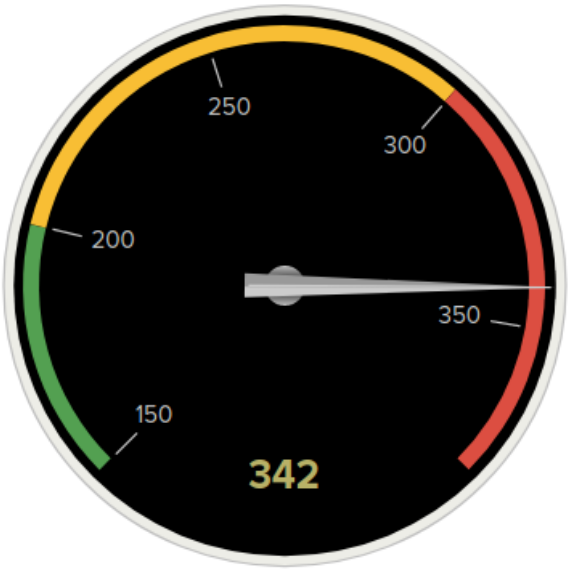
4. Any visualization that illustrates the count of different users.

```
source="windows_server_logs.csv" | top limit=100 user
```

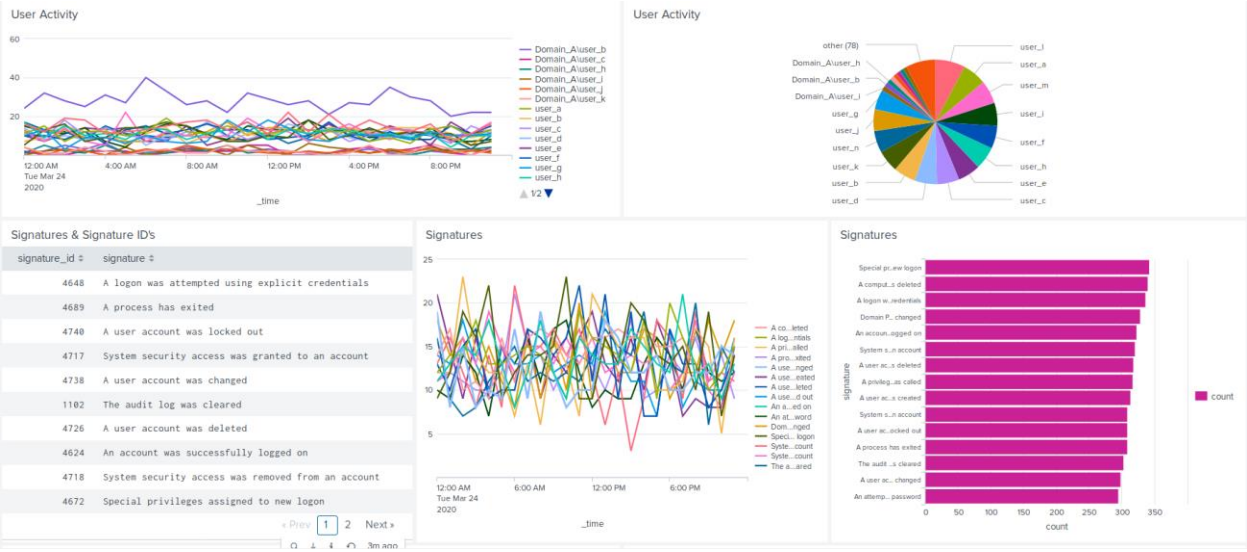


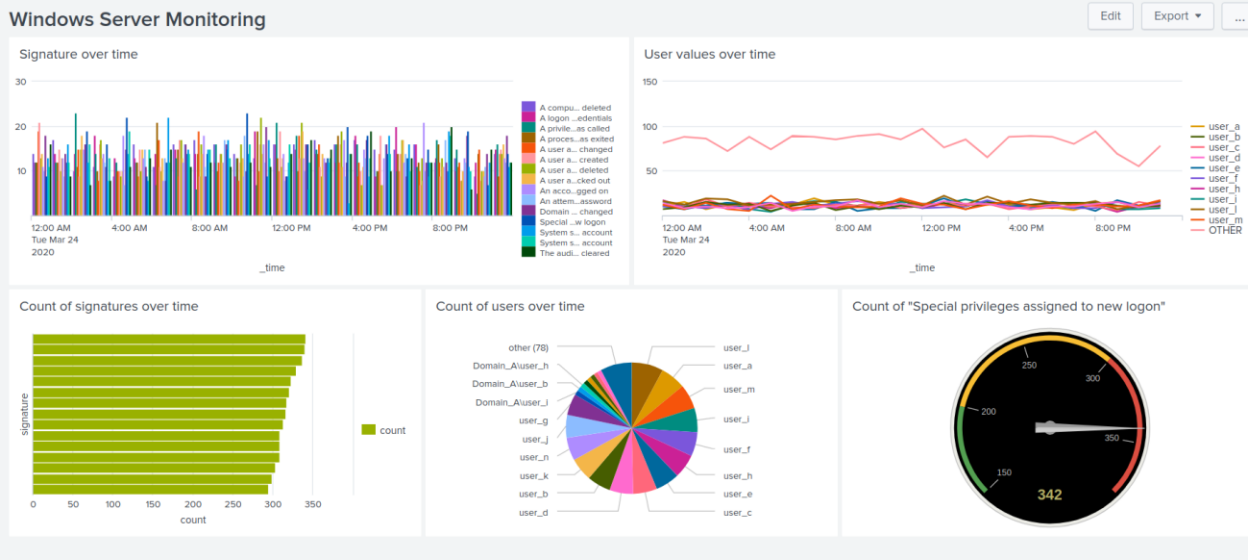
5. Any single-value visualization of your choice that analyzes any single data point—e.g., radial gauge, marker gauge, or a custom visualization from http://localhost:8000/en-US/manager/search/appsremote?content=visualizations&type=app.

```
source="windows_server_logs.csv" signature="Special privileges assigned to new logon" | stats count as sigCount | gauge sigCount 150 200 300 380
```



On your dashboard, add the ability to change the time range for all visualizations.





Part 3: Load and Analyze Apache Logs

In this part, you will upload and analyze Apache web server logs that represent "regular" activity for VSI into your Splunk environment. To do so, complete the following steps:

Select the apache_logs.txt file located in the /splunk/logs/Week-2-Day-3-Logs/ directory.

Briefly analyze the logs and the available fields, specifically examining the following important fields:

- method
- referer_domain
- status
- clientip
- Useragent

Part 4: Create Reports, Alerts, and Dashboards for the Apache Logs

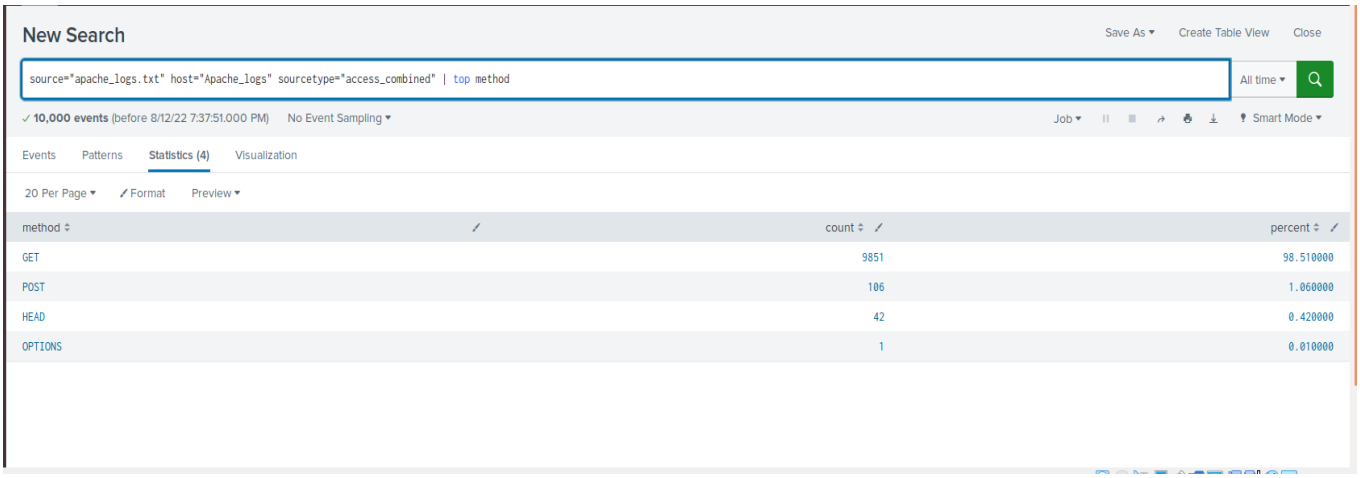
In this part, you will create reports, alerts, and dashboards to monitor for suspicious activity against VSI's Apache web server. To do so, complete the following steps:

Design the following deliverables to protect VSI from potential attacks by JobeCorp:

Reports: Design the following reports to assist VSI in quickly identifying specific information (make sure to grab screenshots of each report):

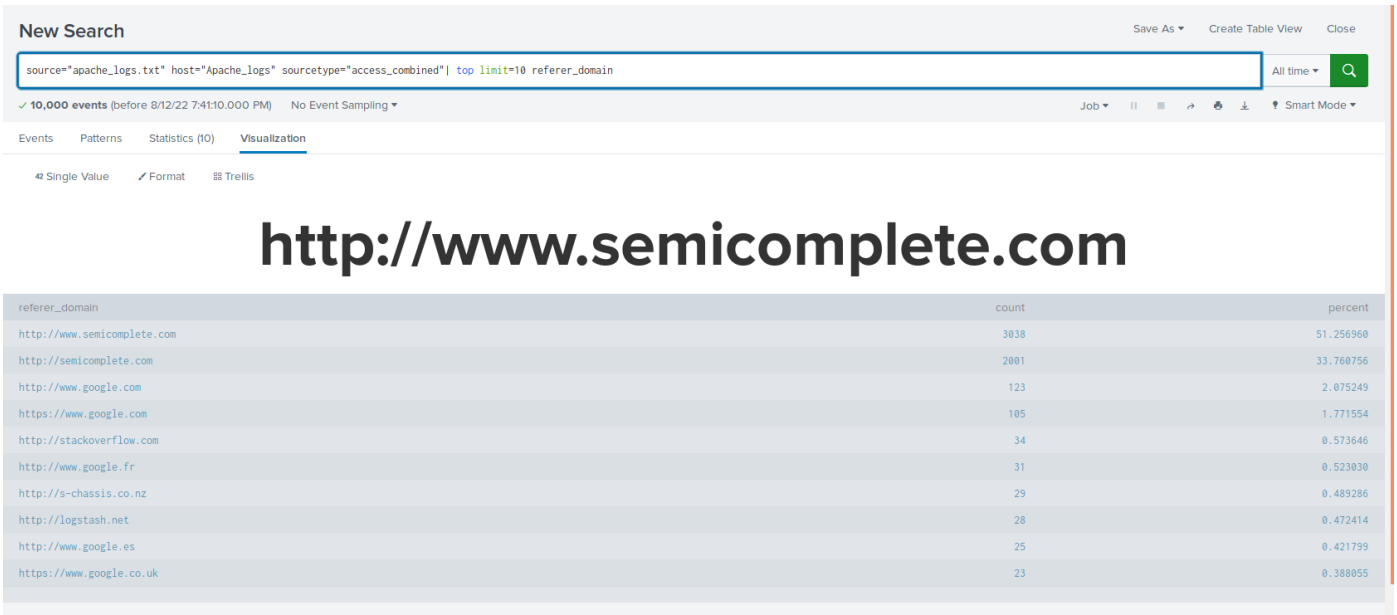
1. A report that shows a table of the different HTTP methods (GET, POST, HEAD, etc.).

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



2. A report that shows the top 10 domains that refer to VSI's website.

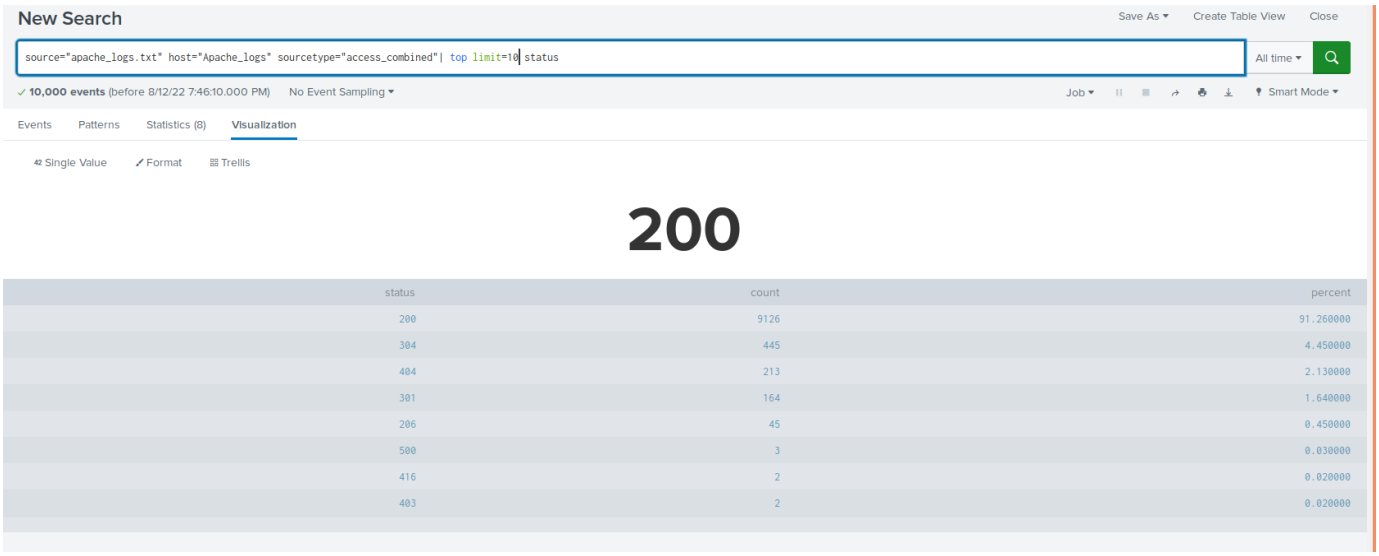
```
source="apache_logs.txt" | top limit=10 referer_domain
```



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

3. A report that shows the count of each HTTP response code.

```
source="apache_logs.txt" | top limit=10 status
```



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

Alerts: Design the following alerts:

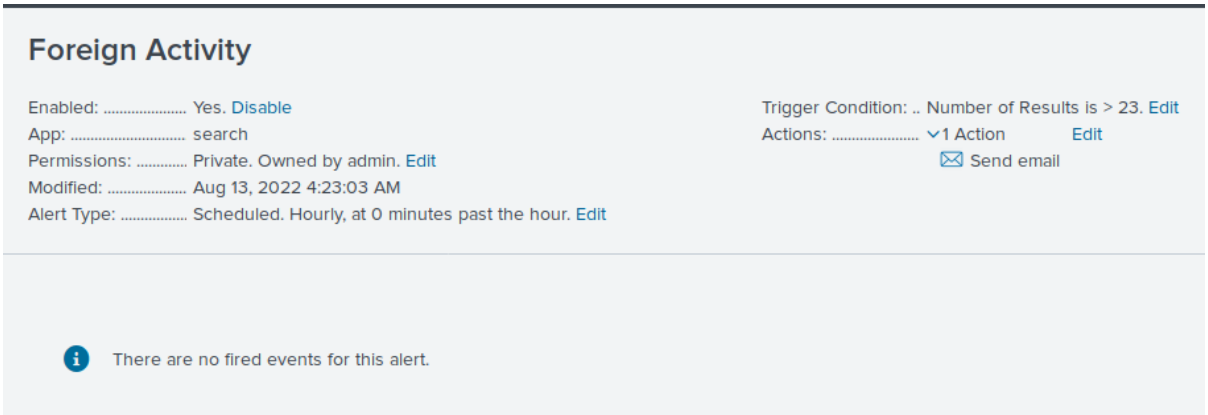
1. Determine a baseline and threshold for hourly activity from any country besides the United States.

- Create an alert that's triggered when the threshold has been reached.

  Baseline: 15 Threshold: 23

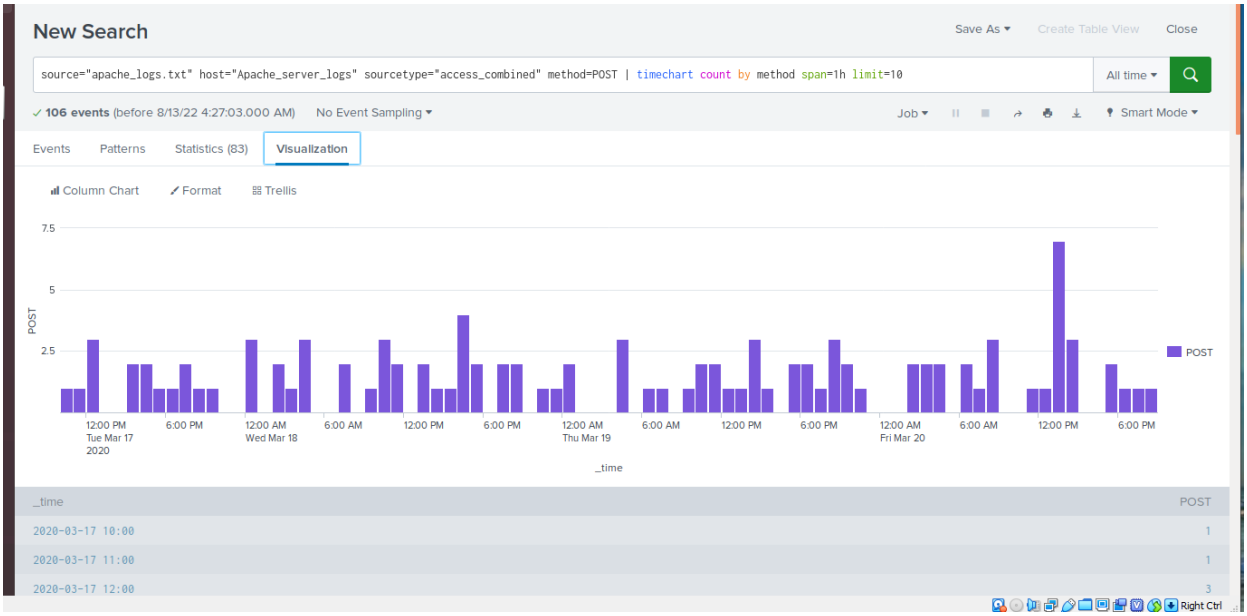
  ```
  source="apache_logs.txt" | iplocation clientip| timechart count by Country span=1h limit=100 | fields - "United States"
  ```

  The alert should trigger an email to SOC@VSI-company.com.



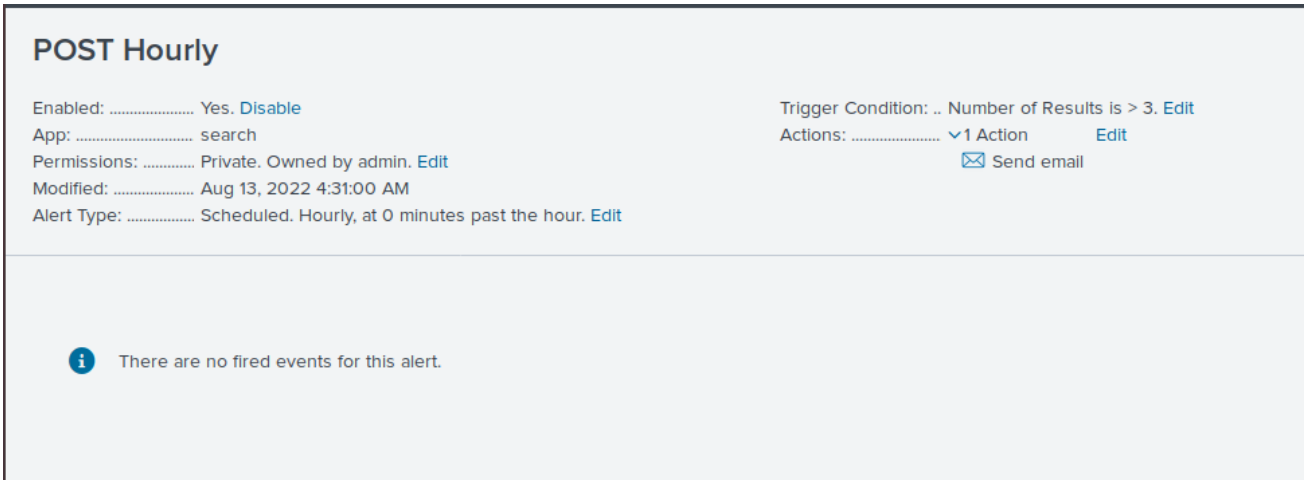
1. Determine an appropriate baseline and threshold for the hourly count of the HTTP POST method.

```
source="apache_logs.txt" method=POST | timechart count by method span=1h limit=10
```



Baseline: 2.5 Threshold: 5

Create an alert that's triggered when the threshold has been reached.



The alert should trigger an email to SOC@VSI-company.com.

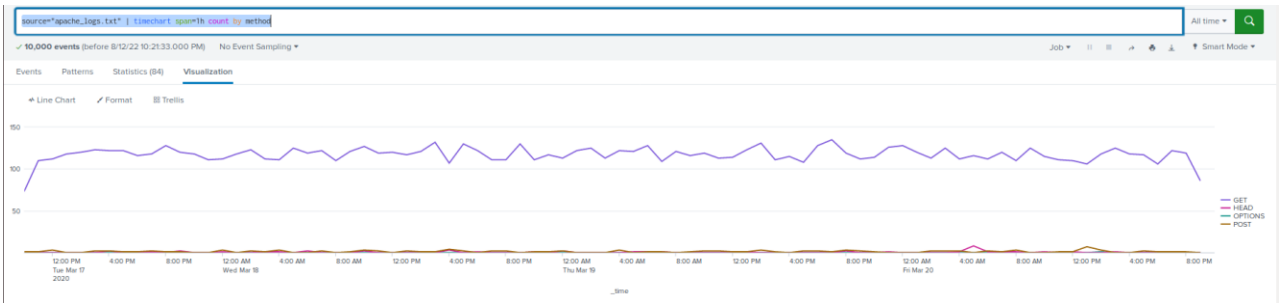
Visualizations and dashboards: Design the following visualizations, and add them to a dashboard called "Apache Web Server Monitoring" (be creative with your visualizations, and

make sure to grab screenshots of each):

1. A line chart that displays the different HTTP "methods" field values over time.

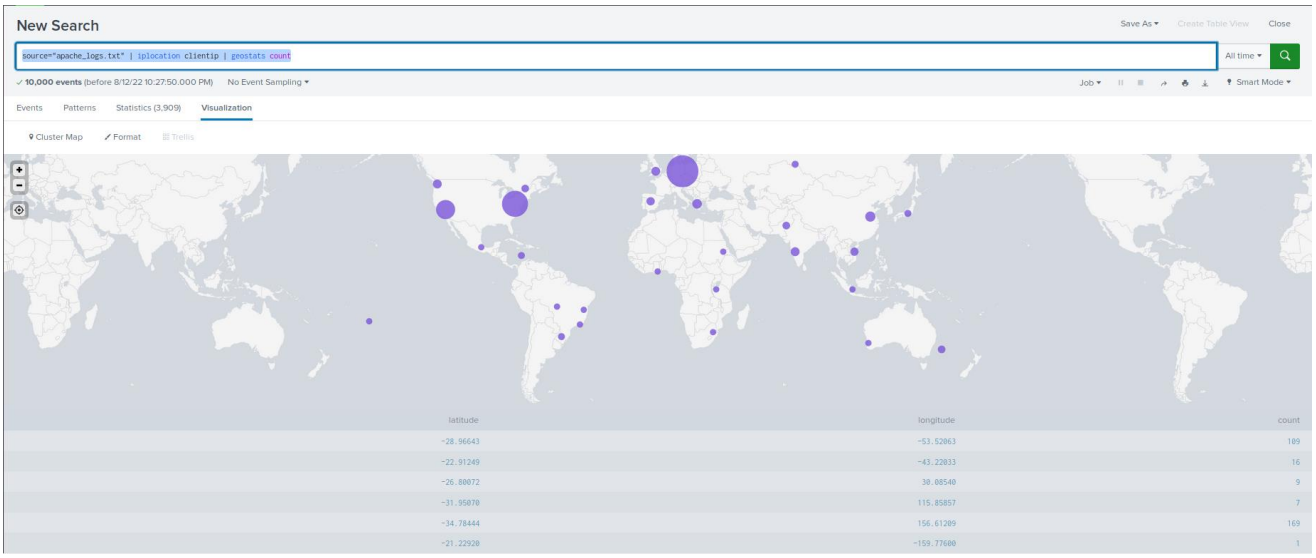
   Hint: Add the following after your search: timechart span=1h count by method.

   ```
   source="apache_logs.txt" | timechart span=1h count by method
   ```



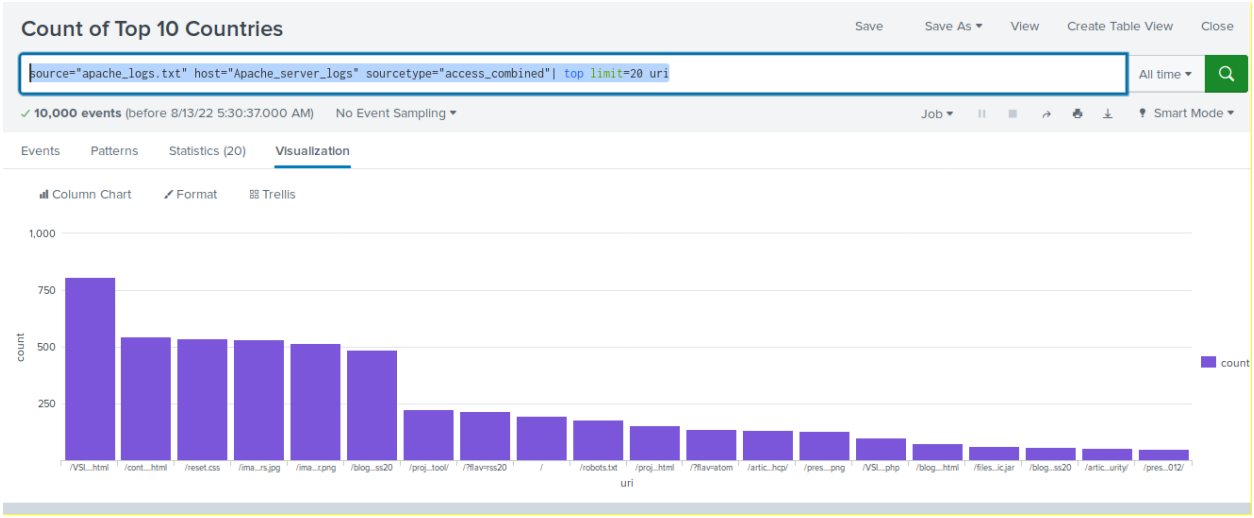
2. A geographical map showing the location based on the "clientip" field.

   ```
   source="apache_logs.txt" | iplocation clientip | geostats count
   ```



2. Any visualization of your choice that displays the number of different URIs.

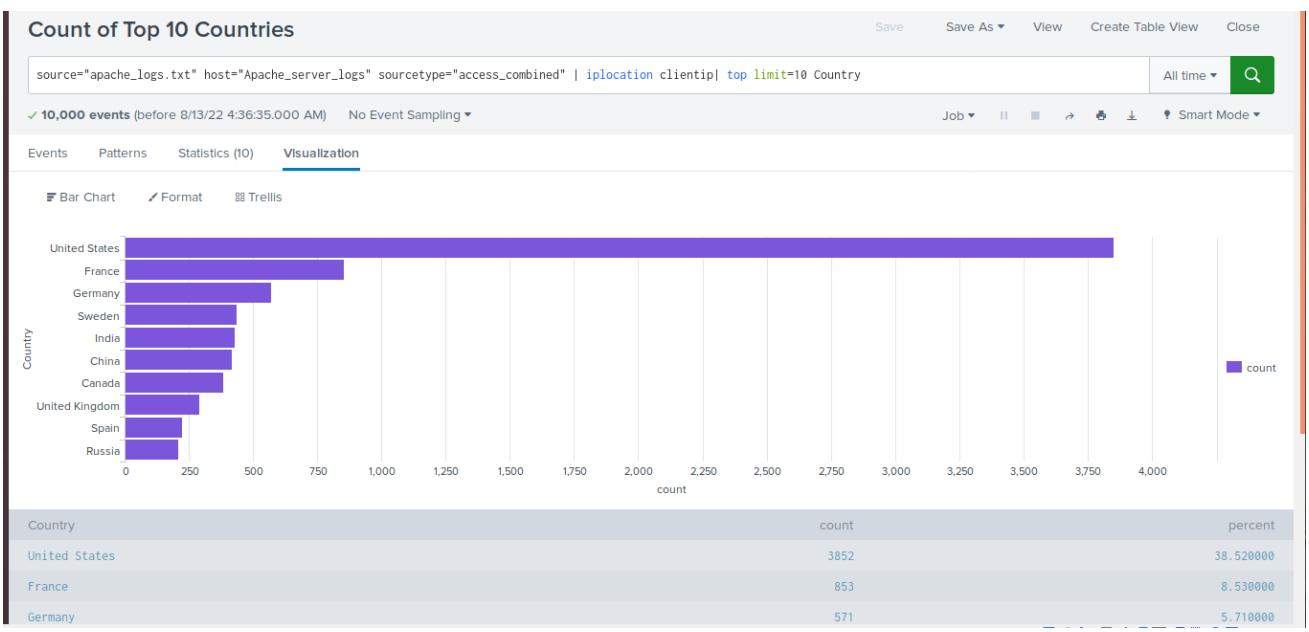
   ```
   source="apache_logs.txt" | top limit=20 uri
   ```



Hint: You can add brand-new custom visualizations by accessing this page inside your VM: [Additional Viz](#).

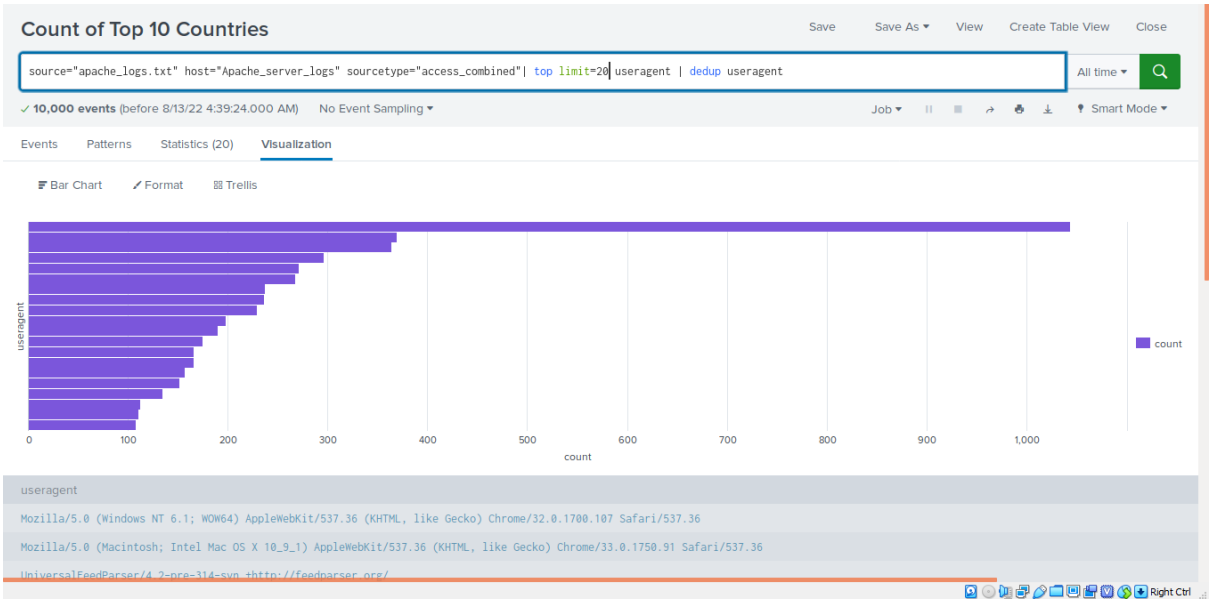
3. Any visualization of your choice that displays the count of the top 10 countries that appear in the log.

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



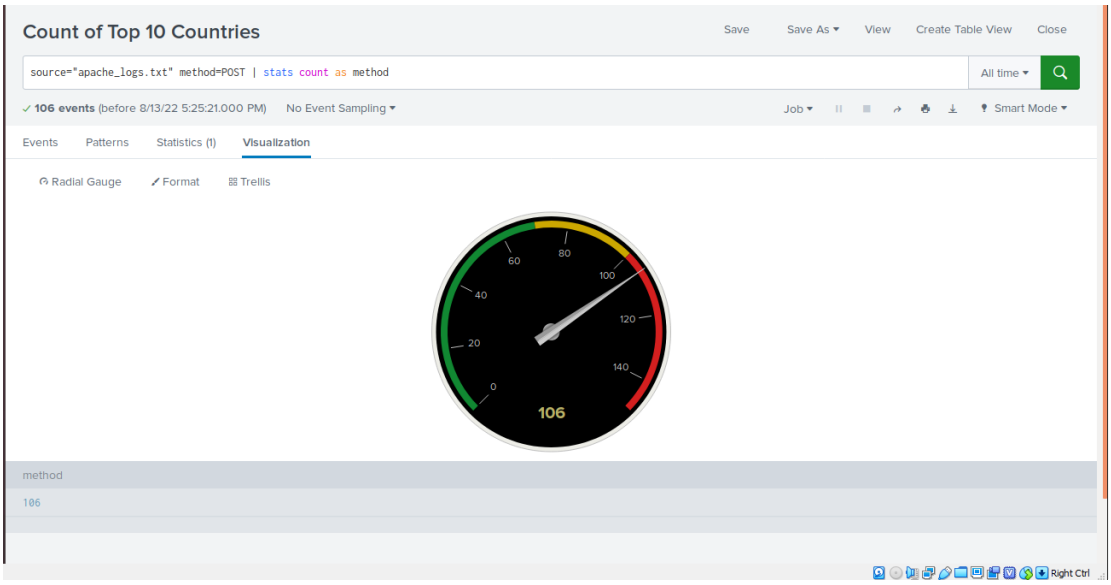
4. Any visualization that illustrates the count of different user agents.

```
source="apache_logs.txt" | top limit=20 useragent | dedup useragent
```



5. A single-value visualization of your choice that analyzes any single data point: e.g., radial gauge, marker gauge, or a custom visualization from http://localhost:8000/en-US/manager/search/appsremote?content=visualizations&type=app).

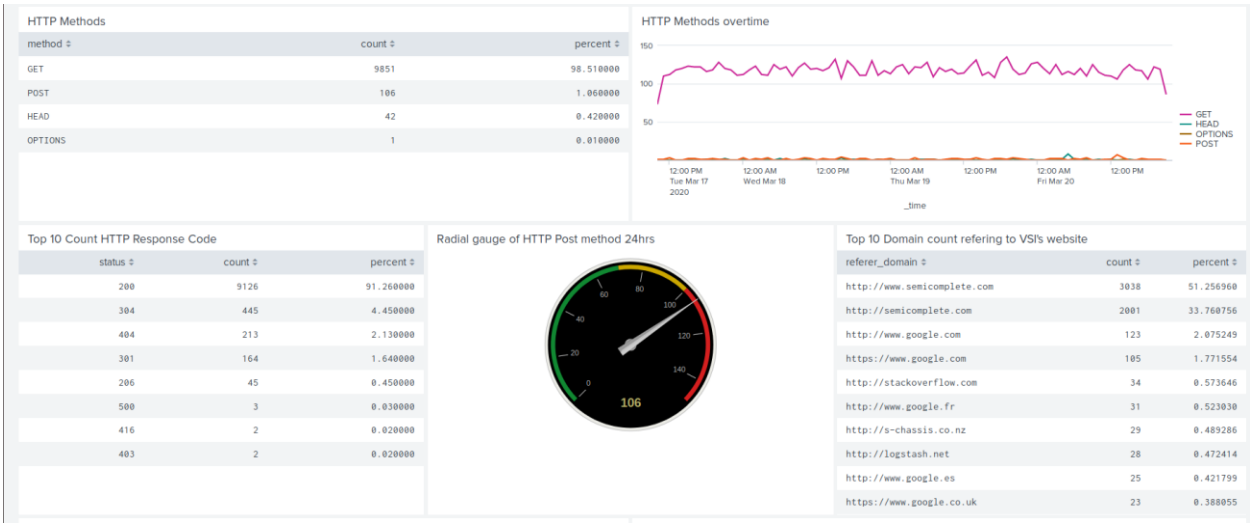
```
source="apache_logs.txt" method=POST | stats count as method
```



On your dashboard, add the ability to change the time range for all visualizations.

Be sure to title all of your panels appropriately.

Organize the panels on your dashboard as you see fit.



HTTP Methods

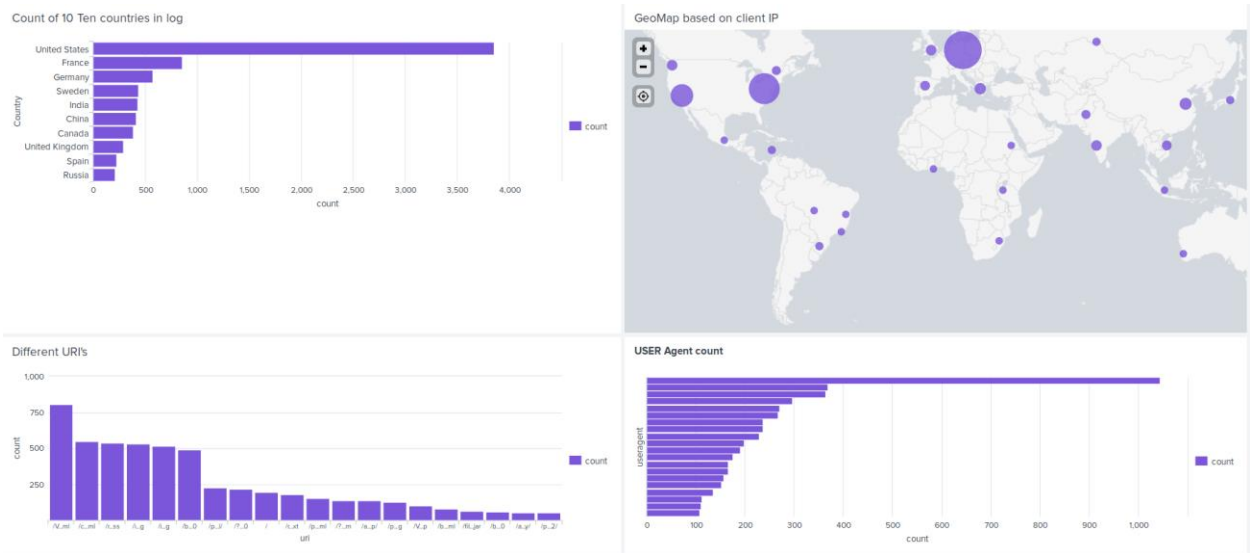
method	count	percent
GET	9851	98.510000
POST	106	1.060000
HEAD	42	0.420000
OPTIONS	1	0.010000

Top 10 Count HTTP Response Code

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

Top 10 Domain count refering to VSI's website

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



Part 5: Install an Add-On Splunk Application for Additional Monitoring

In this part, your team will choose a Splunk add-on app to provide additional monitoring for VSI's systems. To do so, complete the following steps:

1. First, select any **ONE** of the Splunk add-on apps from https://splunkbase.splunk.com/ to provide additional security monitoring for VSI.

- You can choose any app from Splunkbase as long as you are able to meet the following requirements:
    - You must be able to install and use the add-on app.
    - You must be able to describe a scenario that illustrates how the app's features will protect VSI.
- Use the following guide to install your add-on app: Choosing your own add-on app from Splunkbase.

2. You are also welcome to choose one of these Splunk add-on apps with a pre-defined scenario:

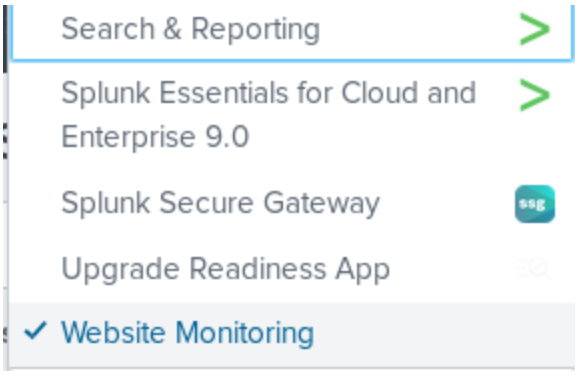
- **Website Monitoring**: App details here | **Install Instructions**: Website Monitoring App
- **Whois XML IP Geolocation API**: App details here | **Install Instructions**: Whois XML IP Geolocation API
- **Website Input**: App details here | **Install Instructions**: Website Input

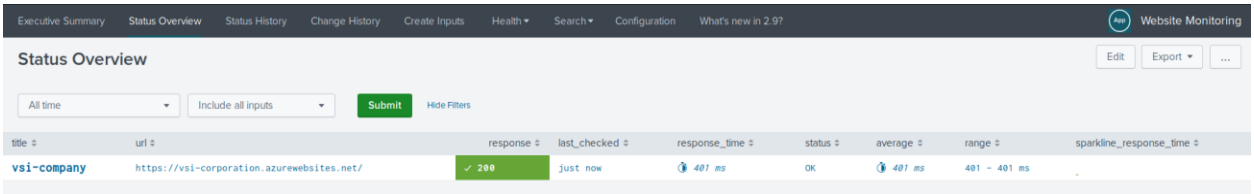
3. **Be sure to grab screenshots of your add-on app!**

Website Monitoring: App to monitor VSI's web app

Monitor websites to detect downtime and performance problems. This app uses a modular input that can be setup easily (in 5 minutes or less).

Scenario: JobeCorp, VSI's adversary, has been known to attack their competitors by launching DDOS attacks to take down their web applications. You will be using this web app to monitor if VSI's web application is up and functioning.





Day 2

Part 2: Analyze Windows Attack Logs

In this part, you will review the reports, alerts, and dashboards that you created in Day 1 and analyze the results. To do so, complete the following steps:

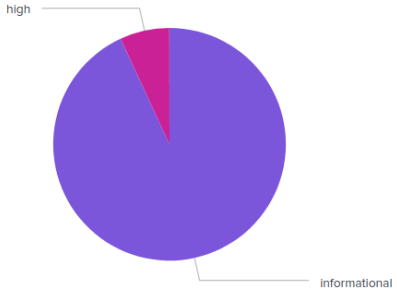
Report Analysis for Severity

Review the updated results, and answer the following question in the [Project 3 Review Questions]() document:

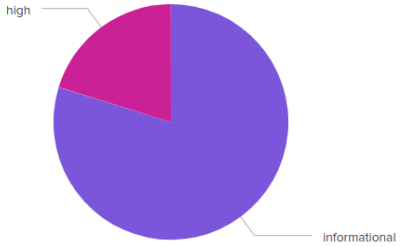
Did you detect any suspicious changes in severity?

- High severity jumped from 329 to 1111. 6.9% to 20.2%

Pie Chart Format Trellis



severity	count	percent
informational	4435	93.094039
high	329	6.905961



severity	count	percent
informational	4383	79.777940
high	1111	20.222060

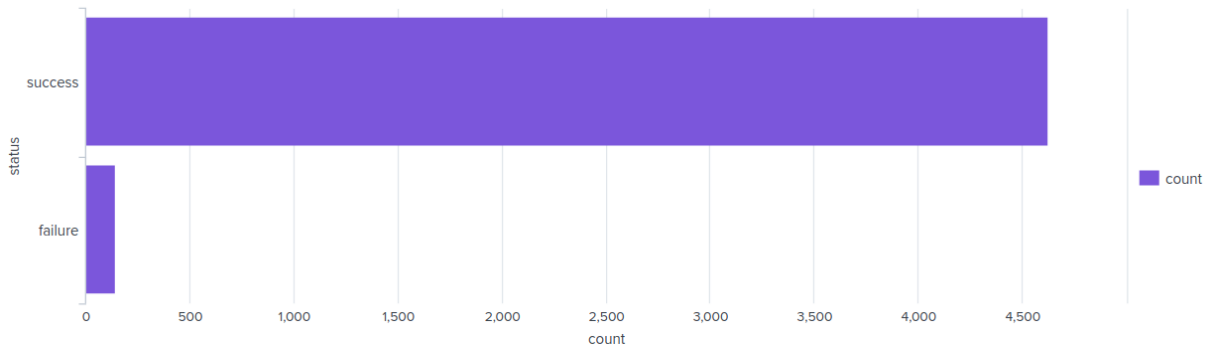
Note: You will use this same document for the remaining review questions.

Report Analysis for Failed Activities

Review the updated results, and answer the following question in the review document:

Did you detect any suspicious changes in failed activities?

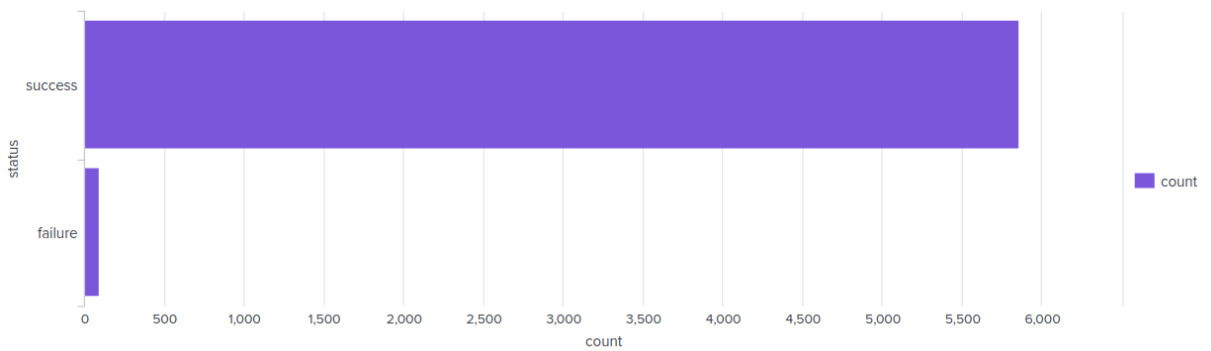
- Login failure decreased from 142 to 93.



status	count	percent
success	4622	97.019312
failure	142	2.980688

Events Patterns Statistics (2) Visualization

Bar Chart Format Trellis



status	count	percent
success	5856	98.436712
failure	93	1.563288

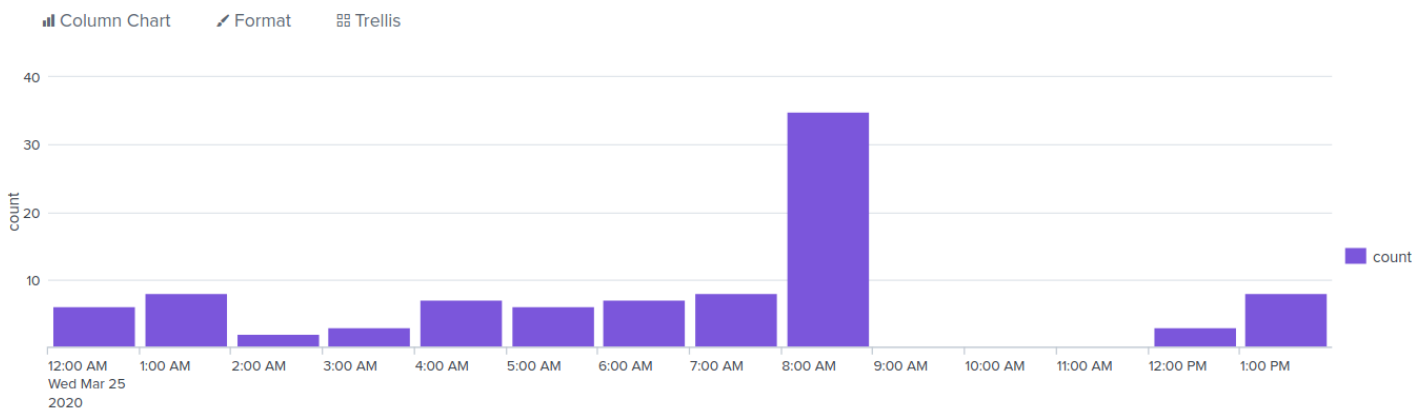
Show Applications

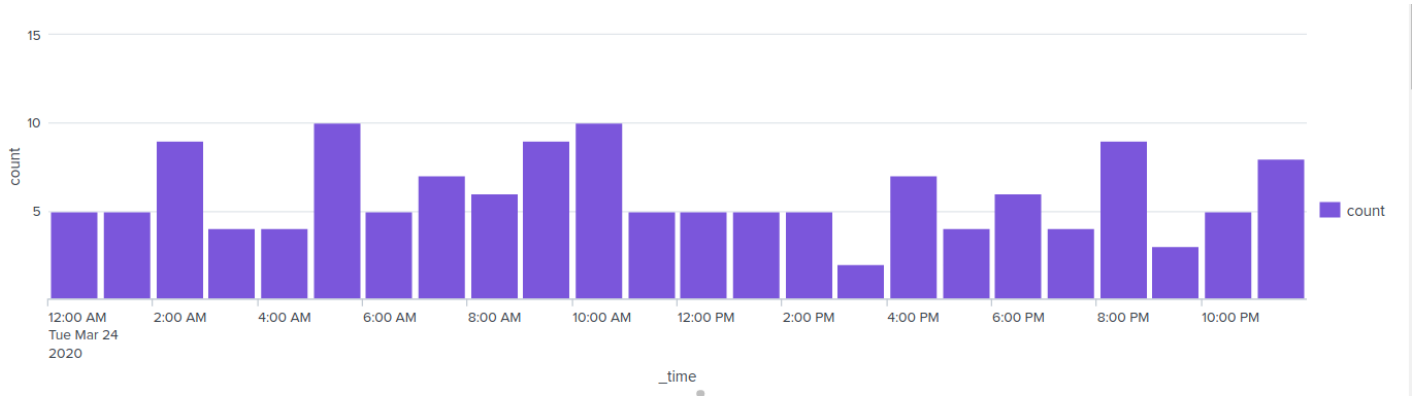
Alert Analysis for Failed Windows Activity

Review the updated results, and answer the following questions in the review document (*note that your alerts will not trigger; this is a theoretical exercise*):

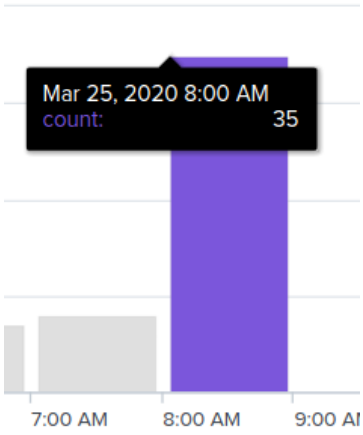
- Did you detect a suspicious volume of failed activity?

  Failure spiked during 8AM-9AM





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



- When did it occur?

  8AM

- Would your alert be triggered for this activity?

  Yes

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

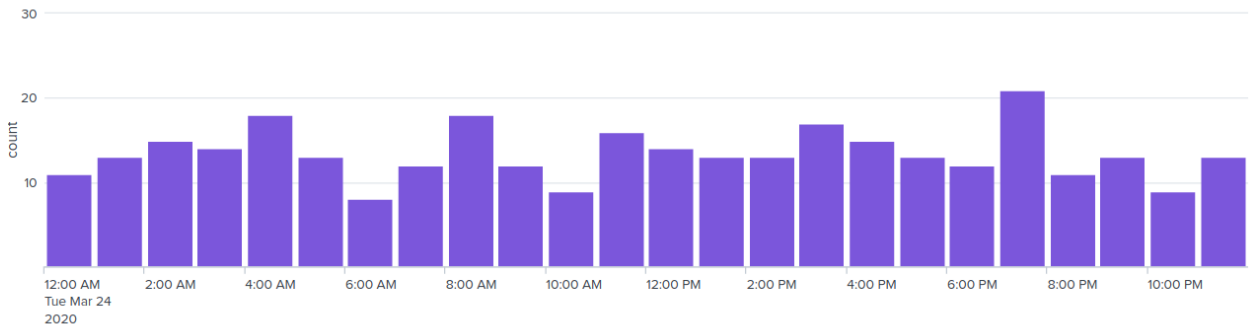
  No

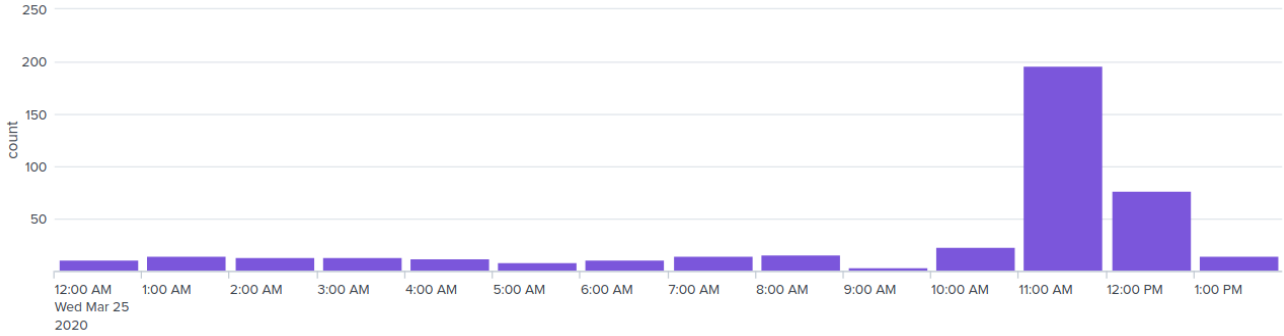
Alert Analysis for Successful Logins

Review the updated results, and answer the following questions in the review document:

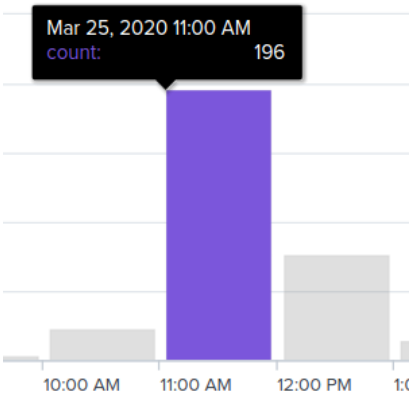
- Did you detect a suspicious volume of successful logins?

  Successful logins spiked during 11AM - 12PM



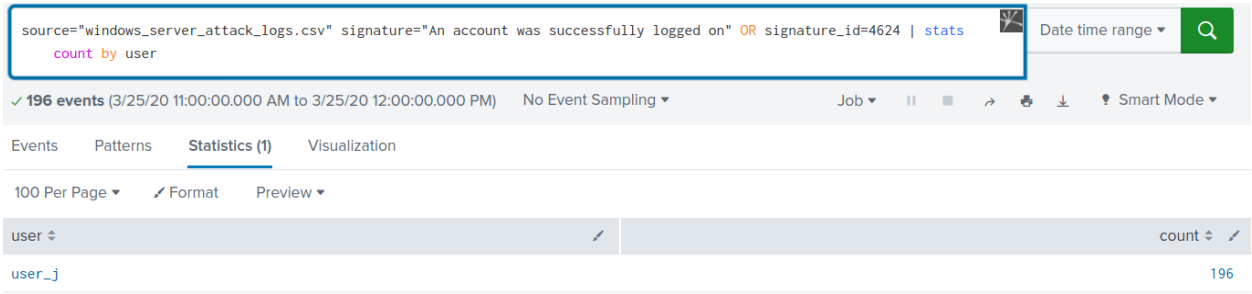


- If so, what was the count of events in the hour(s) it occurred?



- Who is the primary user logging in?

  User j



- When did it occur?

  11AM

- Would your alert be triggered for this activity?

  Yes

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

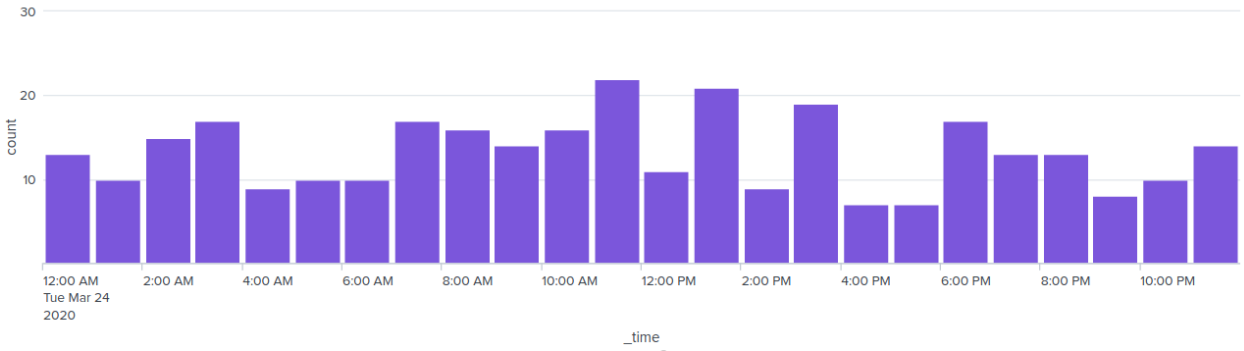
  No

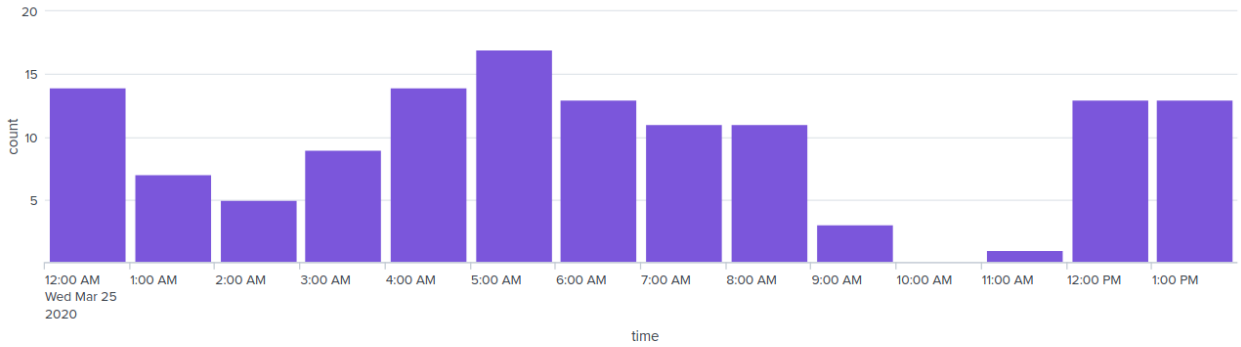
Alert Analysis for Deleted Accounts

Review the updated results, and answer the following question in the review document:

- Did you detect a suspicious volume of deleted accounts?

  Not really??





Dashboard Setup

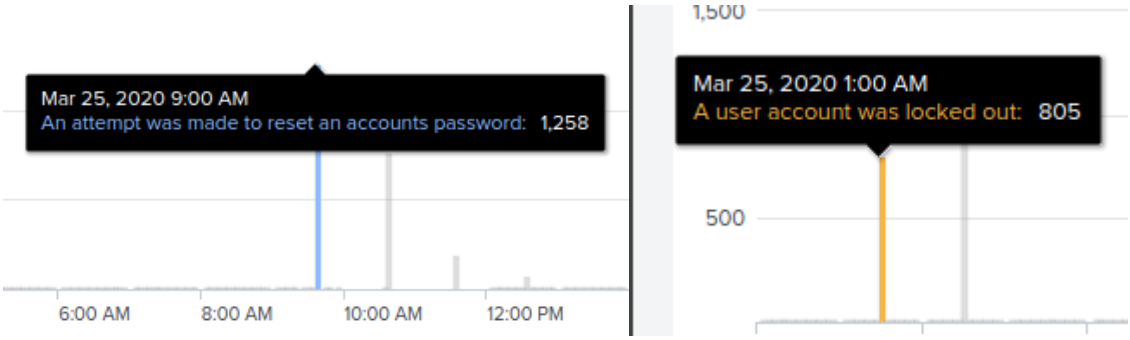
1. Access the Windows Web Server Monitoring dashboard.
    - Select "Edit."
2. For each panel that you created, access the panel and complete the following steps:
    - Select "Edit Search."
    - Change the source from windows_server_logs.csv to source="windows_server_attack_logs.csv".
    - Select "Apply."
    - Save the dashboard.
    - Change the time on the whole dashboard to "All Time."

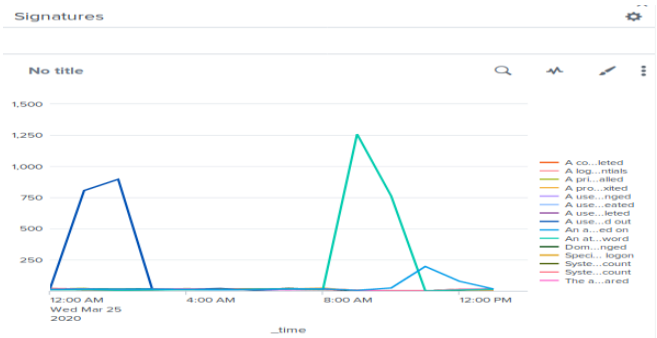
Dashboard Analysis for Time Chart of Signatures

Analyze your new dashboard results, and answer the following questions in the review document:

- Does anything stand out as suspicious?

  High account locked out during 1-2AM. High attempts to reset password at 9 AM. High amount of successful logons at 11am.





- What signatures stand out?

  An attempt was made to reset an accounts password

  User accounts being locked out

  An account being successfully logged on

- What time did each signature's suspicious activity begin and stop?

  9AM - 10AM: account password reset

  12 am - 3am: for lock out

  11am -1pm: successful logons

- What is the peak count of the different signatures?
  1258 for password reset.

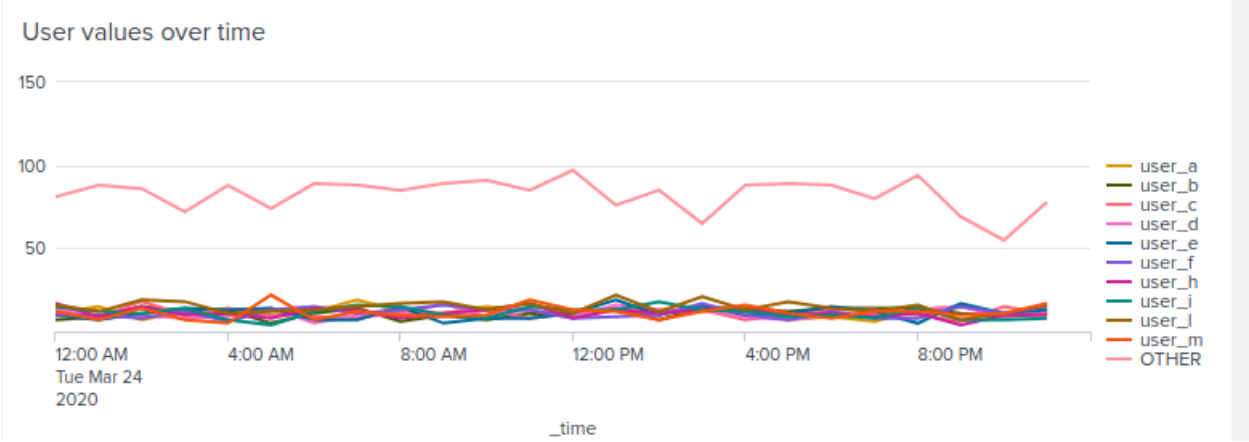
  805 for lock out.

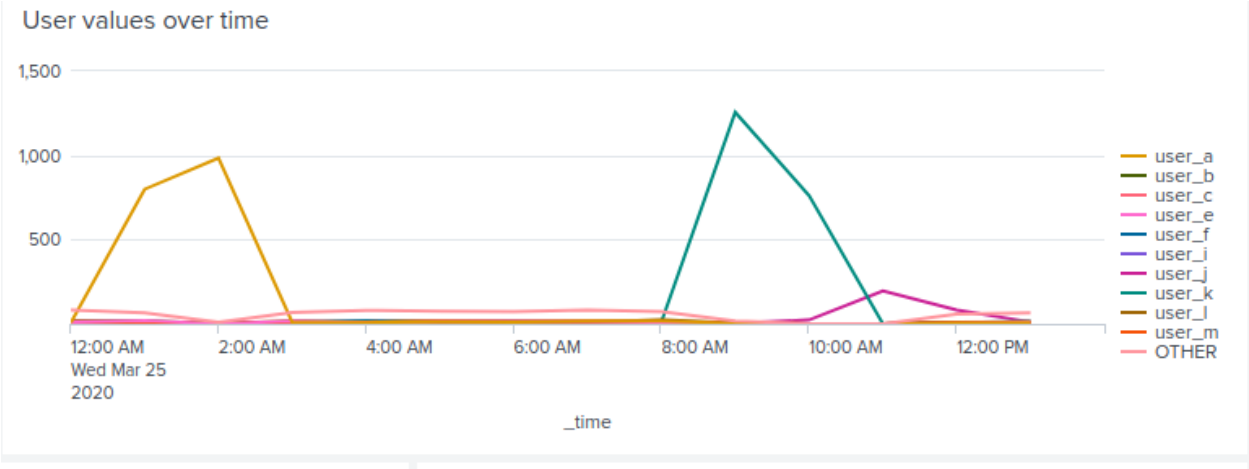
  196 for logons

Dashboard Analysis for Users

Analyze your new dashboard results, and answer the following questions in the review document:

- Does anything stand out as suspicious?





- Which users stand out?
  User a, User k, User j

- What time did each user's suspicious activity begin and stop?
  User a: 12AM to 3AM

  User k: 8AM to 11AM

  User j: 11am to 1pm

- What is the peak count of the different users?

  User a:984

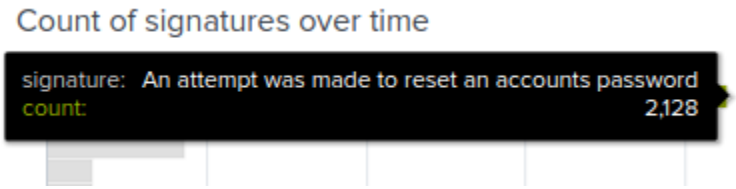
  User k:1256

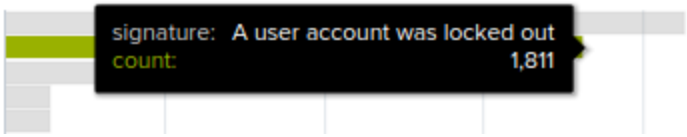
  User j: 196

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

Analyze your new dashboard results, and answer the following questions in the review document:

- Does anything stand out as suspicious?
  Large number of attempts for password reset and lockout.



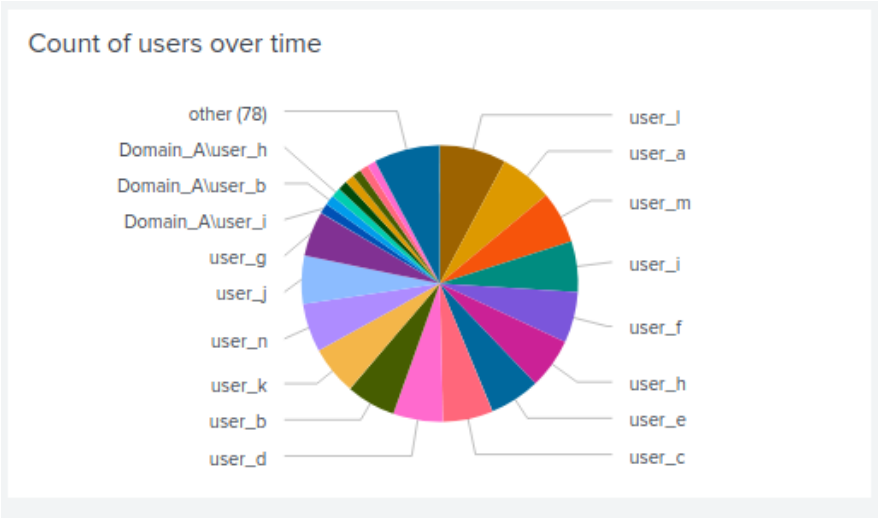


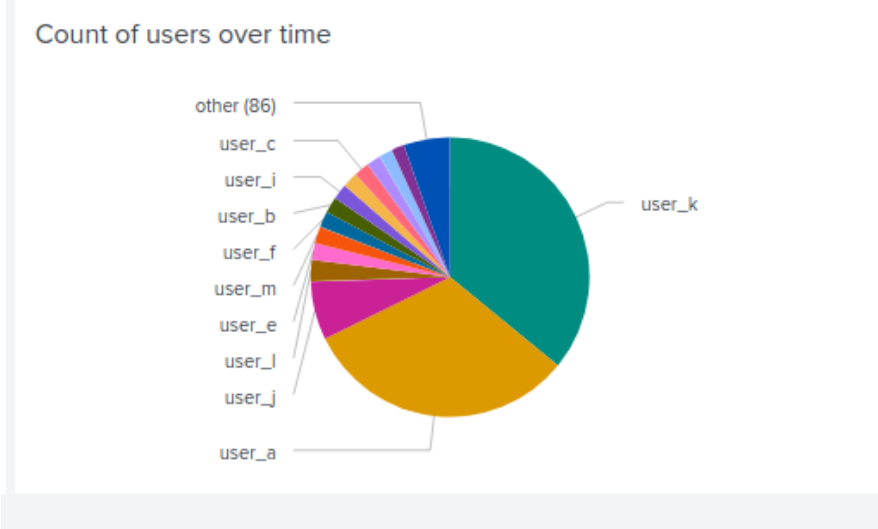
- Do the results match your findings from the time chart for signatures?
  Yes

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

Analyze your new dashboard results, and answer the following questions in the review document:

- Does anything stand out as suspicious?





Yes. User_a, user_k, and user_j

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

Yes

Dashboard Analysis for Users with Statistical Charts

Analyze your new dashboard results, and answer the following question in the review document:

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

  Advantages -

  Able to sort results to highest vs lowest count

  Easy to read when there are few results

  Great for looking at total counts, percentage, etc.

  Disadvantages -

  Other panels are clearer when there is unusual activity with large amount of results

  If looking for activities on a span of time, it is difficult to read the results for any unusual activity

Part 3: Load Apache Attack Logs

apache_attack_logs.txt

Part 4: Analyze Apache Attack Logs

In this part, you will review the reports, alerts, and dashboards that you created on Day 1 and analyze the results. To do so, complete the following steps:

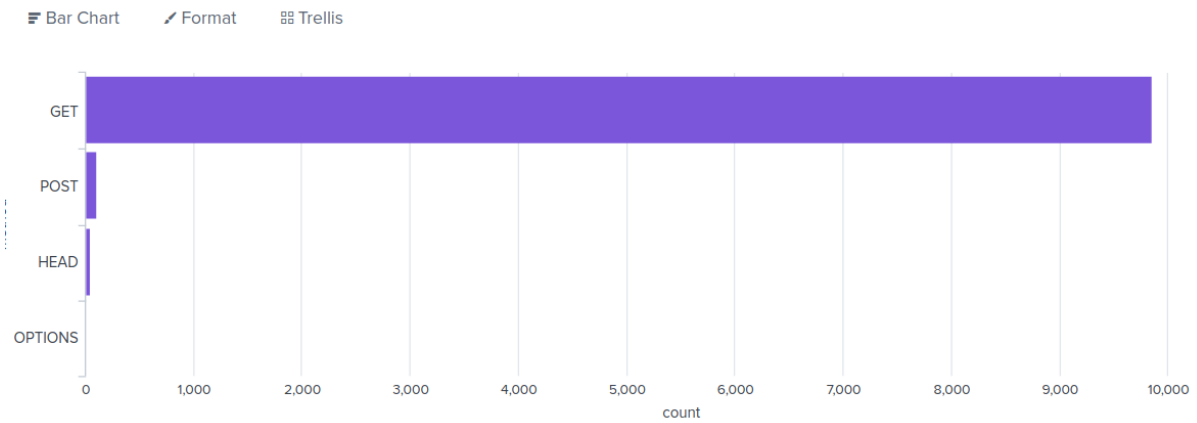
Report Analysis for Methods

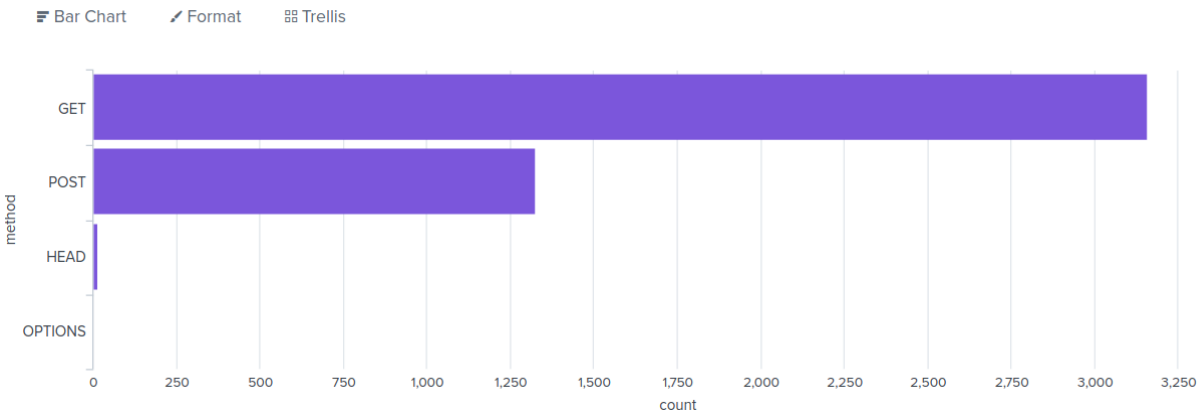
Review the updated results, and answer the following questions in the review document:

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

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

  Post request increased from 106 to 1324





- What is that method used for?
  POST - used at the client side to send data to a server

Report Analysis for Referrer Domains

Review the updated results, and answer the following question in the review document:

- Did you detect any suspicious changes in referrer domains?

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

  No suspicious changes, but less activity in the referrer domain in the attacks logs.

apache_logs.txt

50 Per Page ▾ Format Preview ▾

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_logs.txt

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

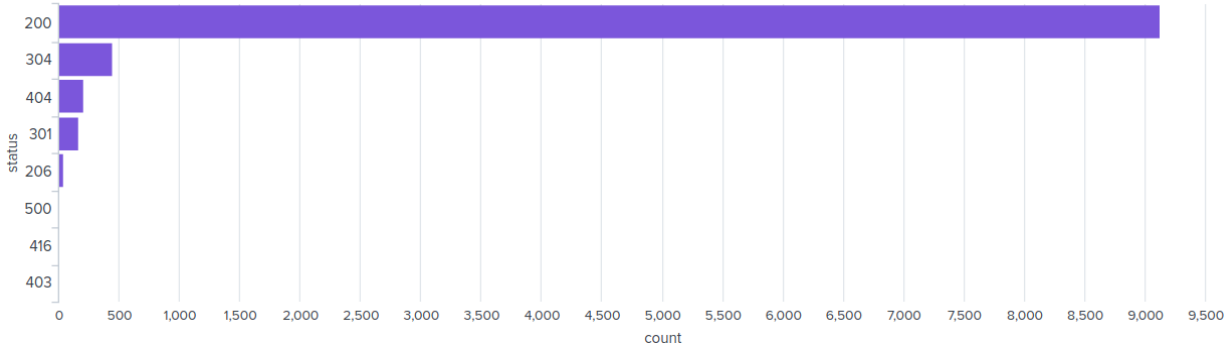
Report Analysis for HTTP Response Codes

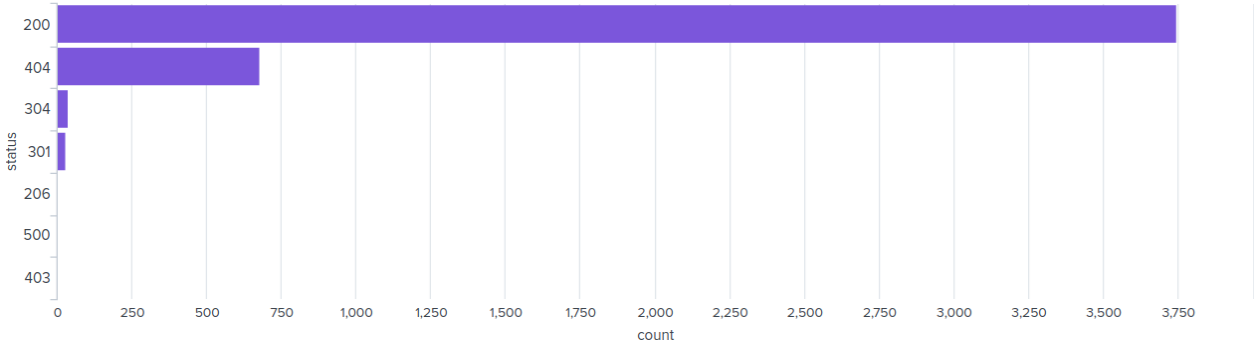
Review the updated results and answer the following question in the review document:

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

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

  Increase in 404 responses, and decrease in the 200 responses





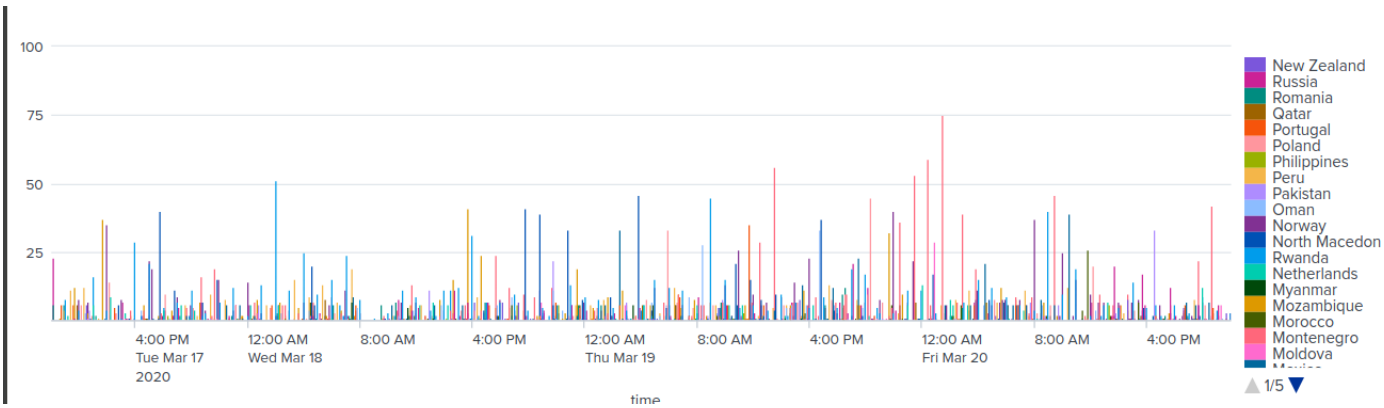
Alert Analysis for International Activity

Review the updated results, and answer the following questions in the review document:

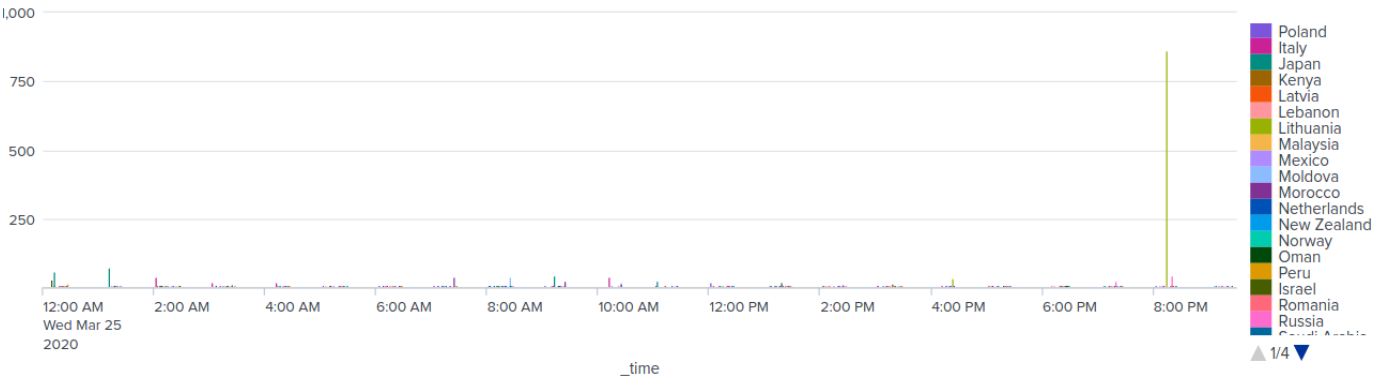
```
source="apache_attack_logs.txt" | iplocation clientip| timechart count
by Country span=1h limit=100 | fields - "United States"
```

- Did you detect a suspicious volume of international activity?

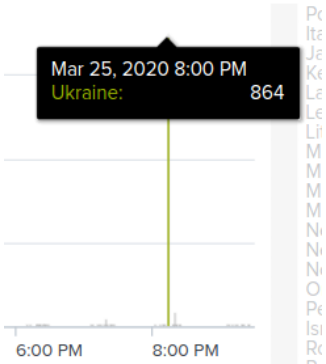
  Event from Ukraine spiked since 8PM



Column Chart Format Trellis



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



- Would your alert be triggered for this activity?

  Yes

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

  Yes, there may have been an overload of alerts, we would change it to 45.

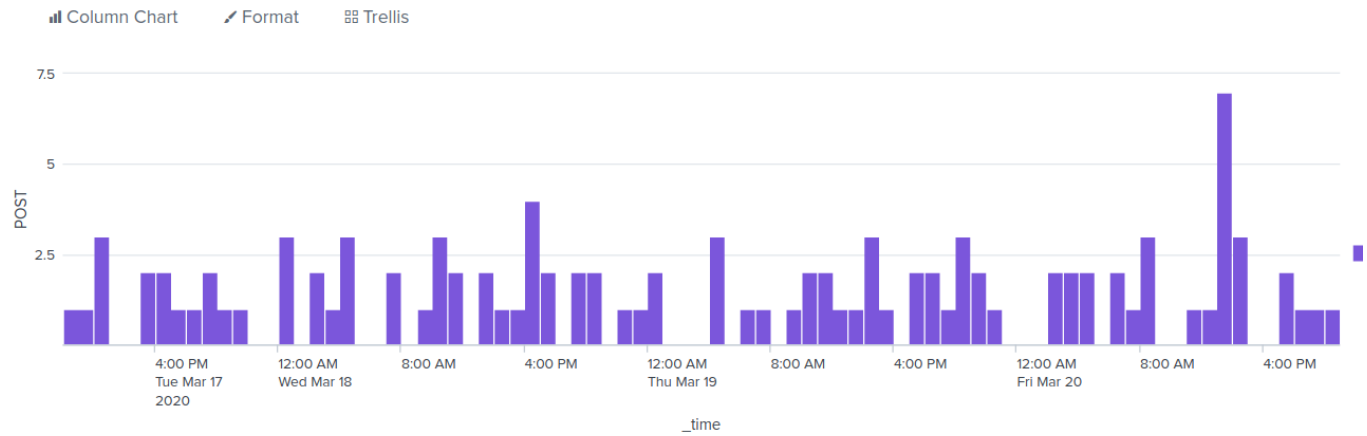
Alert Analysis for HTTP POST Activity

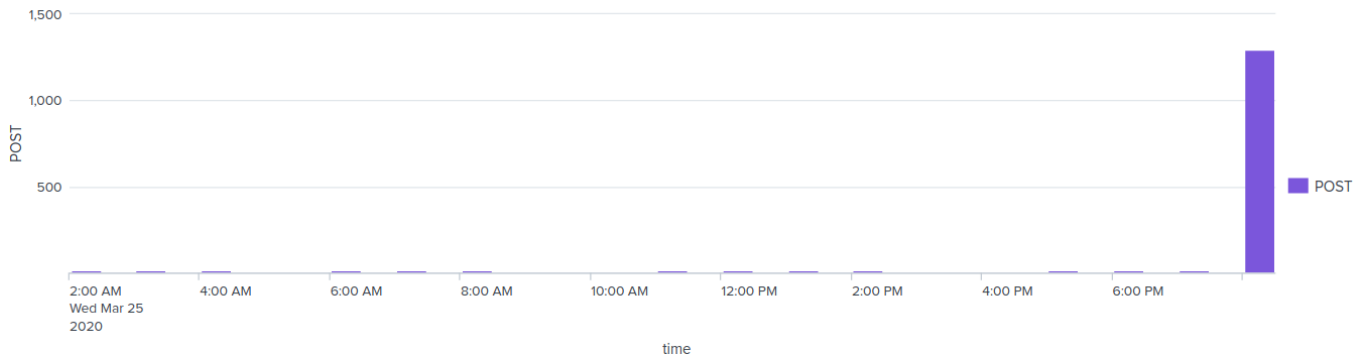
Review the updated results, and answer the following questions in the review document:

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

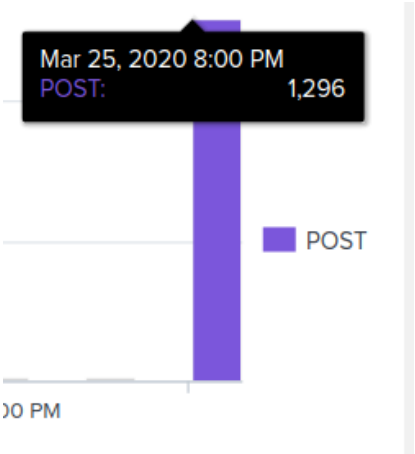
  ```
  source="apache_attack_logs.txt" method=POST | timechart count by method span=1h limit=10
  ```

  High Post request during 8PM





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



- When did it occur?

  8PM

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

  No

Dashboard Setup

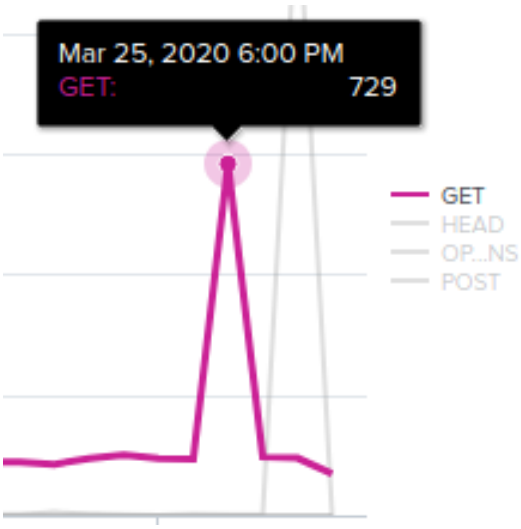
1. Access the Apache Web Server Monitoring dashboard.
2. Select "Edit."
3. For each panel that you created, access the panel and complete the following steps:
   - Select "Edit Search."
   - Change the source from source=apache_logs.txt to source="apache_attack_logs.txt.
   - Select "Apply."
4. Save the whole dashboard.
5. Change the time on the whole dashboard to "All Time."

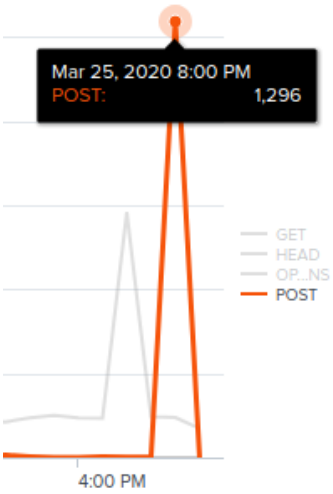
Dashboard Analysis for Time Chart of HTTP Methods

Analyze your new dashboard results, and answer the following questions in the review document:

- Does anything stand out as suspicious?

  1258 GET requests at 8PM (Mar 25)





- Which method seems to be used in the attack?

  GET and POST

- At what times did the attack start and stop?

  GET: 6PM - 7PM

  POST: 8PM - 9PM

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

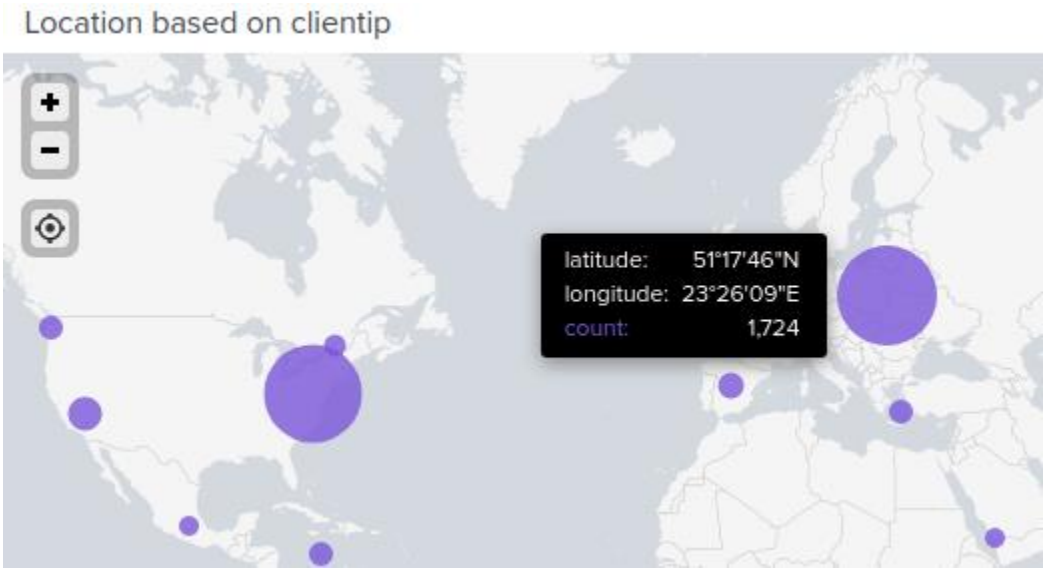
  GET: 729

  POST 1296

Dashboard Analysis for Cluster Map

Analyze your new cluster map results, and answer the following questions in the review document:

- Does anything stand out as suspicious?



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

  Ukraine

- What is the count of that city?

  877

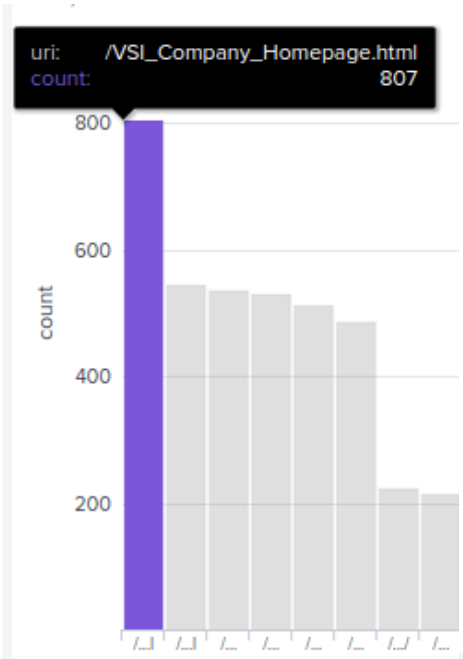
Dashboard Analysis for URI Data

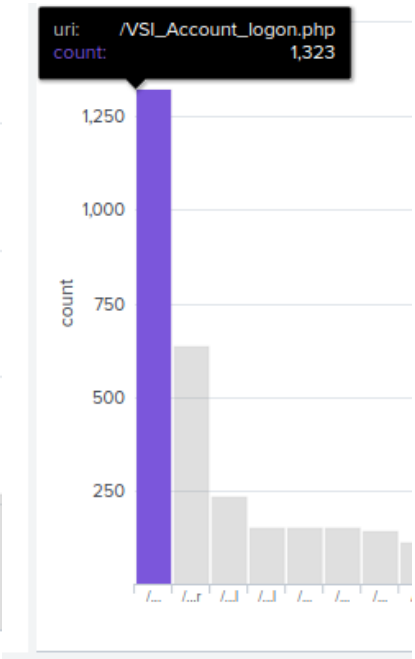
Analyze your dashboard panel of the URI data, and answer the following questions in the review document:

- Does anything stand out as suspicious?

  Normal: homepage.html

  During the attack, visit to VSI_Account_logon.php spiked





- What URI is hit the most?

  /VSI_Account_logon.php

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

  Brute Forcing credentials

Part 5: Create Project Presentations

In this part, you will begin to create a presentation to showcase the work you completed during your project.

Use the following framework to design your team's presentation: Project 3 Presentation Framework.

1. First, make a copy of this presentation.
2. Complete all of the required items in square brackets.
    - Use your review guide to assist you.
3. Feel free to be creative in your project presentations.
    - Add any additional slides that you would like.
    - Add any additional visualizations, images, videos, etc. that you would like.
4. Feel free to split up the work on this presentation, but remember that every student must submit their own complete presentation (even if it is a copy of your other team members').

Link to group slides: Project 3 Presentation Template