## **Activity File: Part 1 - Master of the SOC**

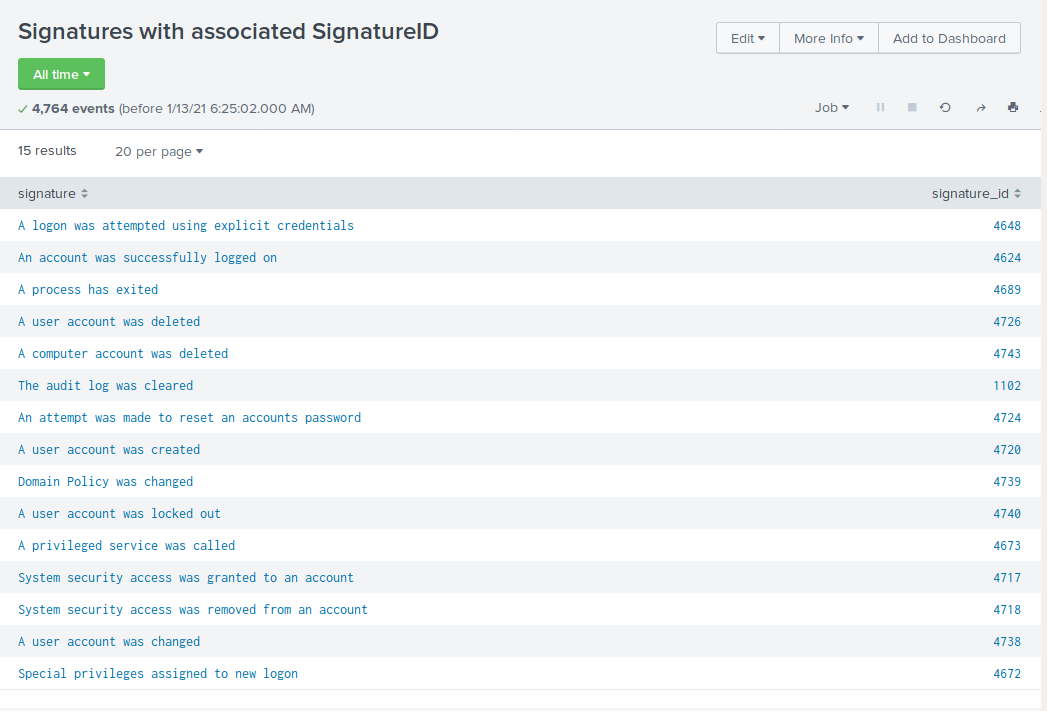
* Each group is playing the role of an SOC analyst at a small company called Virtual Space Industries (VSI), which designs virtual reality programs for businesses.
* VSI has heard rumors that a competitor, JobeCorp, may be launching cyberattacks to disrupt VSI's business.
* As SOC analysts, you are tasked with using Splunk to monitor against potential attacks on your systems and applications.
* Your Networking team has provided you with past logs to help you develop baselines and create reports, alerts, and dashboards.

You've been provided the following logs:

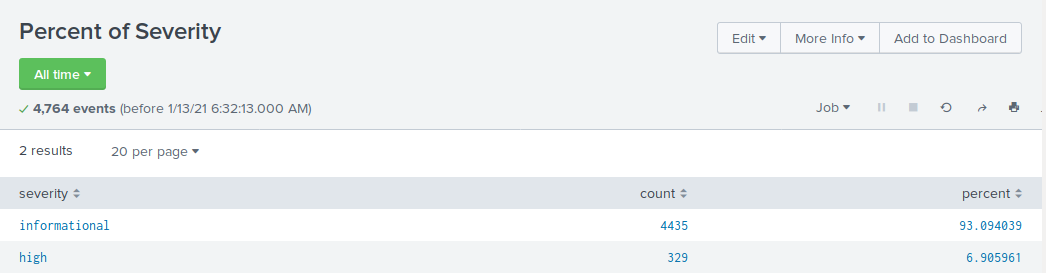
* **Windows Server Logs**  
  + This server contains intellectual property of VSI's next-generation virtual reality programs.
* **Apache Server Logs**  
  + This server is used for VSI's main public-facing website vsi-company.com.

### **Windows Server Logs Instructions and Deliverables**

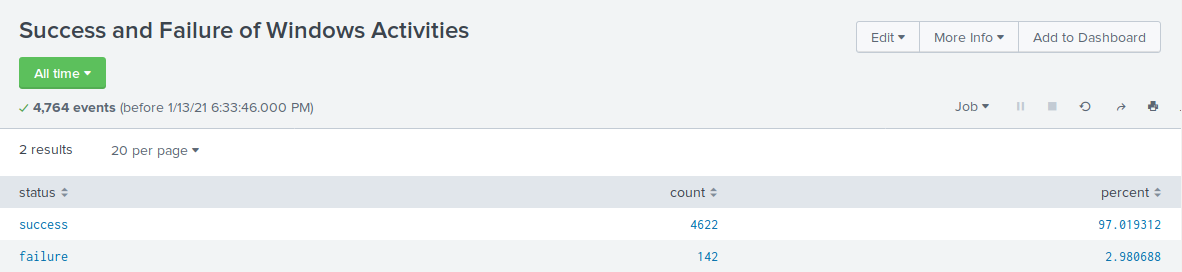
1. Load the logs into your Splunk environment.  
   * Select all default options provided.
   * **Important:** For the time range, select **All Time**.
2. Analyze the logs and the available fields.
3. Design the following deliverables to protect VSI from potential attacks by JobeCorp.  
   * **Reports**: Design the following reports to assist VSI with quickly identifying specific information.  
     1. A report with a table of signatures and associated SignatureID.  
        + This will allow VSI to easily view reports that show the ID number with a specific signature of the Windows activity.  
            
           **Hint:** Research how to remove the duplicate values in your SPL search.



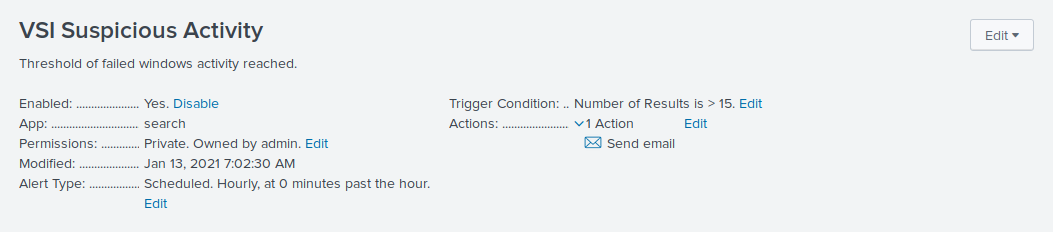
* + 1. A report that provides the count and percent of the severity.  
       - This will allow VSI to quickly know the severity levels of the Windows logs being viewed.



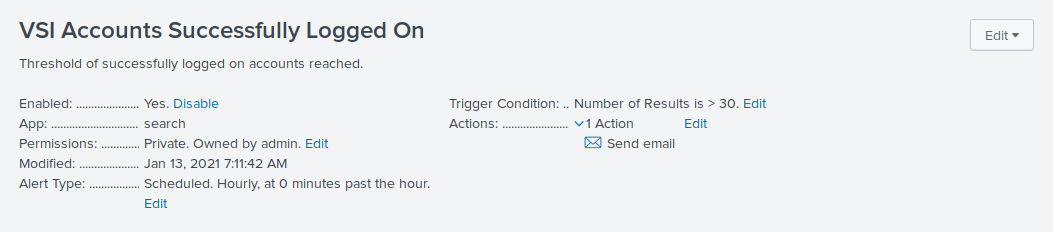
* + 1. A report that provides a comparison between the success and failure of Windows activities.  
       - This will show VSI if there is a suspicious level of failed activities on their server.  
           
          **Hint:** Check the status field for this information.



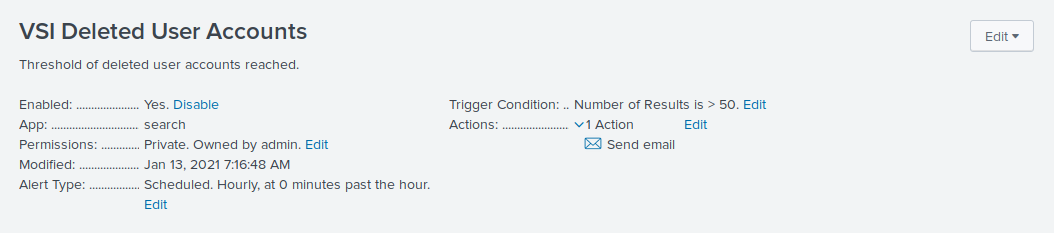
* + **Alerts**: Design the following alerts to notify VSI of suspicious activity:  
    1. Determine a baseline and threshold for hourly level of failed Windows activity.  
       - Create an alert to trigger when the threshold has been reached.
       - The alert should trigger an email to [SOC@VSI-company.com](mailto:SOC@VSI-company.com).
* Baseline for failed hourly attempts: 6.
* Threshold for failed hourly attempts: 15.



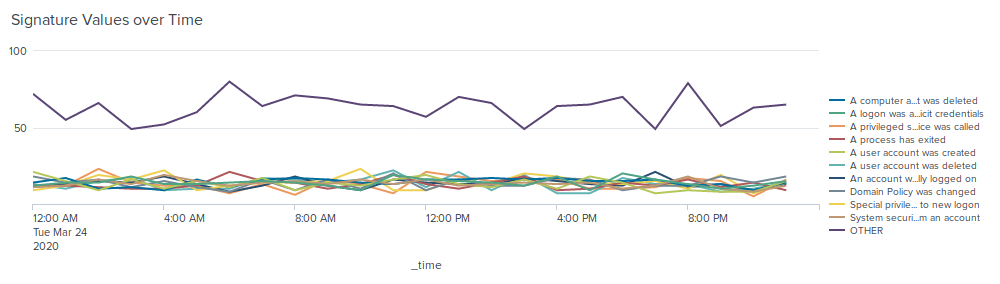
* + 1. Determine a baseline and threshold for hourly count of the signature: **an account was successfully logged on**.  
       - Create an alert to trigger when the threshold has been reached.
       - The alert should trigger an email to [SOC@VSI-company.com](mailto:SOC@VSI-company.com).
* Baseline for hourly success of logged on accounts: 12.
* Threshold for hourly success of logged on accounts: 30.



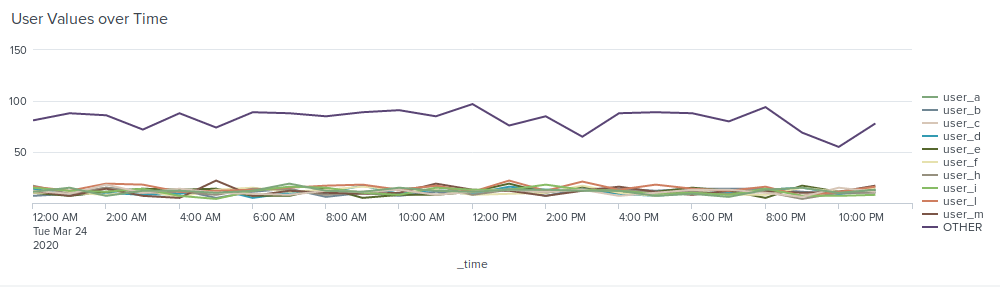
* + 1. Determine a baseline and threshold for hourly count of the signature: **a user account was deleted**.  
       - Design the alert based on the corresponding SignatureID, as the signature name sometimes changes when the Windows system updates.
       - Create an alert to trigger when the threshold has been reached.
       - The alert should trigger an email to [SOC@VSI-company.com](mailto:SOC@VSI-company.com).
* Baseline for hourly deleted user accounts: 13.
* Threshold for hourly deleted user accounts: 50.



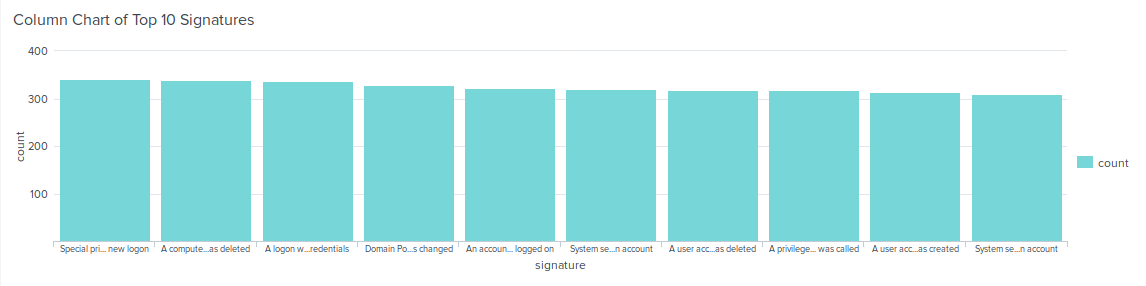
* + **Visualizations and Dashboards**: Design the following visualizations and add them to a dashboard called Windows Server Monitoring:  
    1. A line chart that displays the different signature field values over time.  
       - **Hint:** Add the following after your search: timechart span=1h count by signature.



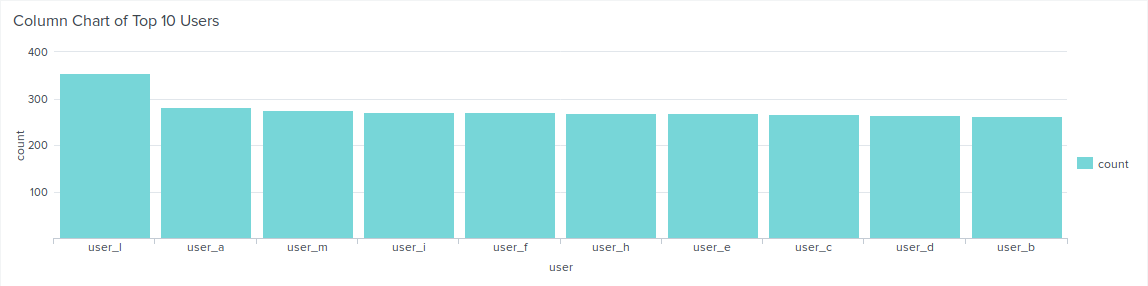
* + 1. A line chart that displays the different user field values over time.



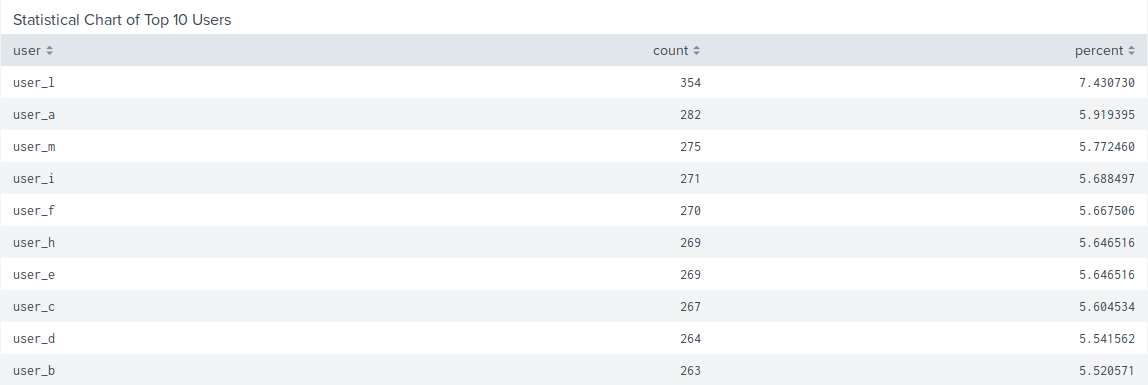
* + 1. A bar, column, or pie chart that illustrates the count of different signatures.



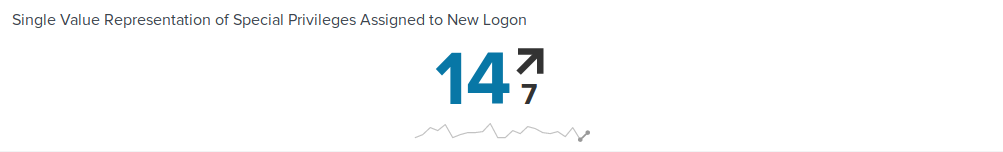
* + 1. A bar, column, or pie chart that illustrates the count of different users.



* + 1. A statistical chart that illustrates the count of different users.



* + 1. One single value visualization of your choice: radial gauge, marker gauge, etc.

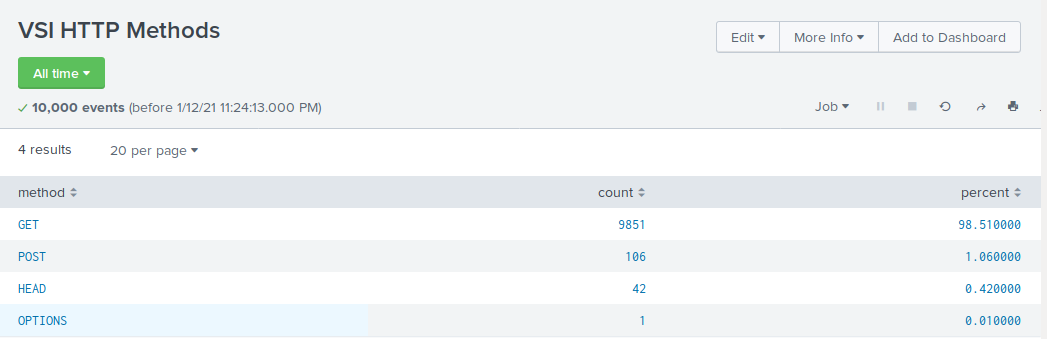


1. On your dashboard, add the ability to change the time range for all your visualizations.  
   * Be sure to title all your panels appropriately.
   * Align your dashboard panels as you see fit.

### 

### **Apache Web Server Instructions and Deliverables**

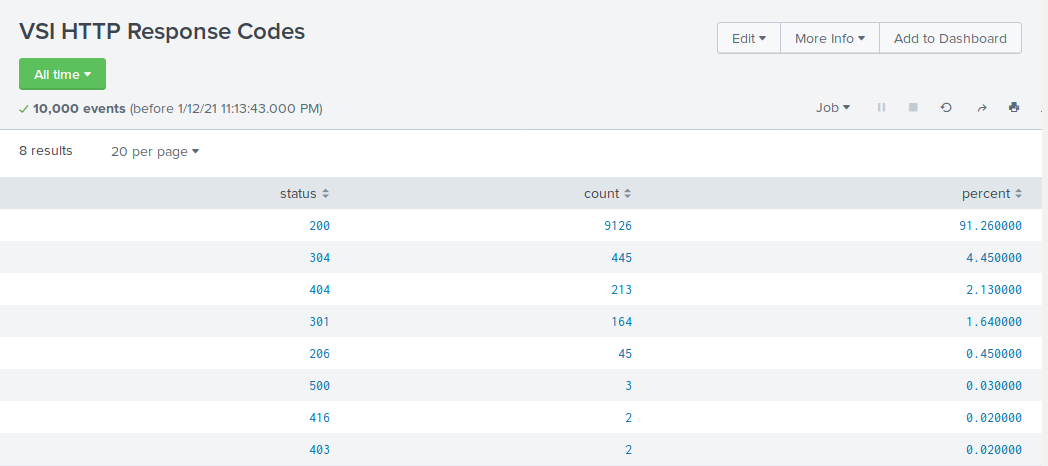
1. Load the logs into your Splunk environment.  
   * Select all default options provided.
   * **Important:** For the time range, select **All Time**.
2. Analyze the logs and the available fields.
3. Design the following deliverables to protect VSI from potential attacks by JobeCorp:  
   * **Reports**: Design the following reports to assist VSI with quickly identifying specific information:  
     1. A report that shows a table of the different HTTP methods (GET, POST, HEAD, etc).  
        + This will provide insight into the type of HTTP activity being requested against their web server.



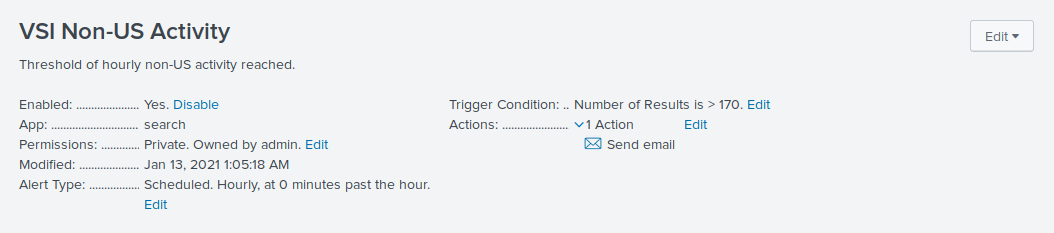
* + 1. A report that shows the top 10 domains that referred to VSI's website.  
       - This will assist VSI with identifying suspicious referrers.



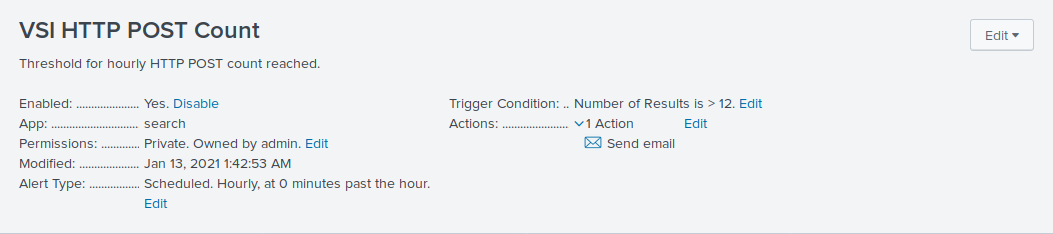
* + 1. A report that shows the count of the HTTP response codes.  
       - This will provide insight into any suspicious levels of HTTP responses.



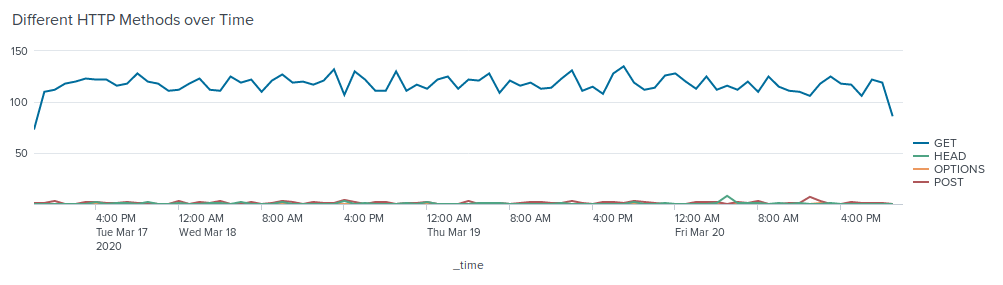
* + **Alerts**: Design the following alerts:  
    1. Determine a baseline and threshold for hourly activity from a country other than the United States.  
       - Create an alert to trigger when the threshold has been reached.
       - The alert should trigger an email to [SOC@VSI-company.com](mailto:SOC@VSI-company.com).
* Baseline for hourly activity is 80
* Threshold for hourly activity is 170



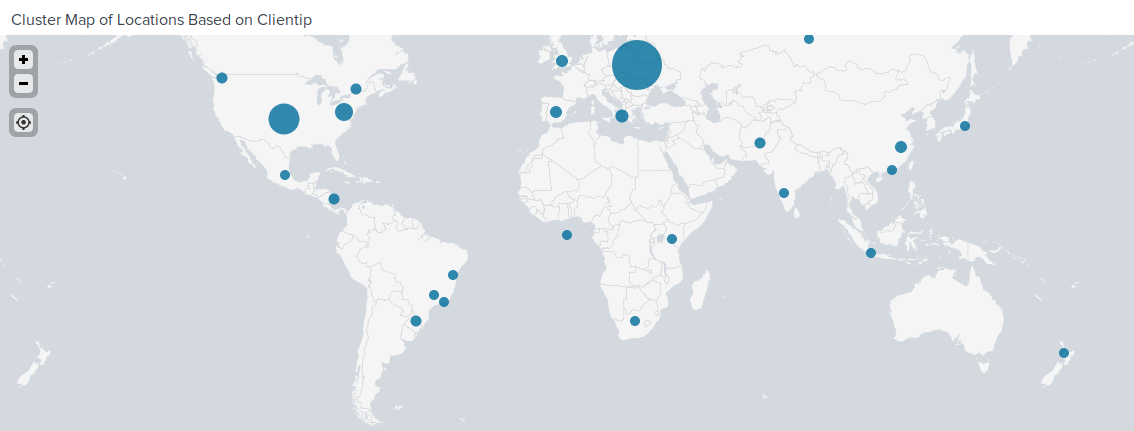
* + 1. Determine an appropriate baseline and threshold for hourly count of the HTTP POST method.  
       - Create an alert to trigger when the threshold has been reached.
       - The alert should trigger an email to [SOC@VSI-company.com](mailto:SOC@VSI-company.com).
* Baseline for hourly count of HTTP POST method is 2
* Threshold for hourly count of HTTP POST method is 12



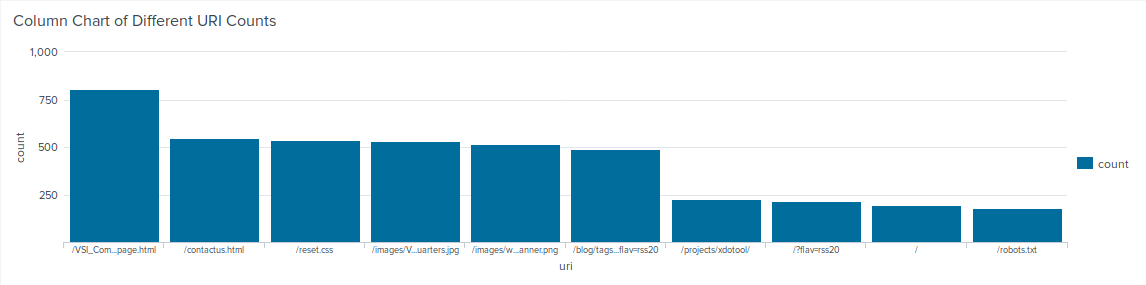
* + **Visualizations and Dashboards**: Design the following visualizations and add them to a dashboard called Apache WebServer Monitoring.  
    1. A line chart that displays the different HTTP methods field over time.  
       - **Hint:** Add the following after your search: timechart span=1h count by method.



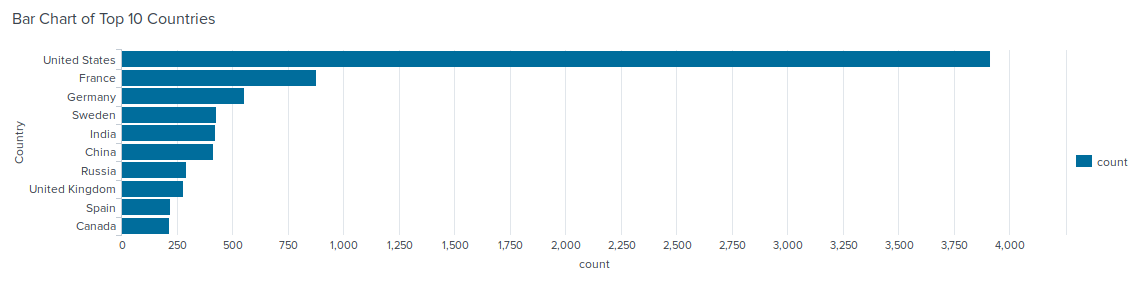
* + 1. A cluster map showing the locations based on the clientip field.



* + 1. A bar, column, or pie chart that displays the number of different URIs.



* + 1. A bar, column, or pie chart that displays the counts of the top 10 countries.



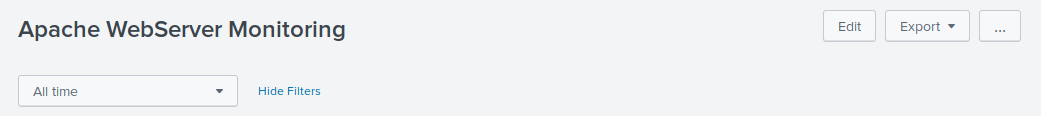
* + 1. A statistical chart that illustrates the count of different user agents.



* + 1. One single value visualization of your choice: radial gauge, marker gauge, etc.



1. On your dashboard, add the ability to change the time range for all your visualizations:  
   * Be sure to title all your panels appropriately.
   * Align your dashboard panels as you see fit.



## **Activity File: Part 2 - Defend Your SOC**

* VSI recently experienced several cyberattacks, likely from their adversary JobeCorp.
* Fortunately, your SOC team had set up several monitoring solutions to help VSI quickly identify what was attacked.
* These monitoring solutions will also help VSI create mitigation strategies to protect the organization.

You have been provided two logs files of suspicious activity:

* One for a Windows server
* One for an Apache web server

### **Windows Server Logs**

Load the logs in your Splunk environment.

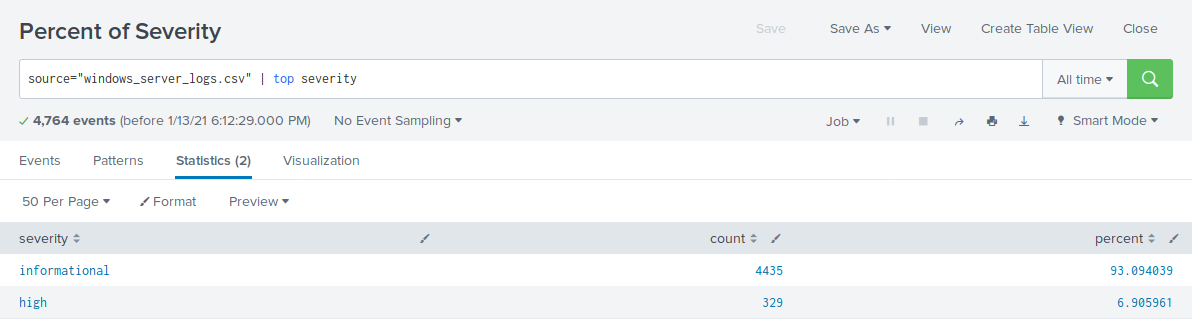
* Select all default options provided.
* **Important:** For the time range, always select **All Time**.  
   - **Important:** For the time range, always select **All Time**.
* **Important:** For the time range, always select **All Time**.

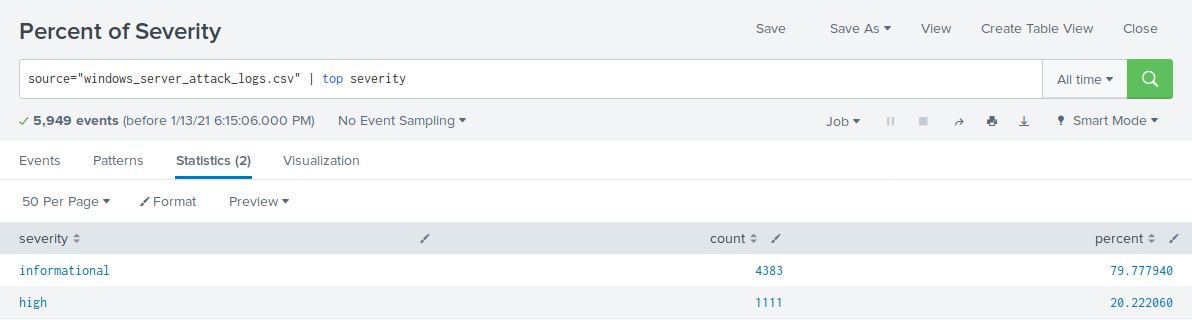
Now you will review the reports you created in Part 1 and analyze the results.

#### **Report Analysis for Severity**

1. Access the **Reports** tab and select **Yours** to view the reports created from Part 1.
2. Select the report you created to analyze the different severities.
3. Select **Edit** > **Open in Search**.
4. Take note of the percentages of different severities.
5. Change the source from source=”windows\_server\_logs.csv” to source="windows\_server\_attack\_logs.csv”.
6. Select **Save**.

Review the updated results and answer the following question:



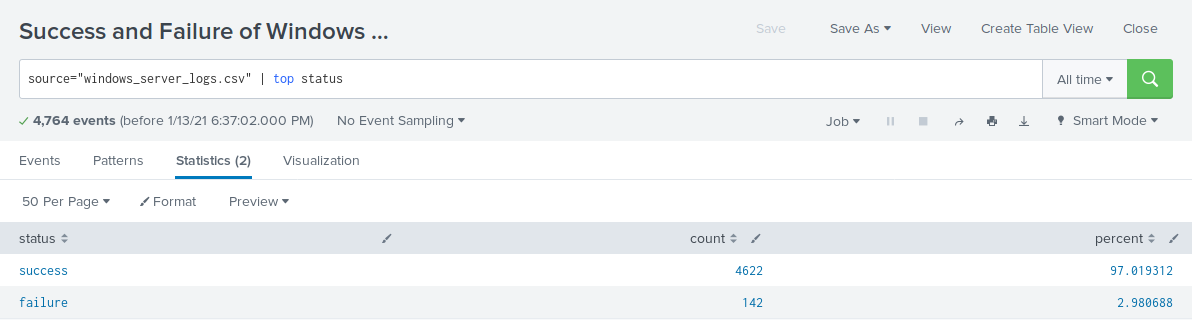


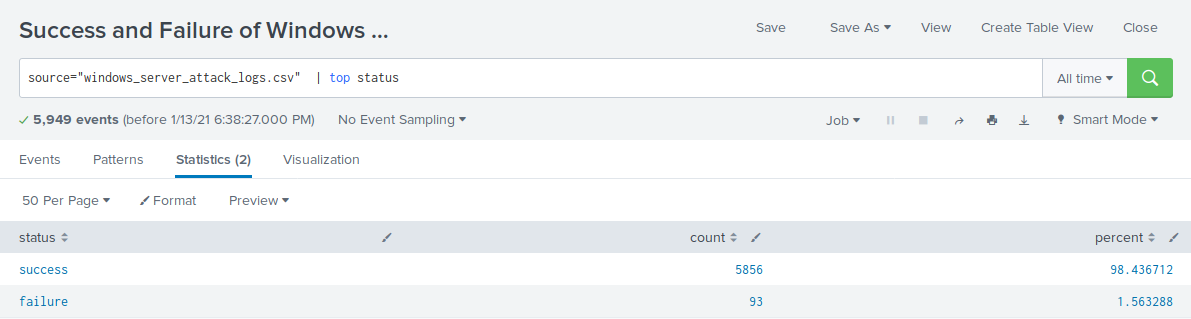
* Did you detect any suspicious changes in severity?
* Informational: Went from 93% to 80% resulting in a 13% decrease.
* High: Went from 7% to 20% resulting in a 13% increase.
* These results suggest there are suspicious changes in severity.

#### **Report Analysis for Failed Activities**

1. Access the **Reports** tab and select **Yours** to view the reports created from Part 1.
2. Select the report you created to analyze the different activities.
3. Select **Edit** > **Open in Search**.
4. Take note of the failed activities percentage.
5. Change the source from windows\_server\_logs.csv to "source="windows\_server\_attack\_logs.csv”.
6. Select **Save**.

Review the updated results and answer the following question:





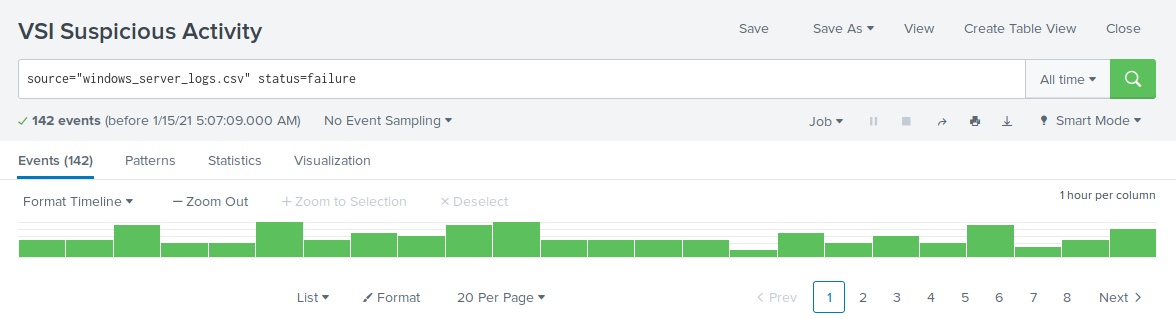
* Did you detect any suspicious changes in failed activities?
* Success: Went from 97% to 98% resulting in a 1% increase.
* Failure: Went from 3% to 2% resulting in a 1% decrease.
* These results suggest there were no major changes in failed activities.

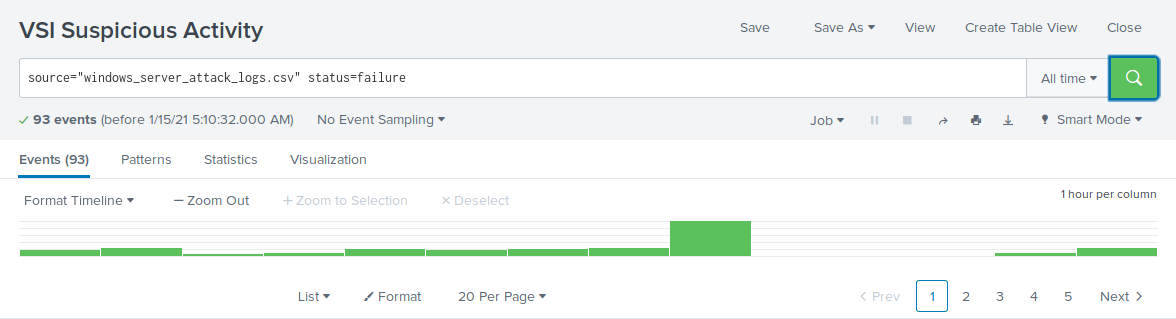
Now you will review the alerts you created in Part 1 and analyze the results.

#### **Alert Analysis for Failed Windows Activity**

1. Access the **Alerts** tab and select **Yours** to view the alerts created in Part 1.
2. Select the alert for suspicious volume of failed activities.
3. Select **Open in Search**.
4. Change the source from source=”windows\_server\_logs.csv” to source="windows\_server\_attack\_logs.csv”.

Review the updated results and answer the following questions:





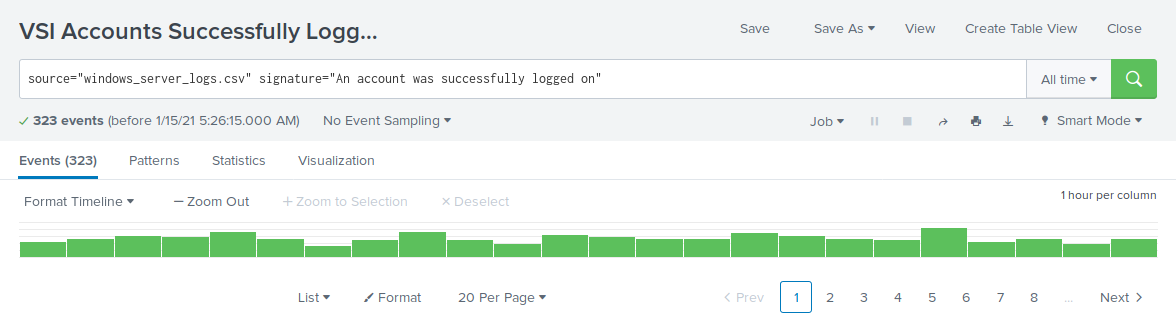
* Did you detect a suspicious volume of failed activity?
* There was potential for a suspicious volume of failed activity at 8:00 a.m. on Wednesday, March 25th.
* If so, what was the count of events in the hour(s) it occurred?
* The count of activity was 35 events during this hour.
* When did it occur?
* 8:00 a.m. on Wednesday, March 25th.
* Would your alert be triggered for this activity?
* Yes, the alert is within the trigger threshold.
* After reviewing, would you change your threshold from what you previously selected?
* No change in threshold necessary.

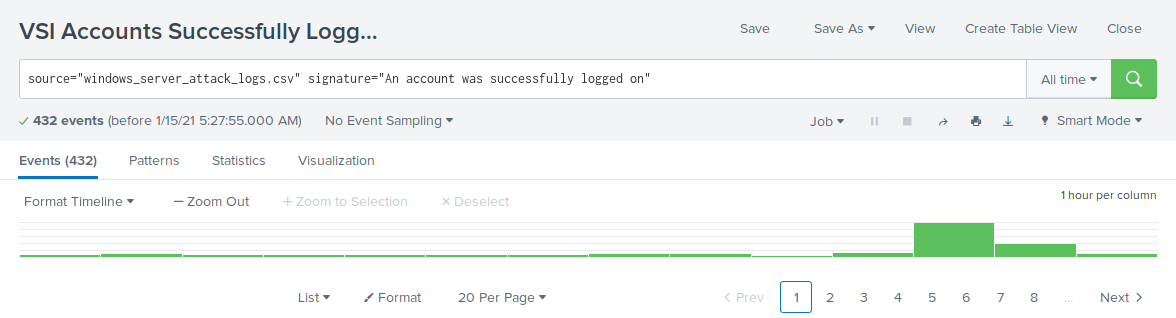
#### 

#### **Alert Analysis for Successful Logons**

1. Access the **Alerts** tab and select **Yours** to view the alerts created in Part 1.
2. Select the alert of suspicious volume of successful logons.
3. Select **Open in Search**.
4. Change the source from source=”windows\_server\_logs.csv” to source="windows\_server\_attack\_logs.csv”.

Review the updated results, and answer the following questions:



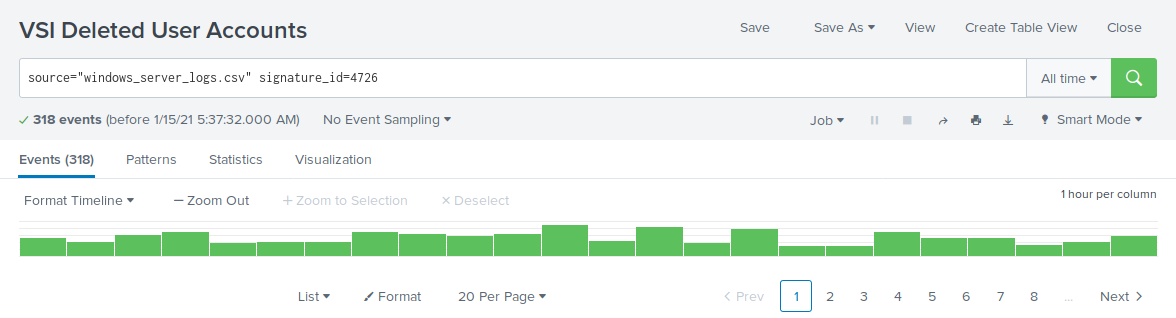


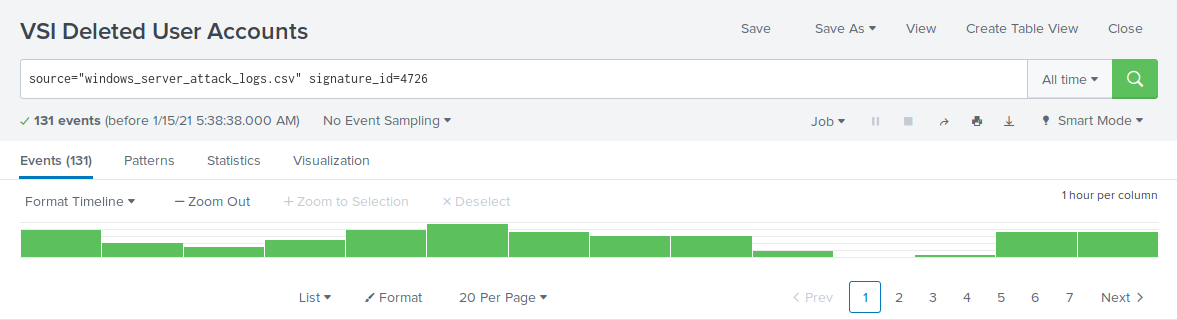
* Did you detect a suspicious volume of successful logons?
* There was potential for suspicious activity at 11:00 a.m. and 12:00 p.m. on Wednesday, March 25th.
* If so, what was the count of events in the hour(s) it occurred?
* The count of activity is 196 events at 11:00 a.m. and 77 events at 12:00 p.m.
* Who is the primary user logging in?
* The primary user logging in was user\_j.
* When did it occur?
* The suspicious activities occurred at 11:00 a.m. and 12:00 p.m. on Wednesday, March 25th.
* Would your alert be triggered for this activity?
* Yes, the alert is within the trigger threshold.
* After reviewing, would you change your threshold from what you previously selected?
* No change in threshold necessary.

#### **Alert Analysis for Deleted Accounts**

1. Access the **Alerts** tab and select **Yours** to view the alerts created in Part 1.
2. Select the alert of suspicious volume of deleted accounts.
3. Select **Open in Search**.
4. Change the source from windows\_server\_logs.csv to source="windows\_server\_attack\_logs.csv”.

Review the updated results and answer the following question:





Now you will set up a dashboard and analyze the results.

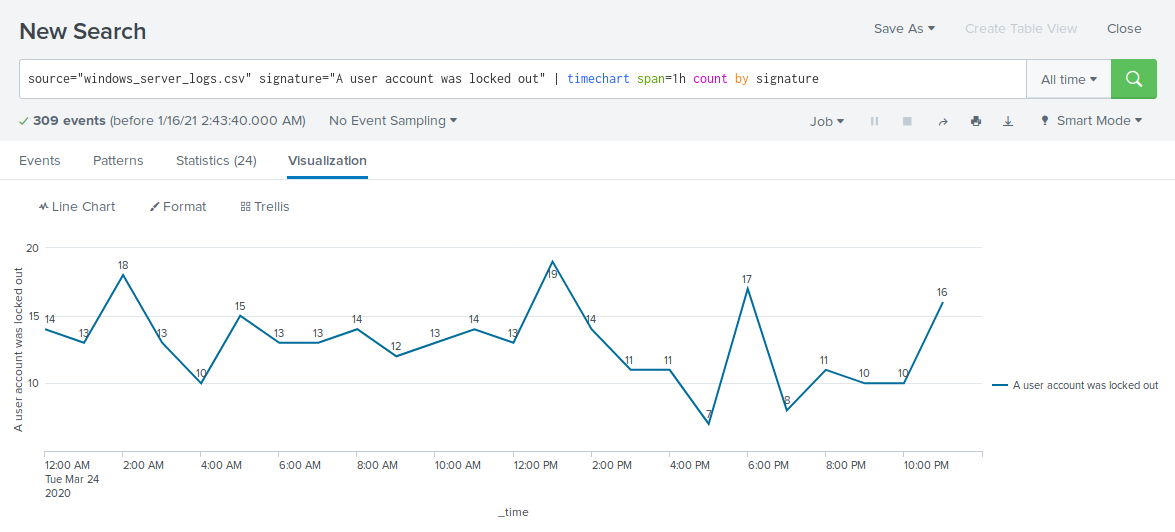
* Did you detect a suspicious volume of deleted accounts?
* There were no signs of suspicious volumes of deleted accounts.

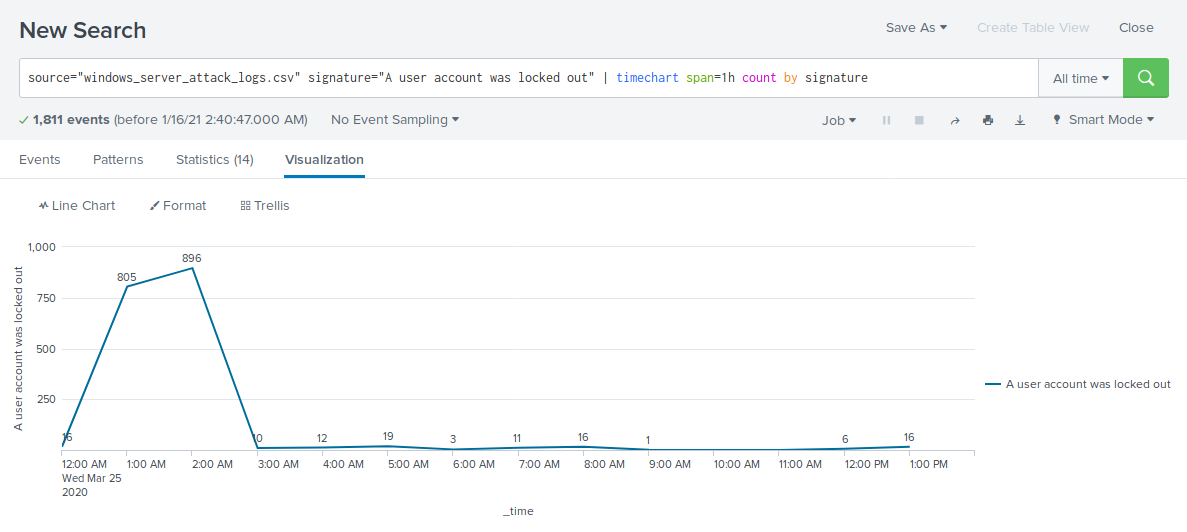
#### **Dashboard Setup**

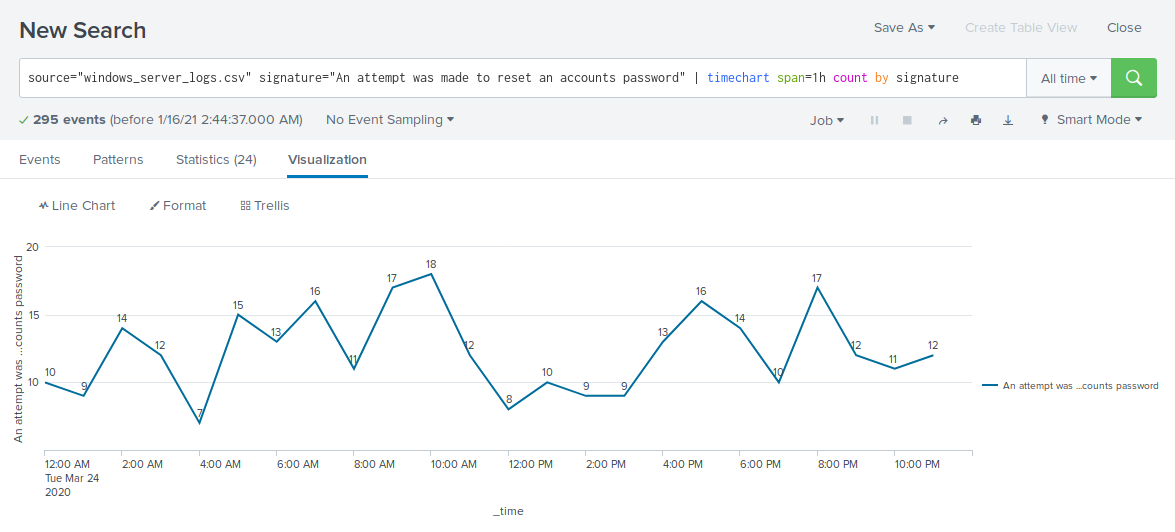
1. Access the **Windows Server Monitoring** dashboard.  
   * Select **Edit**.
2. Access each panel you created and complete the following:  
   * Select **Edit Search**.
   * Change the source from: windows\_server\_logs.csv to source="windows\_server\_attack\_logs.csv”.
   * Select **Apply**.
   * Save the dashboard.
   * Edit the time on the dashboard to be **All Time**.

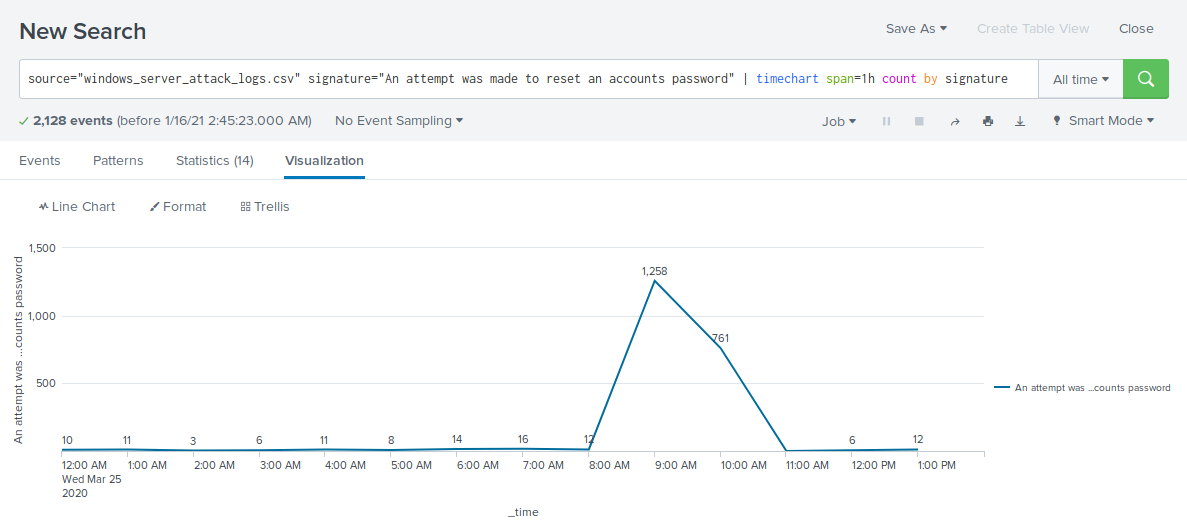
#### **Dashboard Analysis for Time Chart of Signatures**

Analyze your new dashboard results and answer the following questions:





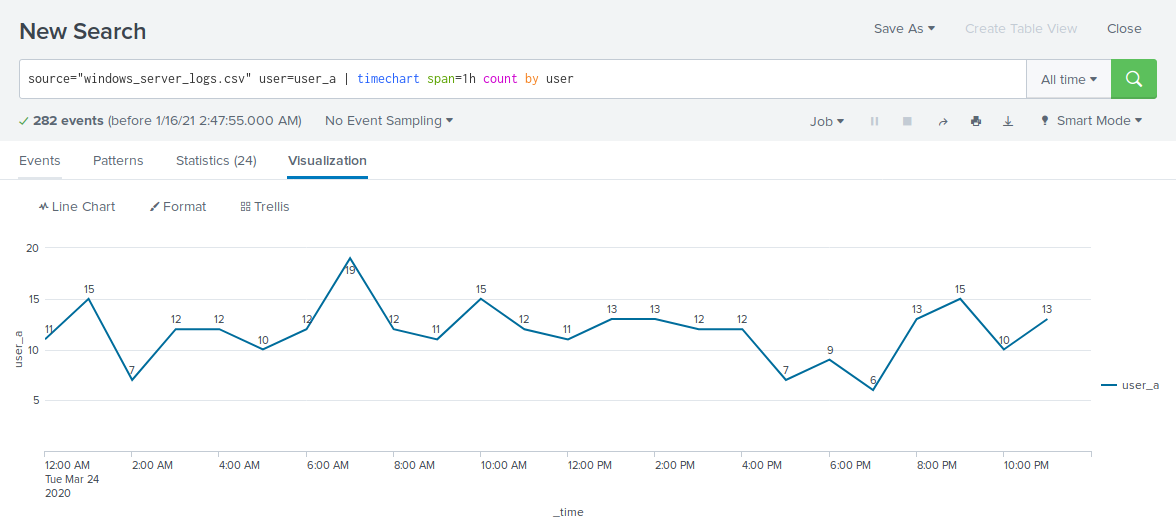


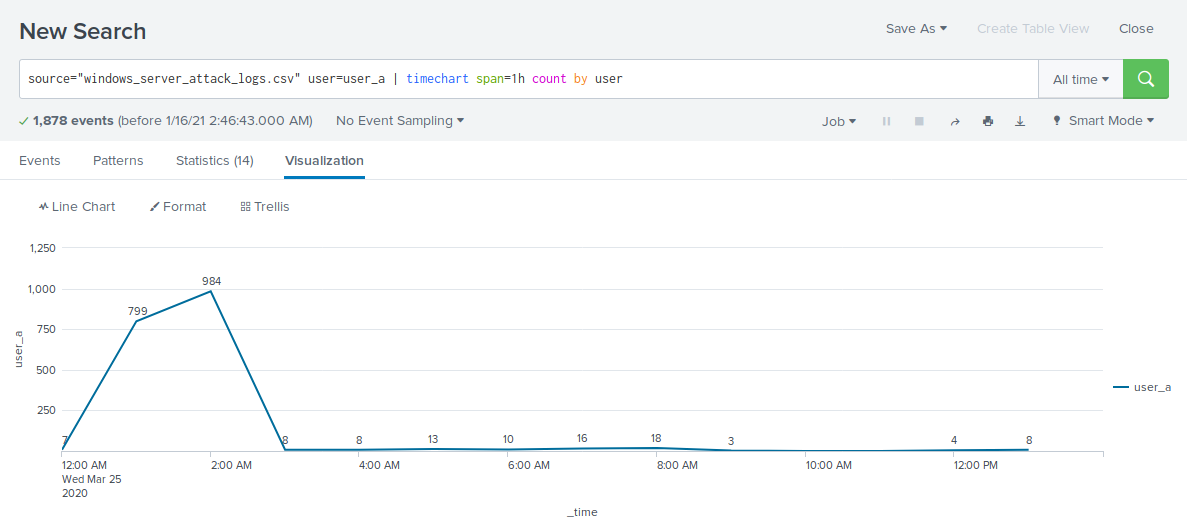


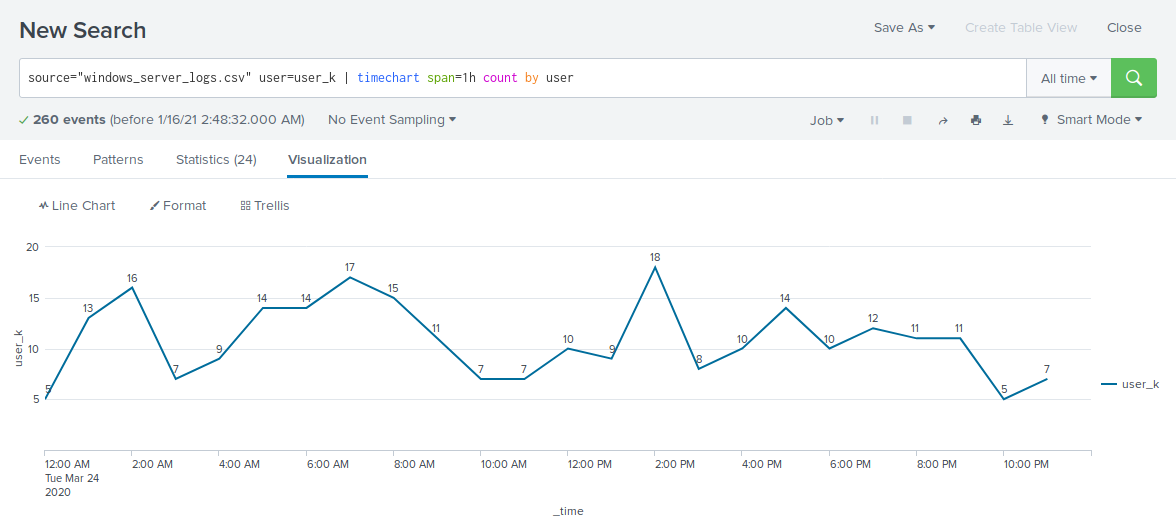
* Does anything stand out as suspicious?
* There was suspicious activity with the signature “An account was locked out” from 12:00 a.m. to 3:00 a.m. on Wednesday, March 25th and with the signature “An attempt was made to reset an accounts password” from 8:00 a.m. to 11:00 a.m. on Wednesday, March 25th.
* Which signatures stand out?
* “A user account was locked out” signature stands out for suspicious activity.
* “An attempt was made to reset an accounts password” signature stands out for suspicious activity.
* What time did it begin/stop for each signature?
* A user account was locked out: Started at 12:00 a.m. on Wednesday, March 25th and stopped at 3:00 a.m. on Wednesday, March 25th.
* An attempt was made to reset an accounts password: Started at 8:00 a.m on Wednesday, March 25th and stopped at 11:00 a.m. on Wednesday, March 25th.
* What is the peak count of the different signatures?
* A user account was locked out: Peak count during the attack was at 896.
* An attempt was made to reset an accounts password: Peak count during the attack was at 1,258.

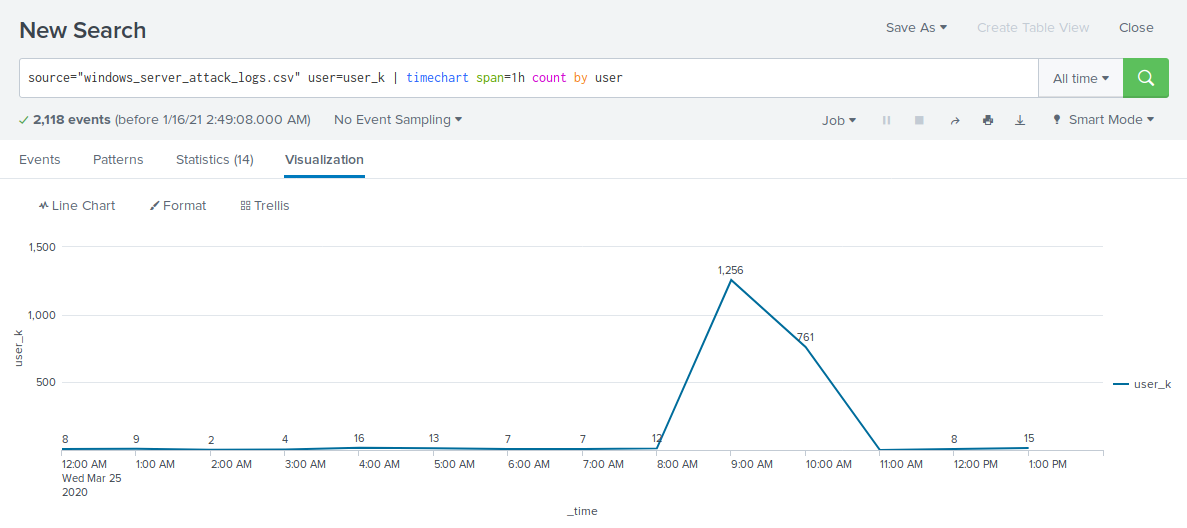
#### **Dashboard Analysis for Time Chart of Users**

Analyze your new dashboard results and answer the following questions:





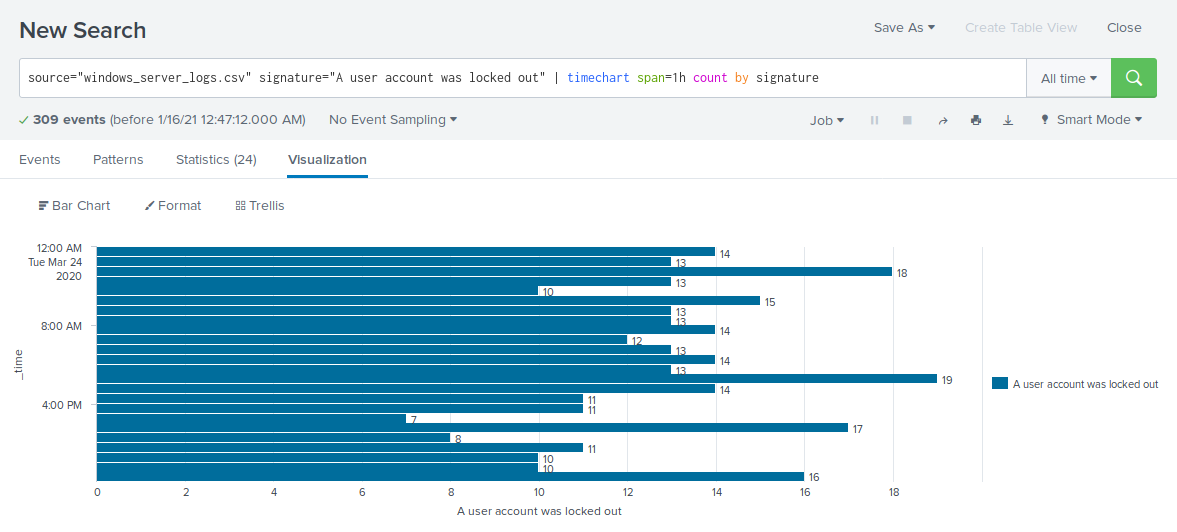


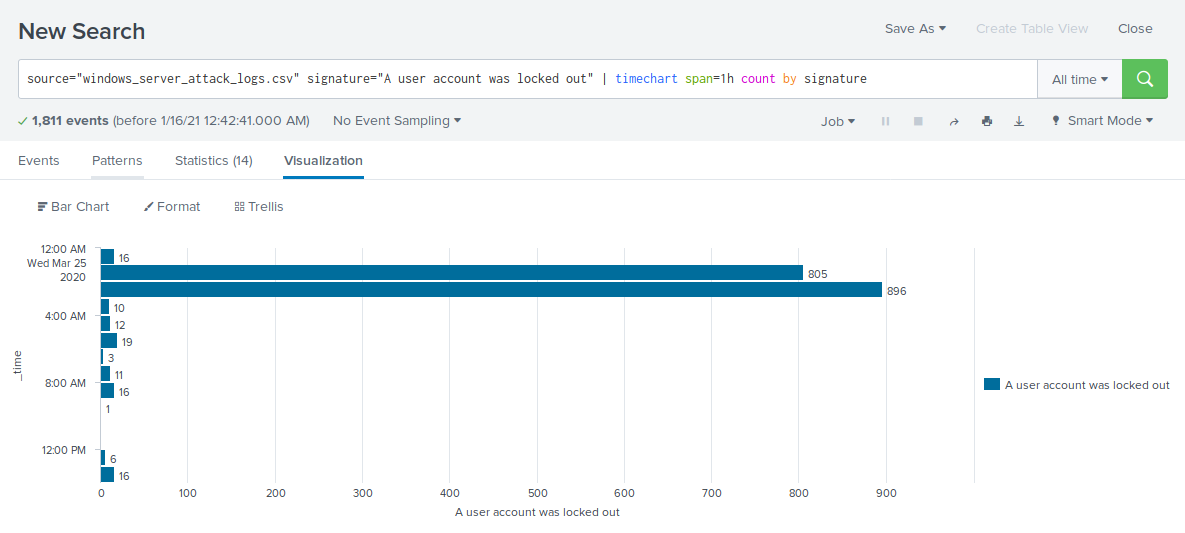


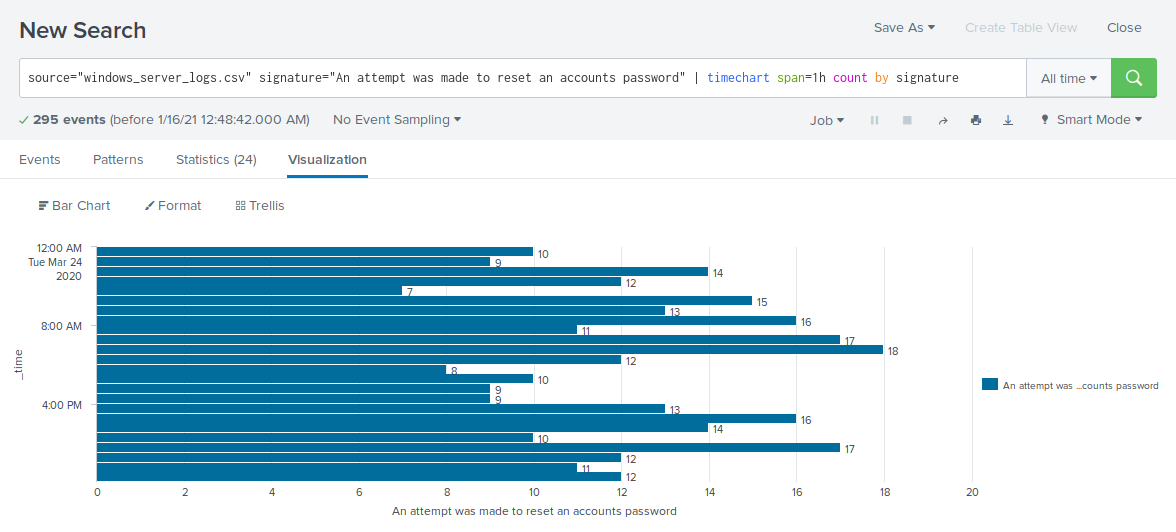
* Does anything stand out as suspicious?
* There was suspicious activity at 12:00 a.m. and 3:00 a.m. on Wednesday, March 25th and at 9:00 a.m. and 10 a.m. on Wednesday, March 25th.
* Which users stand out?
* user\_a and user\_k stand out for suspicious activity.
* What time did it begin and stop for each user?
* user\_a: Started at 12:00 a.m. on Wednesday, March 25th and stopped at 3:00 a.m. on Wednesday, March 25th.
* user\_k: Started at 8:00 a.m on Wednesday, March 25th and stopped at 11:00 a.m. on Wednesday, March 25th.
* What is the peak count of the different users?
* user\_a: Peak count was at 984.
* user\_k: Peak count was at 1,256.

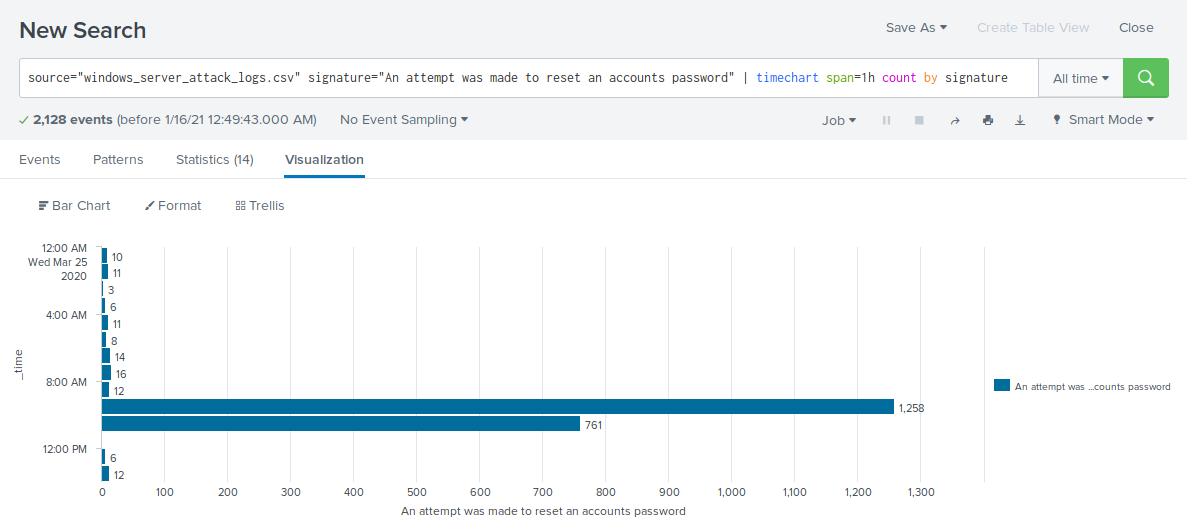
#### **Dashboard Analysis for Signatures with Bar, Graph, and Pie Charts**

Analyze your new dashboard results and answer the following questions:









* Does anything stand out as suspicious?
* There was suspicious activity starting at 12:00 a.m. and 3:00 a.m. on Wednesday, March 25th and at 8:00 a.m. and 11 a.m. on Wednesday, March 25th.
* Which signatures stand out?
* “A user account was locked out” signature stands out for suspicious activity.
* “An attempt was made to reset an accounts password” signature stands out for suspicious activity.
* What time did it begin/stop for each signature?
* A user account was locked out: Started at 12:00 a.m. on Wednesday, March 25th and stopped at 3:00 a.m. on Wednesday, March 25th.
* An attempt was made to reset an accounts password: Started at 8:00 a.m on Wednesday, March 25th and stopped at 11:00 a.m. on Wednesday, March 25th.
* What is the peak count of the different signatures?
* A user account was locked out: Peak count was at 896.
* An attempt was made to reset an accounts password: Peak count was at 1,258.
* Do the results match your findings in your time chart for signatures?
* Yes, the results were synonymous with the findings.

#### 

#### 

#### 

#### 

#### 

#### 

#### 

#### 

#### 

#### 

#### 

#### 

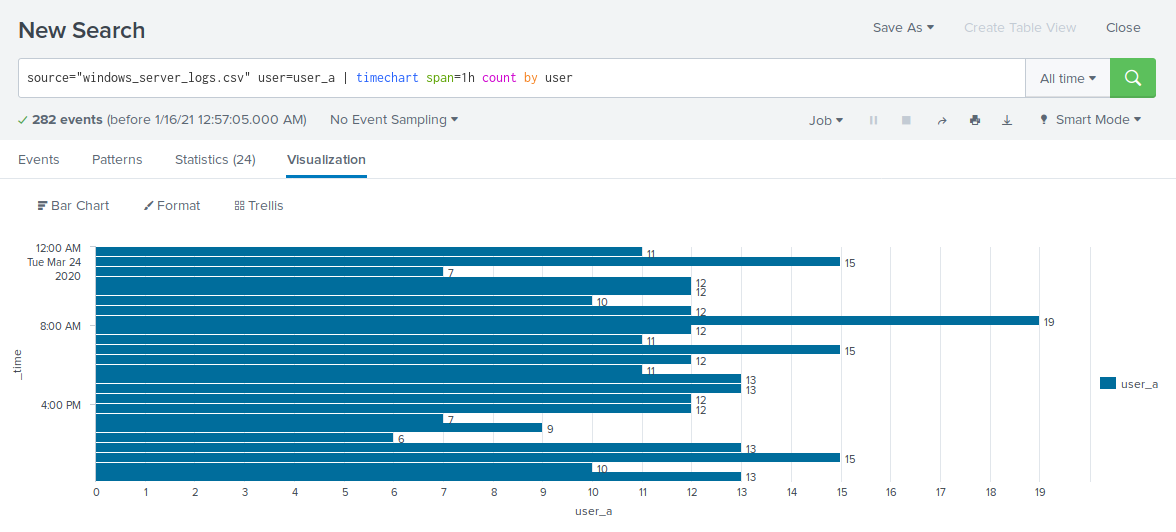
#### 

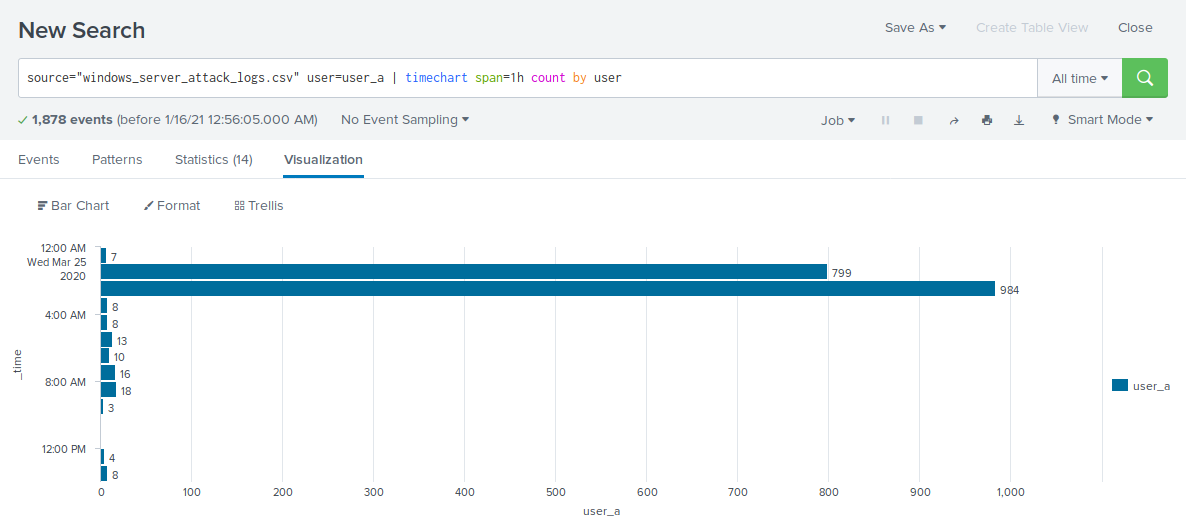
#### 

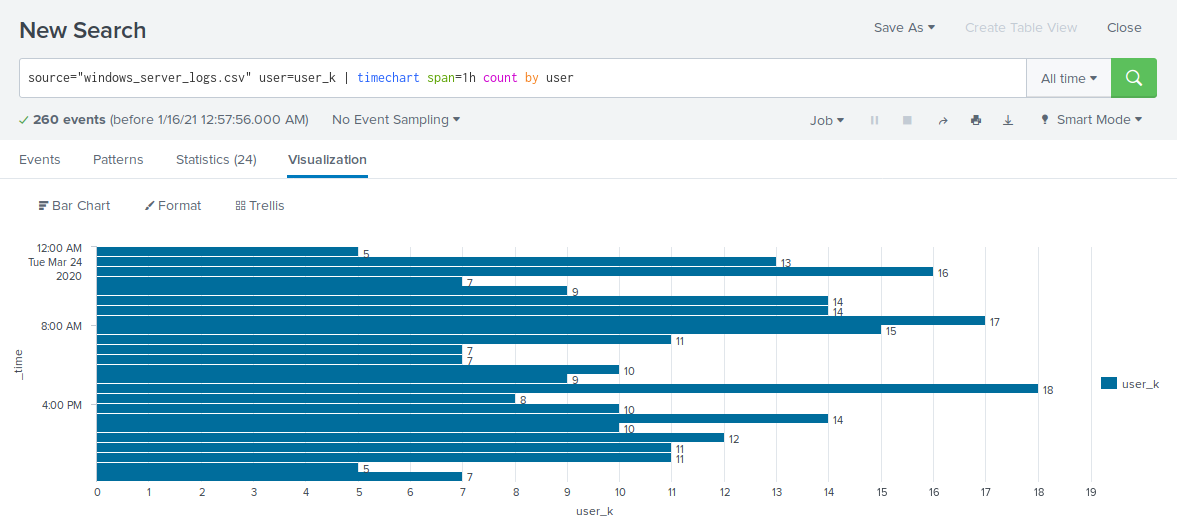
#### 

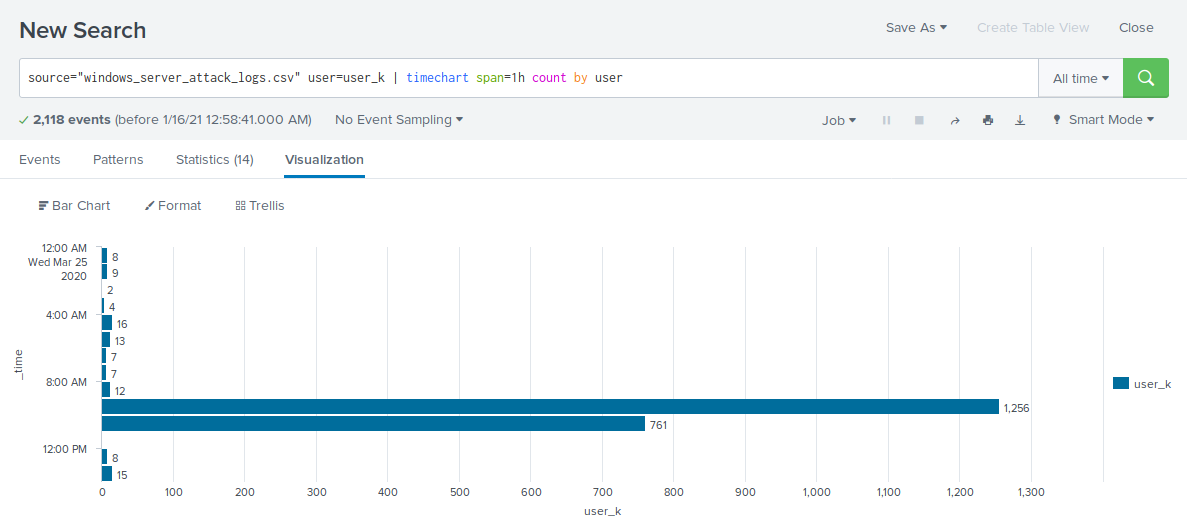
#### **Dashboard Analysis for Users with Bar, Graph, and Pie Charts**

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



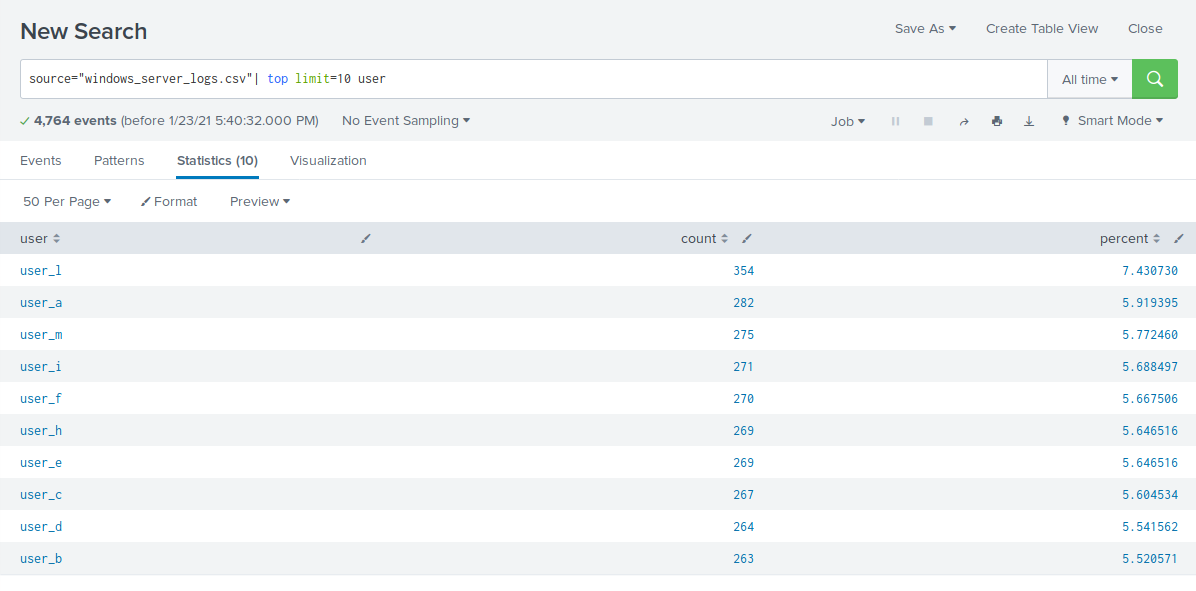


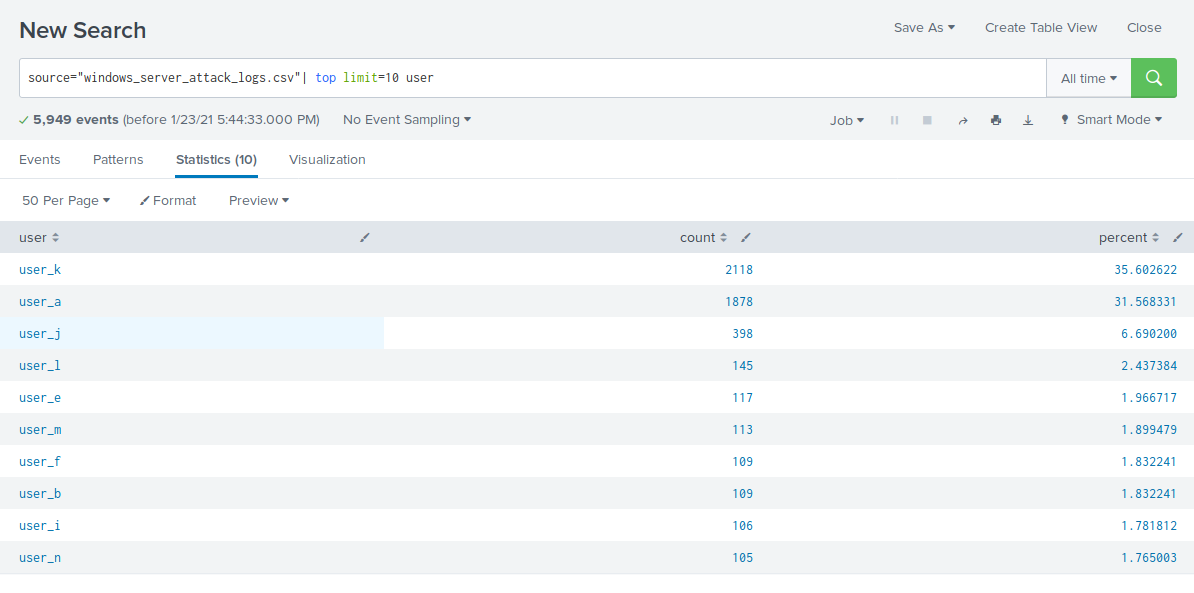




* Does anything stand out as suspicious?
* There was suspicious activity at 12:00 a.m. and 3:00 a.m. on Wednesday, March 25th and at 9:00 a.m. and 10 a.m. on Wednesday, March 25th.
* Which users stand out?
* user\_a and user\_k stand out for suspicious activity.
* What time did it begin and stop for each user?
* user\_a: Started at 12:00 a.m. on Wednesday, March 25th and stopped at 3:00 a.m. on Wednesday, March 25th.
* user\_k: Started at 8:00 a.m on Wednesday, March 25th and stopped at 11:00 a.m. on Wednesday, March 25th.
* What is the peak count of the different users?
* user\_a: Peak count was at 984.
* user\_k: Peak count was at 1,256.
* Do the results match your findings in your time chart for users?
* Yes, the results were synonymous with the findings.

#### **Dashboard Analysis for Users with Statistical Charts**





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

* What are the advantages and disadvantages of using this report, compared to the other user panels you created?
* An advantage of a statistical chart is a concise list of the top users accused of suspicious activity. A disadvantage of the statistical chart is that it shows a cumulative perspective of data while other approaches to data representation show a shorter, more specific perspective of data.

### 

### 

### 

### 

### 

### 

### 

### 

### **Apache Web Server Logs**

Load the logs in your Splunk environment.

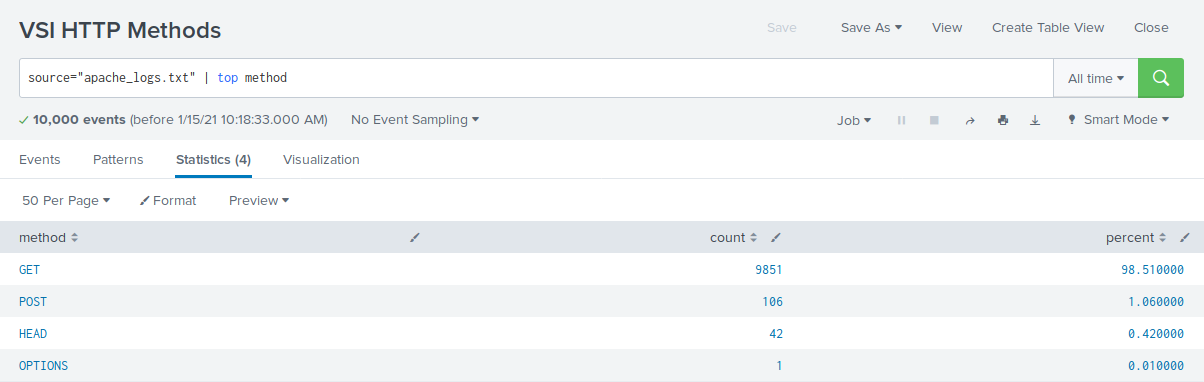
* Select all default options provided.
* **Important:** For the time range, always select **All Time**.

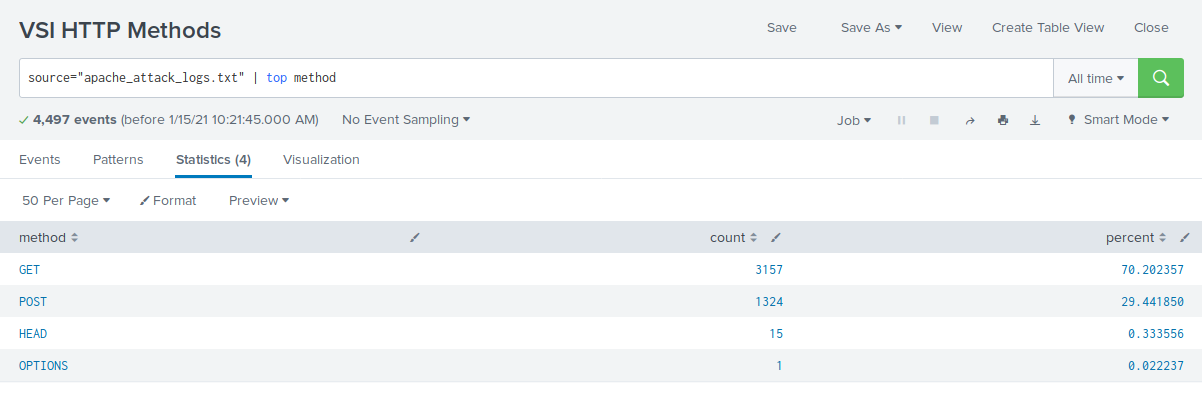
Now you will review the reports you created in Part 1 and analyze the results.

#### **Report Analysis for Methods**

1. Access the **Reports** tab and select **Yours** to view the reports created from Part 1.
2. Select the report that analyzes the different HTTP methods.
3. Select **Edit** > **Open in Search**.
4. Take note of the percent/count of the various methods.
5. Change the source from: source=”apache\_logs.txt” to source="apache\_attack\_logs.txt”.
6. Select **Save**.

Review the updated results and answer the following questions:





1. Did you detect any suspicious changes in HTTP methods? If so which one?

* Get: Yes, there was a suspicious decrease in GET activity by 29%.
* Post: Yes, there was a suspicious increase in POST activity by 29%.

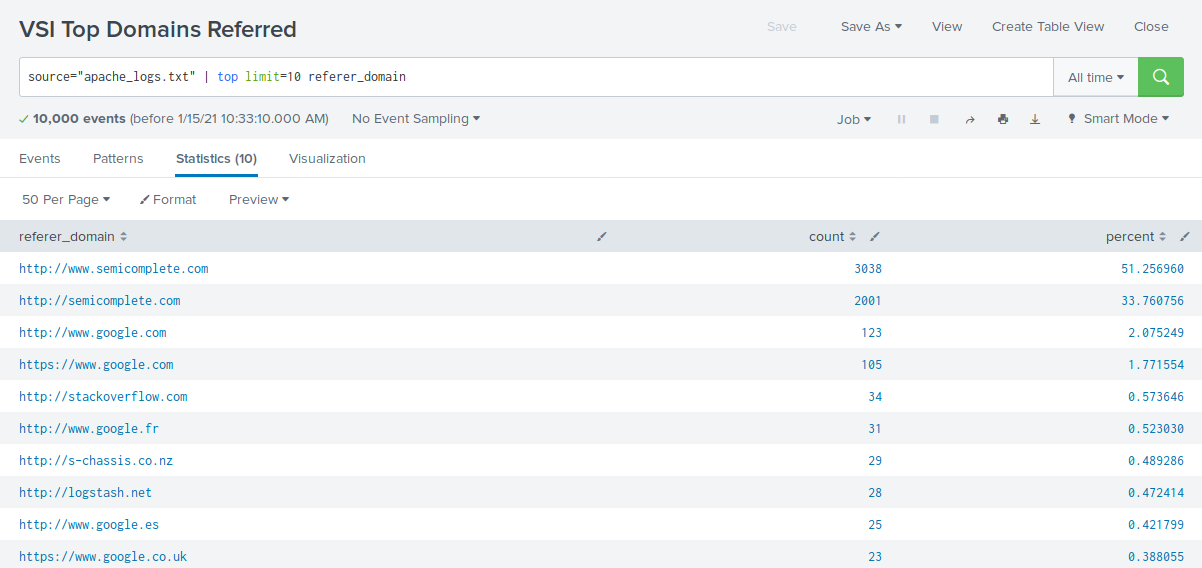
1. What is that method used for?

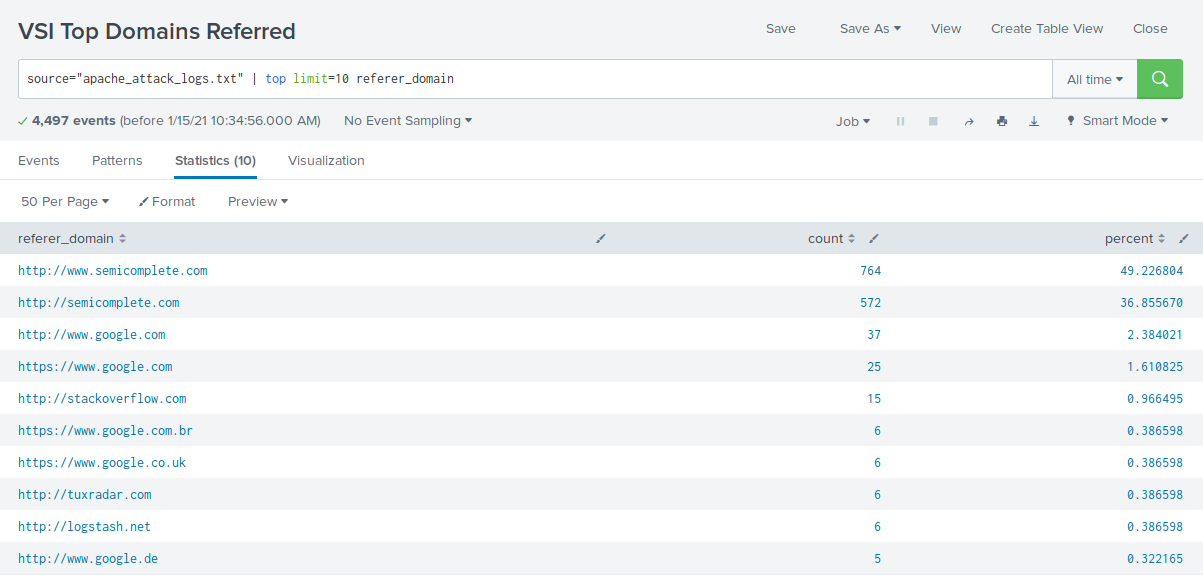
* POST is used to submit or update information to a web server.

#### **Report Analysis for Referrer Domains**

1. Access the **Reports** tab and select **Yours** to view the reports created from Part 1.
2. Select the report that analyzes the different referrer domains.
3. Select **Edit** > **Open in Search**.
4. Take note of the different referrer domains.
5. Change the source from: source=”apache\_logs.txt” to source="apache\_attack\_logs.txt”.
6. Select **Save**.

Review the updated results, and answer the following question:





1. Did you detect any suspicious changes in referrer domains?

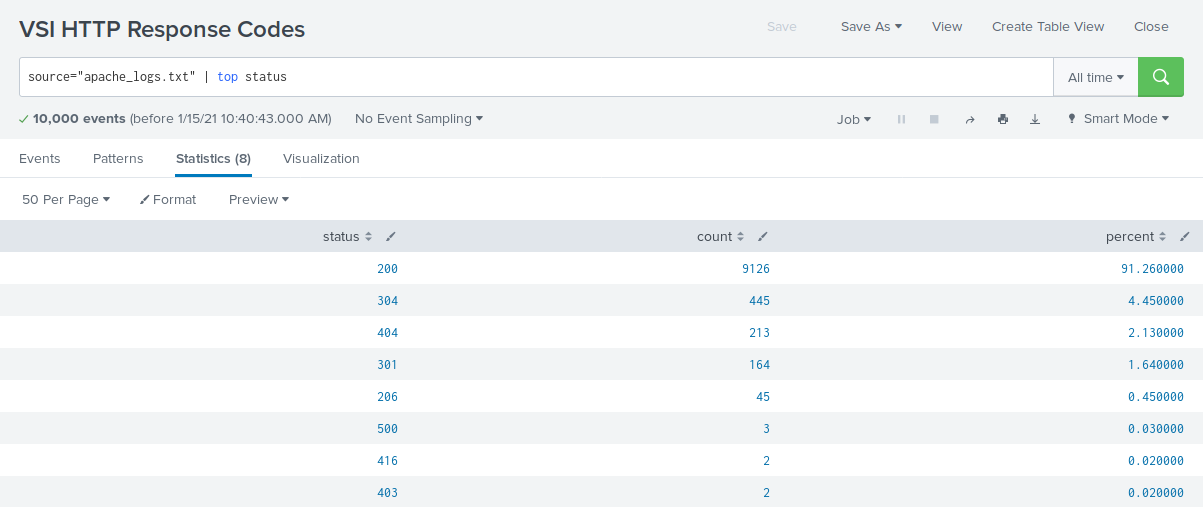
* There were no suspicious referrer domains during the attack.

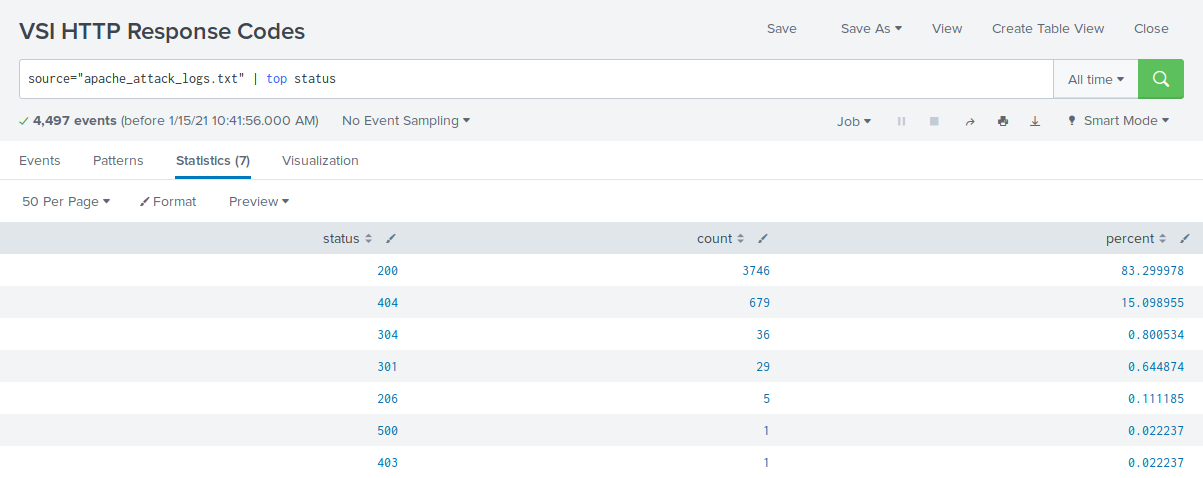
#### 

#### **Report Analysis for HTTP Response Codes**

1. Access the **Reports** tab and select **Yours** to view the reports created from Part 1.
2. Select the report that analyzes the different HTTP response codes.
3. Select **Edit** > **Open in Search**.
4. Take a note of the different HTTP response codes.
5. Change the source from: source=”apache\_logs.txt” to source="apache\_attack\_logs.txt”.
6. Select **Save**.

Review the updated results and answer the following question:





1. Did you detect any suspicious changes in HTTP response codes?

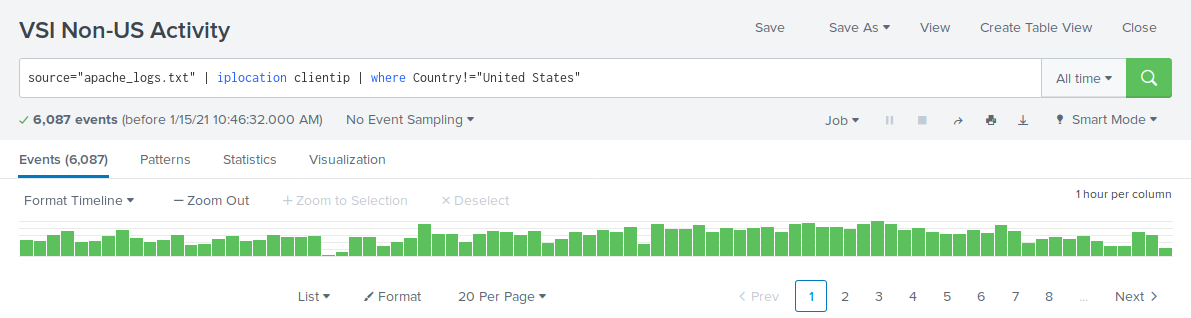
* There are several small changes overall, but the most suspicious change detected was the 404 response code increasing from 2% to 15%.

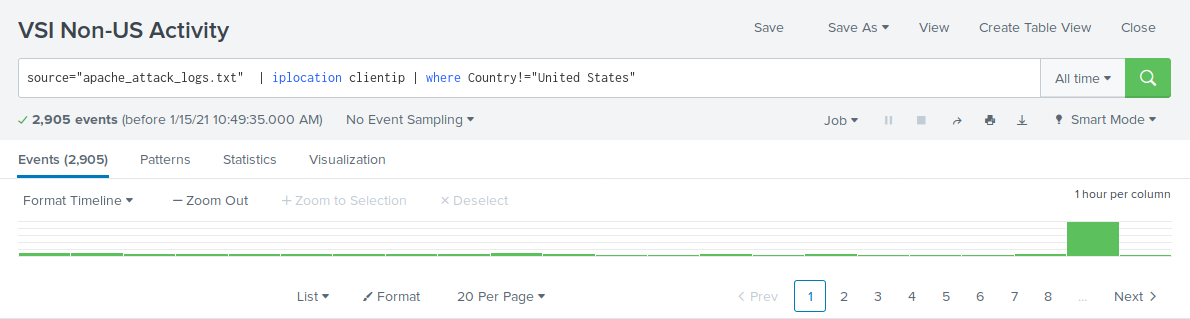
Now you will review the alerts you created in Part 1 and analyze the results.

#### **Alert Analysis for International Activity**

1. Access the **Alerts** tab and select **Yours** to view the alerts created in Part 1.
2. Select the alert of suspicious volume of international activity.
3. Select **Open in Search**.
4. Change the source from: source=”apache\_logs.txt” to source="apache\_attack\_logs.txt”.

Review the updated results and answer the following questions:



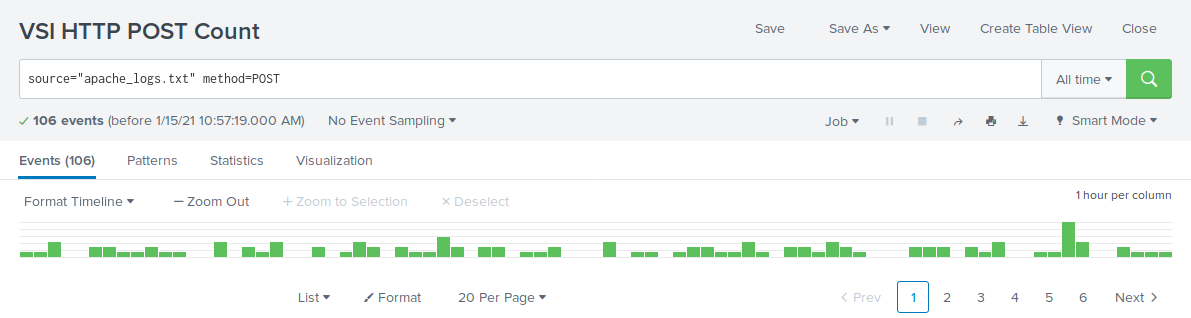


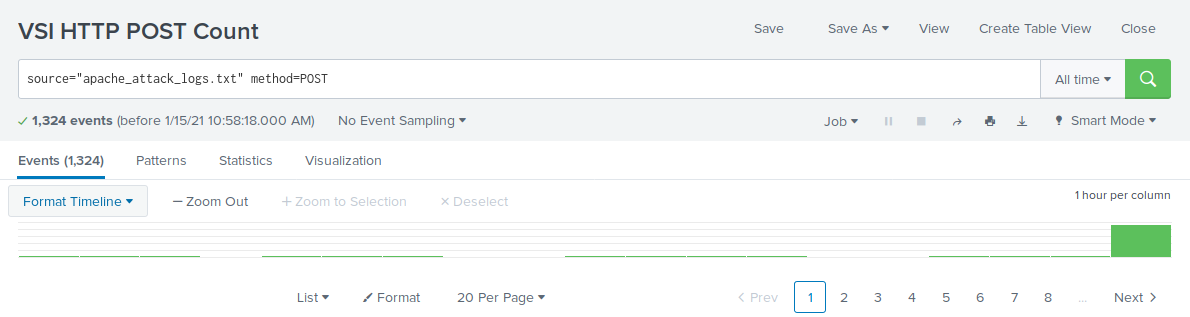
* Did you detect a suspicious volume of international activity?
* Yes, there was a suspicious volume of activity in Ukraine at 8:00 p.m. on March 25th.
* If so, what was the count of the hour it occurred in?
* Ukraine had a count of 1,369 events during the 8:00 p.m. attack.
* Would your alert be triggered for this activity?
* Yes, the alert is within the trigger threshold.
* After reviewing, would you change the threshold you previously selected?
* No change in threshold necessary.

#### **Alert Analysis for HTTP POST Activity**

1. Access the **Alerts** tab and select **Yours** to view the alerts created in Part 1.
2. Select the alert of suspicious volume of HTTP POST activity.
3. Select **Open in Search**.
4. Change the source from: source=”apache\_logs.txt” to source="apache\_attack\_logs.txt”.

Review the updated results, and answer the following questions:





* Did you detect any suspicious volume of HTTP POST activity?
* Yes, there was a suspicious increase of POST method activities.
* If so, what was the count of the hour it occurred in?
* There was a total count of 1,296 events at 8:00 p.m.
* When did it occur?
* The event occurred at 8:00 p.m. on Wednesday, March 25th.
* After reviewing, would you change the threshold that you previously selected?
* No change in threshold necessary.

Now you will set up a dashboard and analyze the results.

#### **Dashboard Setup**

* Access the dashboard for Apache WebServer Monitoring.
* Select **Edit**.
* Access each panel and complete the following:  
  + Select **Edit Search**.
  + Change the source from: source=”apache\_logs.txt” to source="apache\_attack\_logs.txt”.
  + Select **Apply**.
* Save the whole dashboard.
* Edit the time on the whole dashboard to be **All Time**.

#### 

#### 

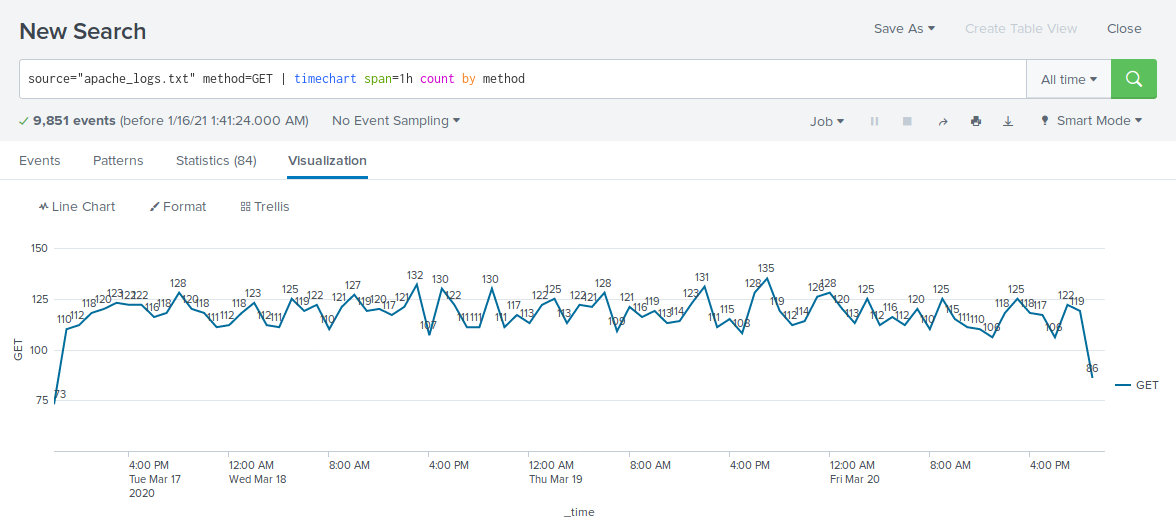
#### 

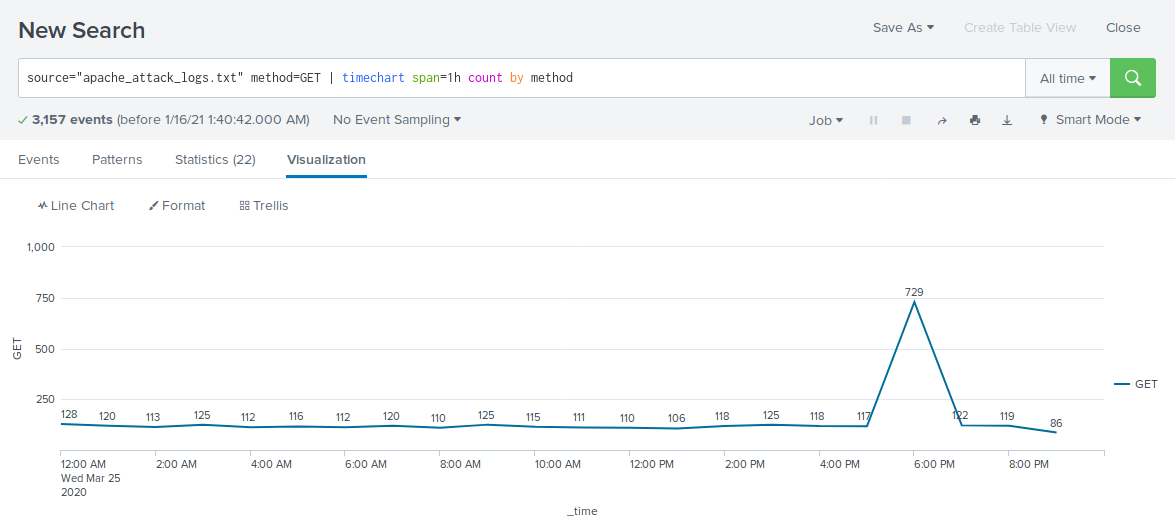
#### 

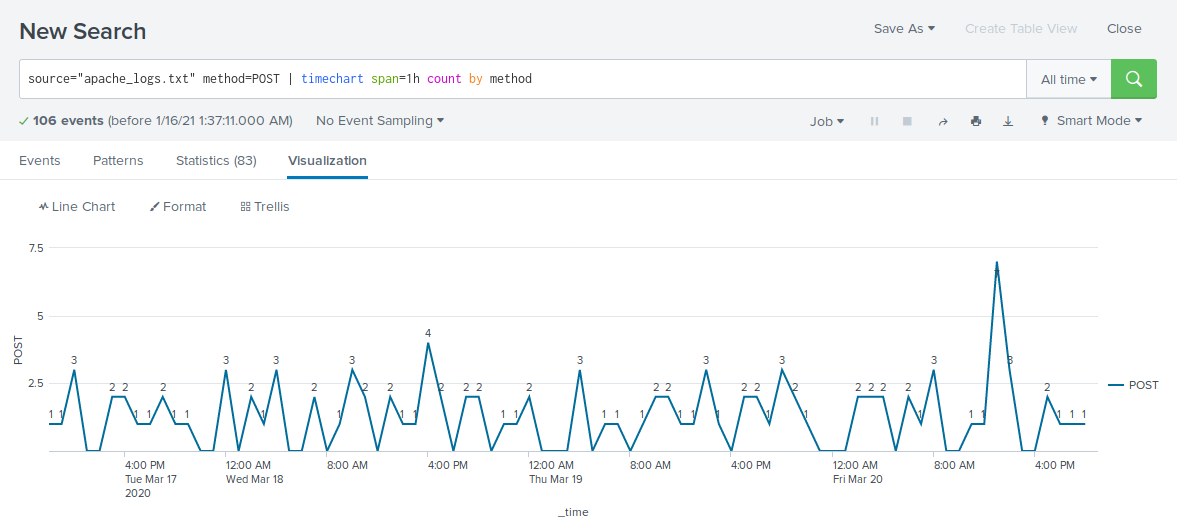
#### 

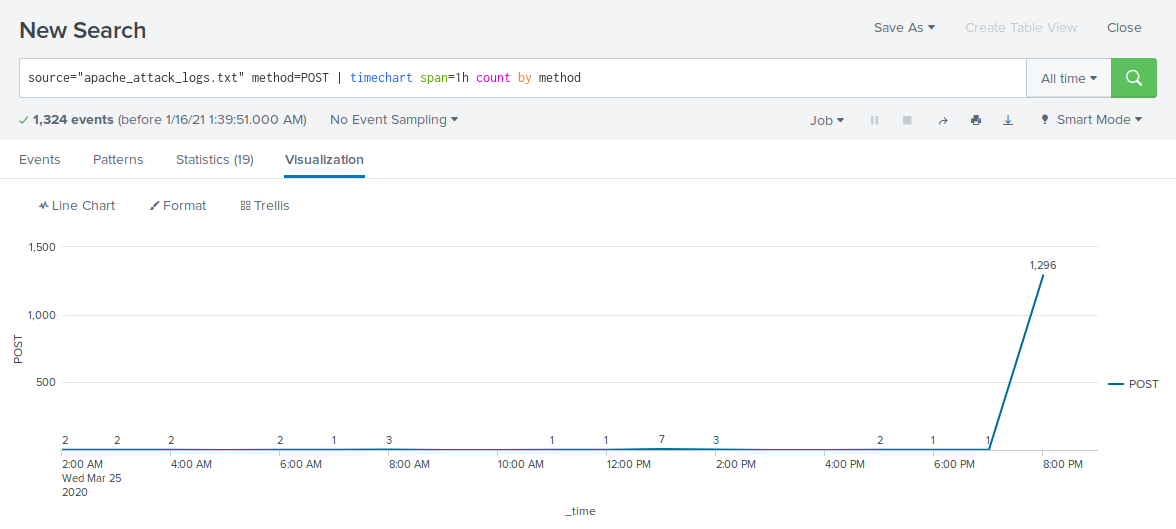
#### **Dashboard Analysis for Time Chart of HTTP Methods**

Analyze your new dashboard results and answer the following questions:









* Does anything stand out as suspicious?
* There was suspicious activity with the method “GET” from 5:00 p.m. to 7:00 p.m. on Wednesday, March 25th and with the method “POST” from 7:00 p.m. to 8:00 p.m. on Wednesday, Match 25th.
* Which method seems to be used in the attack?
* The “GET” method seemed to be used in the attack.
* The “POST” method seemed to be used in the attack.
* At what times did the attack start and stop?
* GET: Started at 5:00 p.m. on Wednesday, March 25th and stopped at 7:00 p.m. on Wednesday, March 25th.
* POST: Started at 7:00 p.m on Wednesday, March 25th and stopped at 8:00 p.m. on Wednesday, March 25th.
* What is the peak count of the top method during the attack?
* GET: Peak count during the attack was 1,296.
* POST: Peak count during the attack was 729.

#### 

#### 

#### 

#### 

#### 

#### 

#### 

#### 

#### 

#### 

#### 

#### 

#### 

#### 

#### 

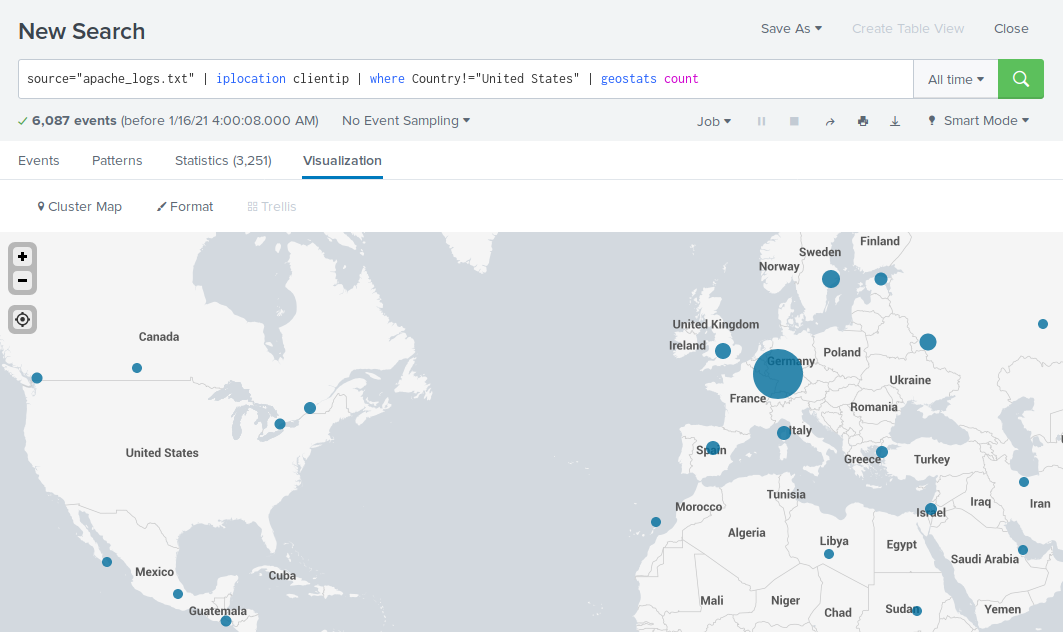
#### 

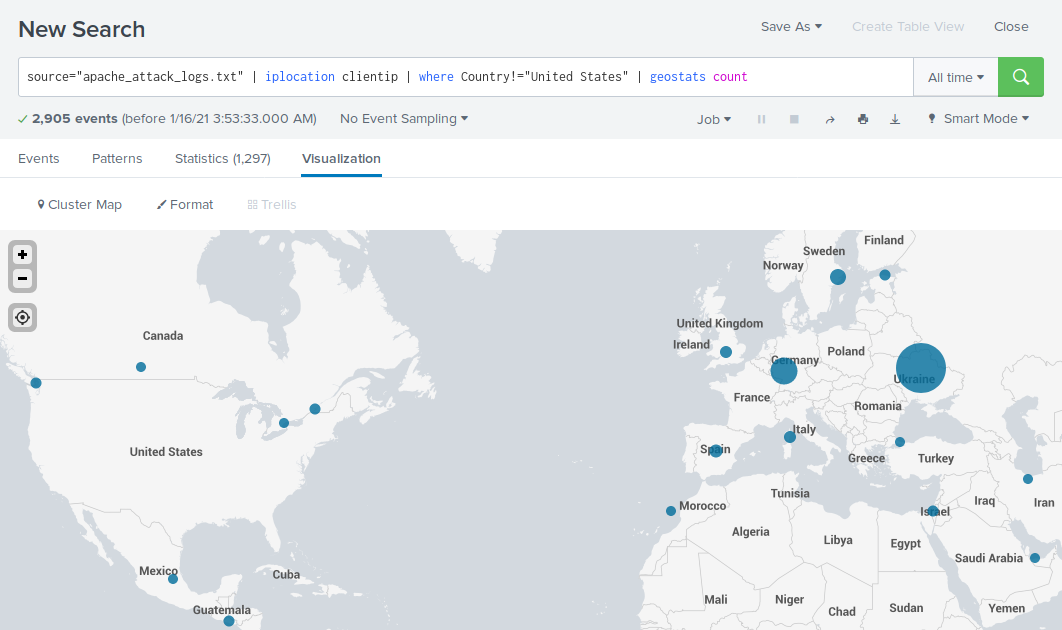
#### 

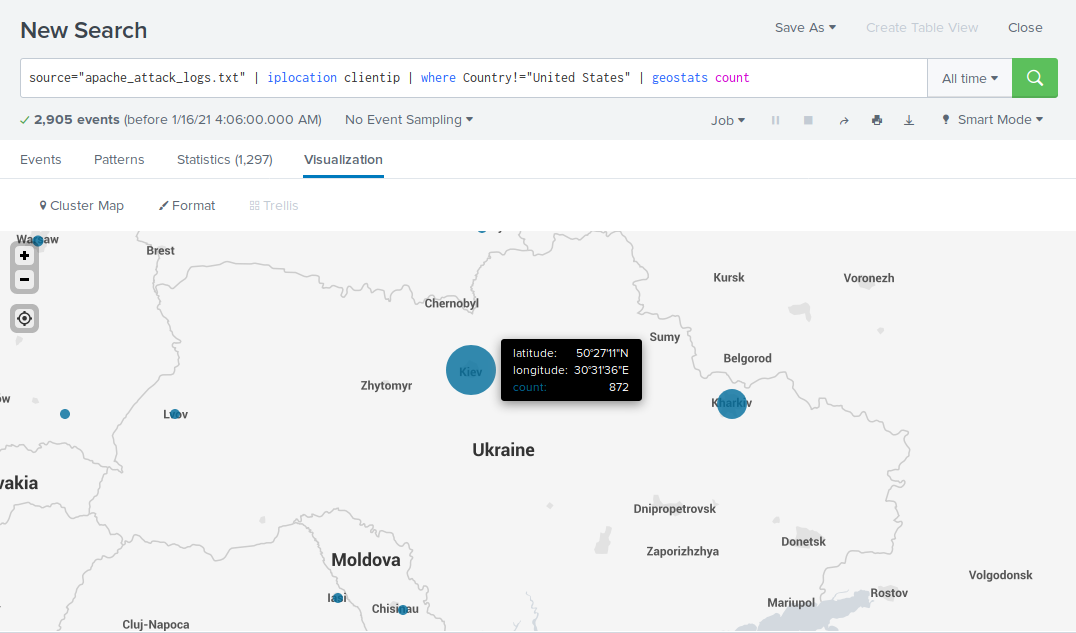
#### 

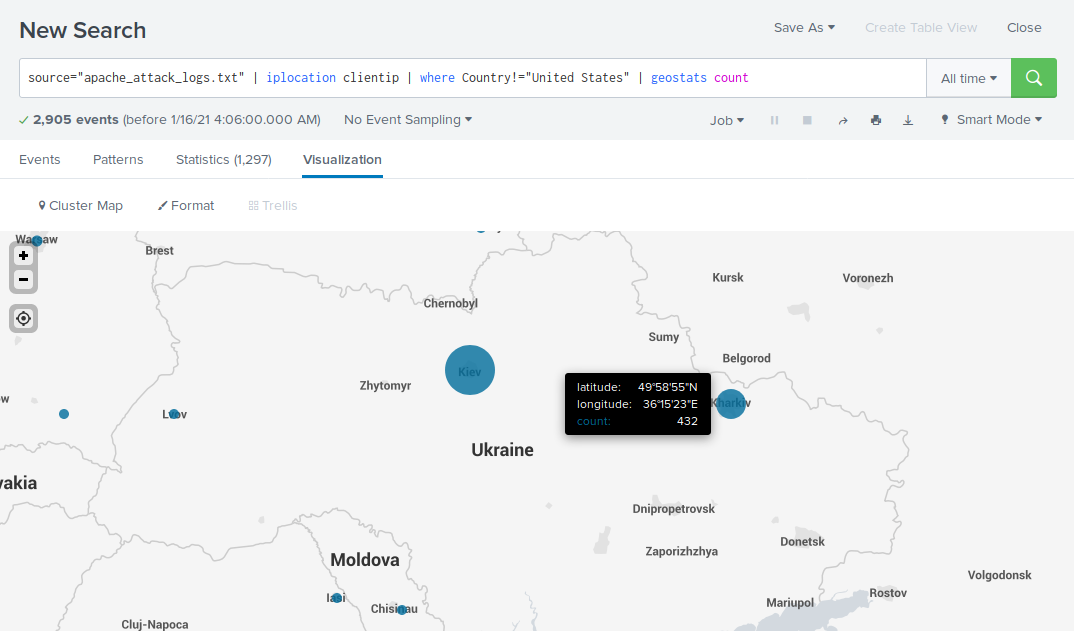
#### **Dashboard Analysis for Cluster Map**

Analyze your new cluster map results and answer the following questions:





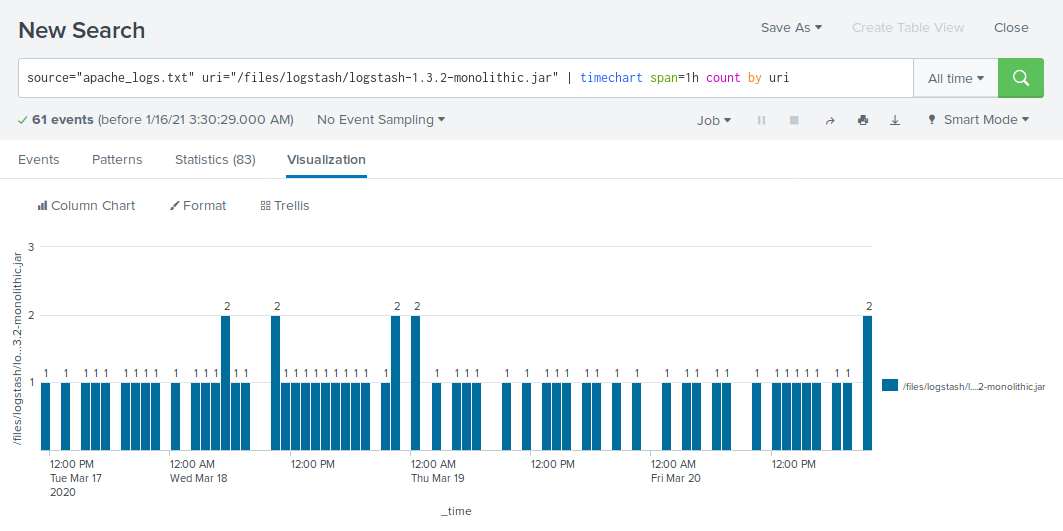


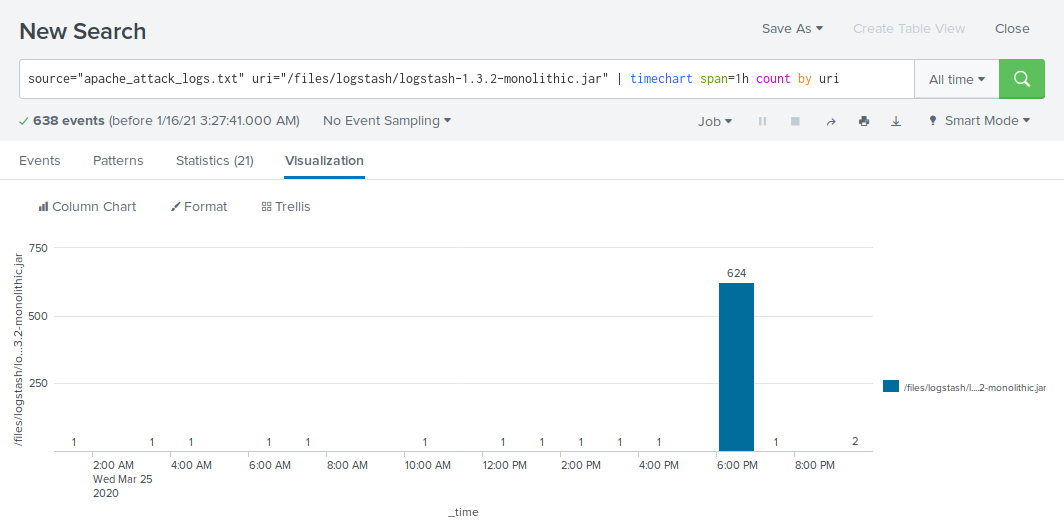


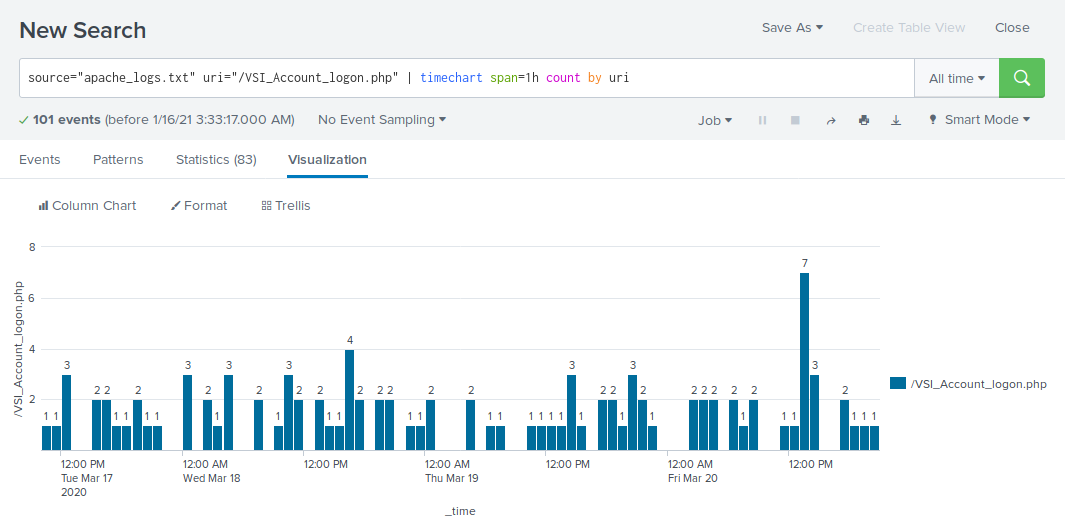
* Does anything stand out as suspicious?
* There was suspicious activity in the country of Ukraine, specifically in the cities of Kiev and Kharkiv.
* Which new city, country on the map has a high volume of activity?  
  + **Hint:** Zoom in on the map.
* The city of Kiev, Ukraine had a high volume of activity.
* The city of Kharkiv, Ukraine had a high volume of activity.
* What is the count of that city?
* Kiev: Count of 872.
* Kharkiv: Count of 432.

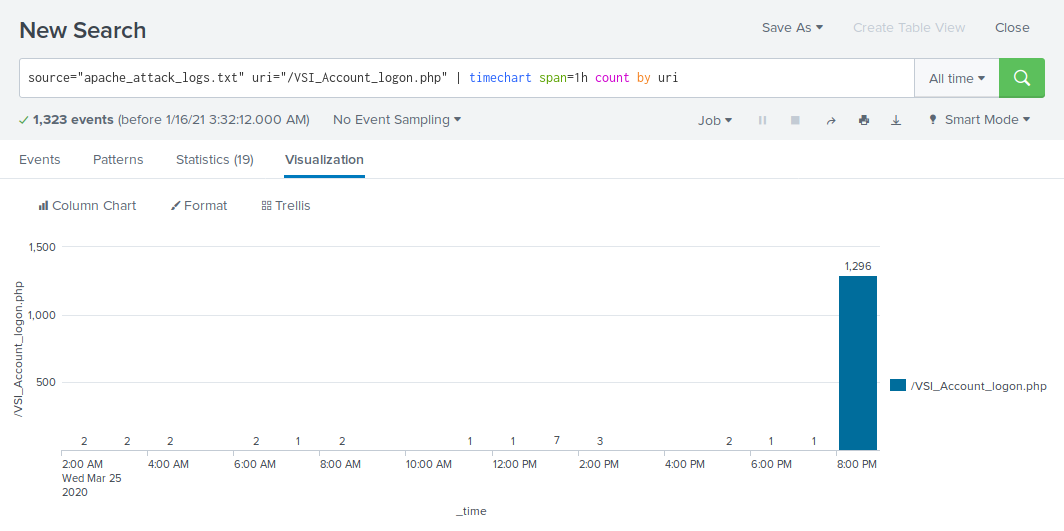
#### **Dashboard Analysis for URI Data**

Analyze your dashboard panel of the URI data and answer the following questions:









* Does anything stand out as suspicious?
* There was suspicious activity with the URI “/files/logstash/logstash-1.3.2-monolithic.jar” from 6:00 p.m. to 7:00 p.m. on Wednesday, March 25th and with the URI “/VSI\_Account\_logon.php” from 8:00 p.m. to 9:00 p.m. on Wednesday, March 25th.
* What URI is hit the most?
* The URI “/VSI\_Account\_logon.php” was hit the most with 1,415 events.
* Based on the URI being accessed, what could the attacker potentially be doing?
* Based on the URI “VSI\_Logon.php” being accessed, the attacker may be trying to brute force the VSI logon page.