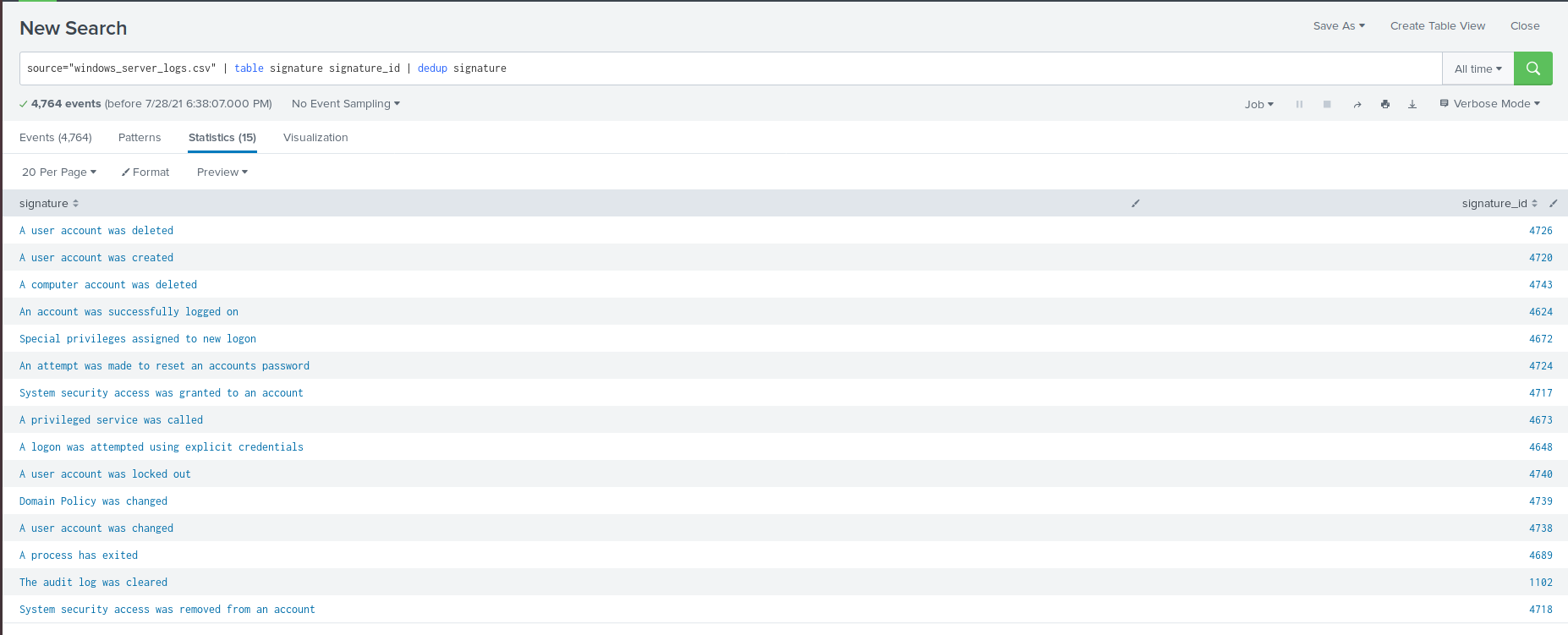
## **Solution Guide: Part 1 - Master of the SOC**

### **Windows Server Logs**

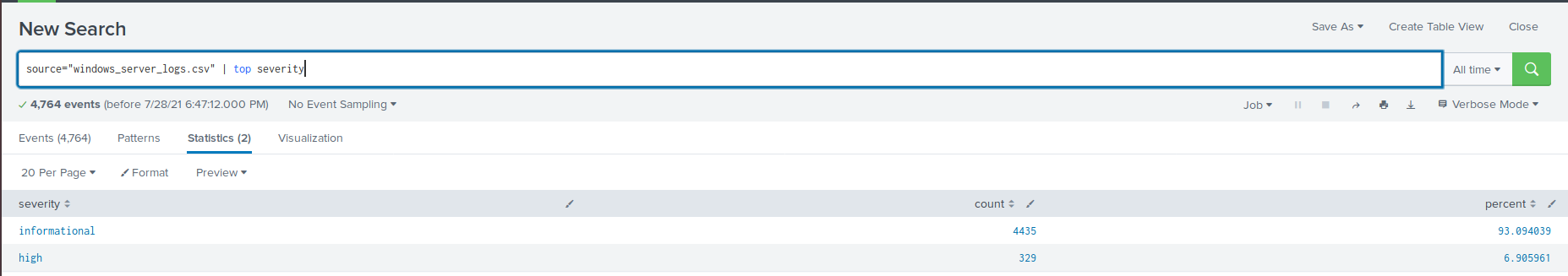
Reports: Design the following reports to assist VSI with quickly identifying specific information.

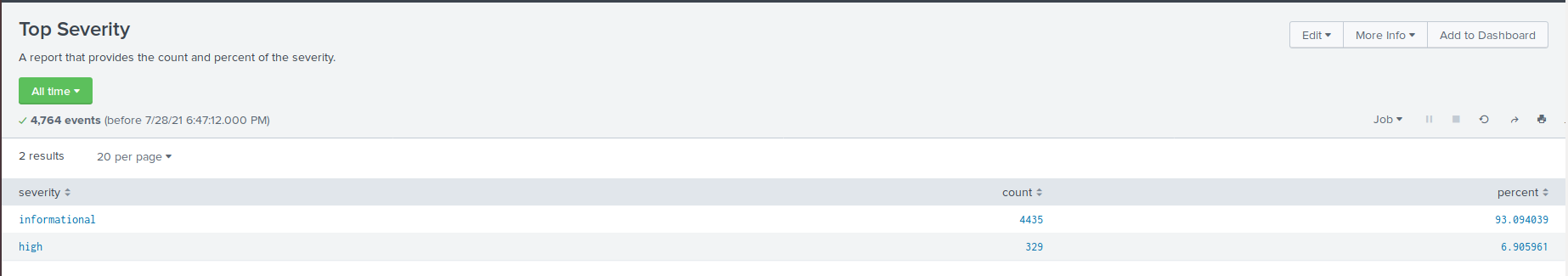
1. A report with a table of signatures with associated SignatureID.
   * **source="windows\_server\_logs.csv" | table signature signature\_id | dedup signature**



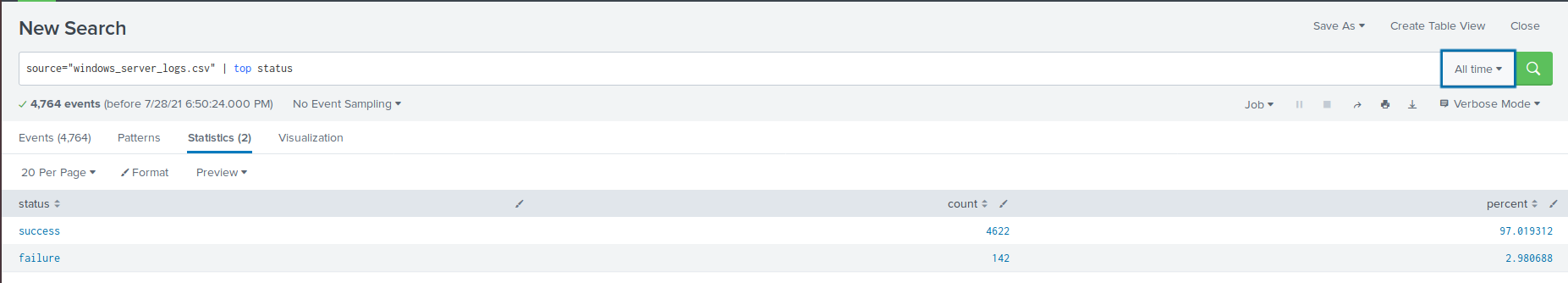


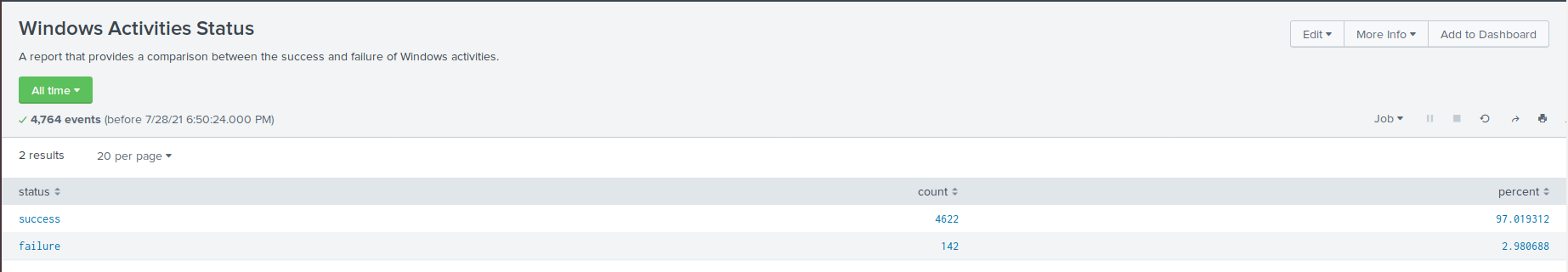
1. A report that provides the count and percent of the severity.
   * **source="windows\_server\_logs.csv" | top severity**





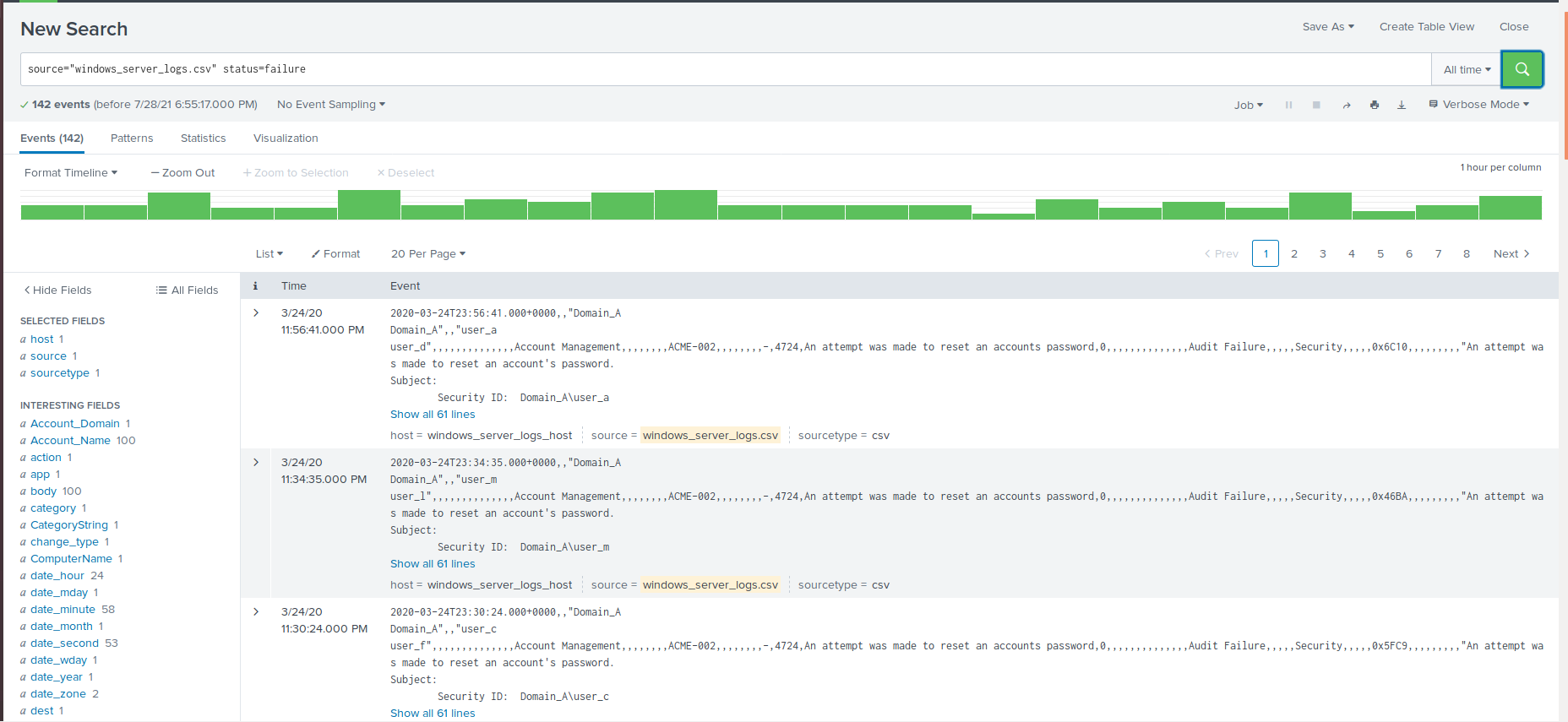
1. A report that provides a comparison between the success and failure of Windows activities.
   * **source="windows\_server\_logs.csv" | top status**



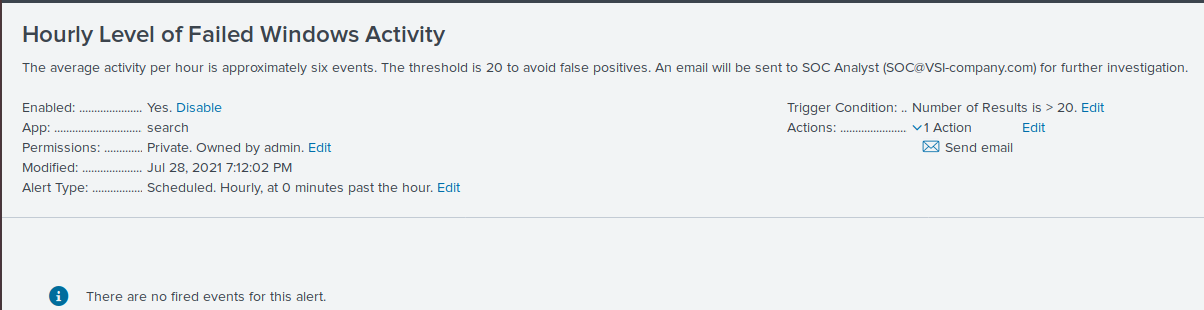


Alerts: Design the following alerts to notify VSI of suspicious activity.

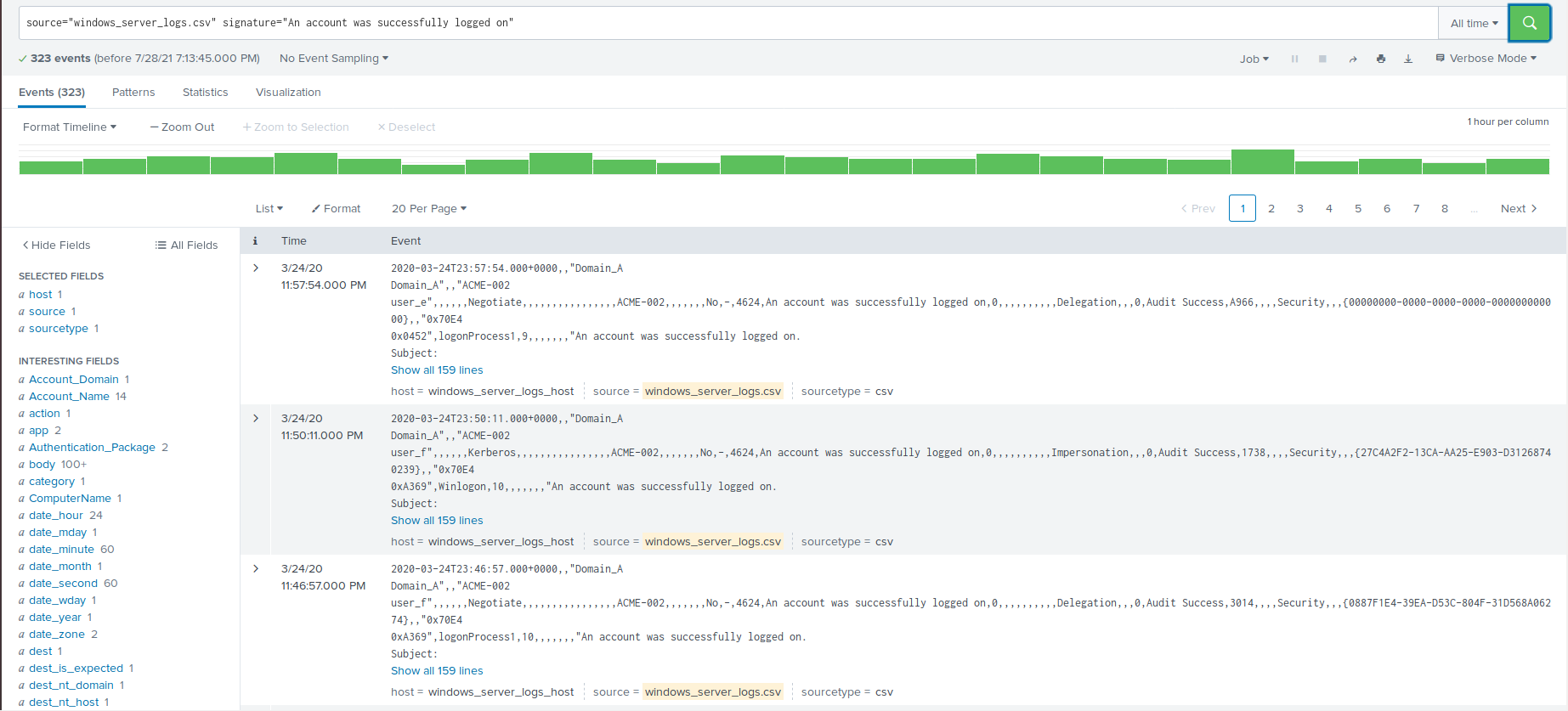
1. Determine an appropriate baseline and threshold for hourly level of failed Windows activity. Create an alert to trigger when the threshold has been reached. The alert should trigger an email to SOC@VSI-company.com.
   * **source="windows\_server\_logs.csv" status=failure**



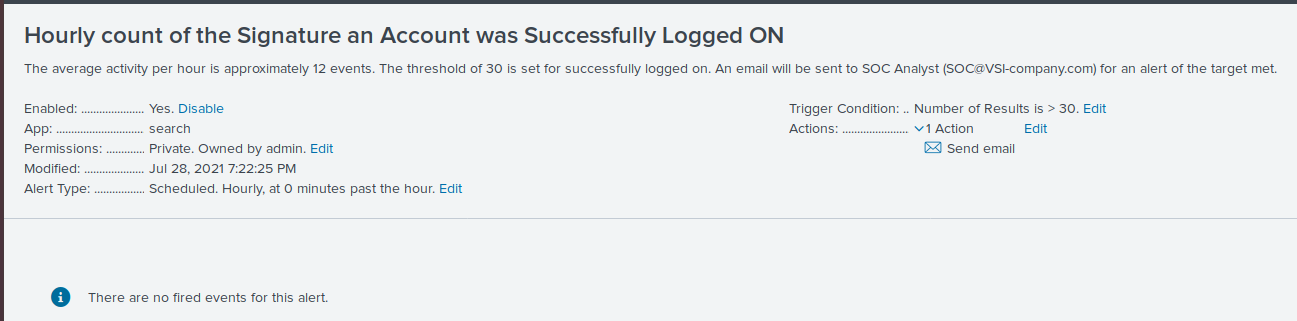
* + The average activity per hour is approximately six events. The threshold is up to each group, but should be in the range of 15-25 to avoid false positives.
  + To create alert, change the search to one hour
  + Set to run every hour.
    - Set alert to trigger when count is greater than chosen threshold.
    - Add action Send email to [SOC@VSI-company.com](mailto:SOC@VSI-company.com).



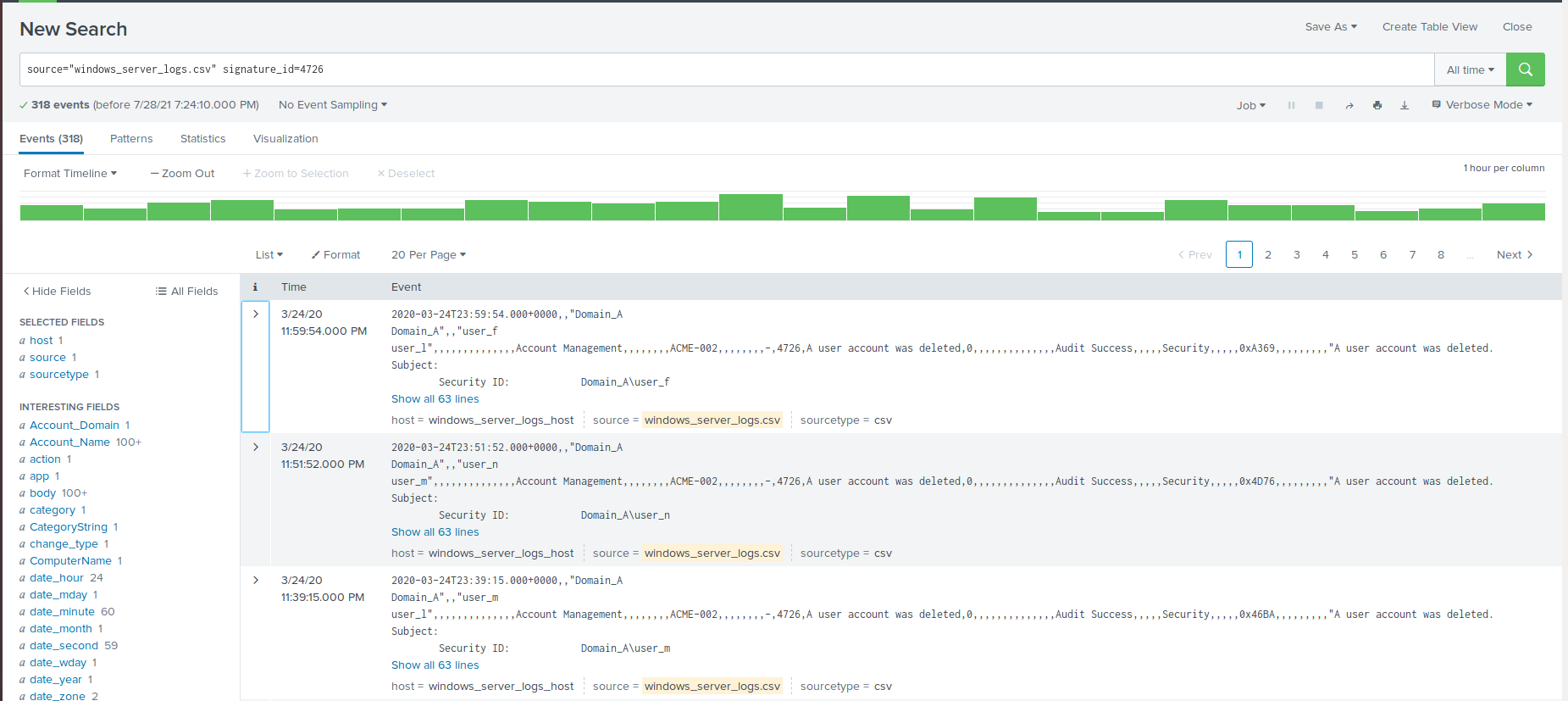
1. Determine a baseline and threshold for hourly count of the signature an account was successfully logged on. Create an alert to trigger when the threshold has been reached. The alert should trigger an email to SOC@VSI-company.com.
   * **source="windows\_server\_logs.csv" signature="An account was successfully logged on"**



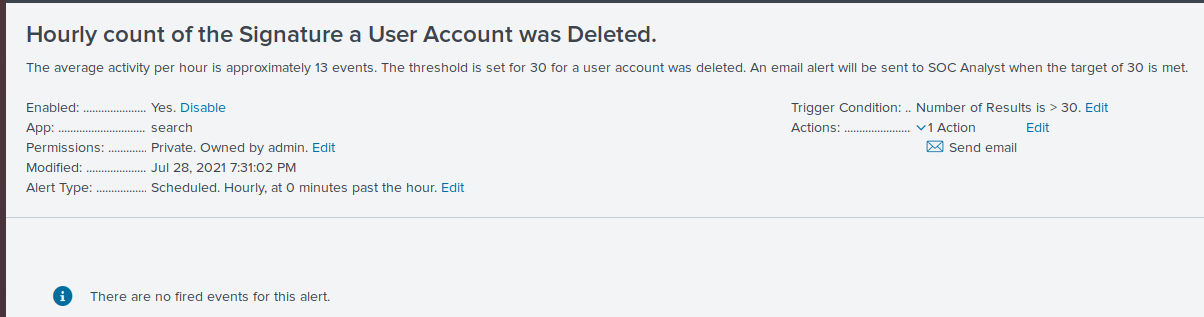
* + The average activity per hour is approximately 12 events. The threshold is up to each group, but should be in the range of 30-50.
  + To create alert, change the search to one hour and click Save As > Alert.
  + Set to run every hour.
  + Set alert to trigger when count is greater than chosen threshold.
  + Add action Send email to [SOC@VSI-company.com](mailto:SOC@VSI-company.com).



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. Create an alert to trigger when the threshold has been reached. The alert should trigger an email to SOC@VSI-company.com.
   * **source="windows\_server\_logs.csv" signature\_id=4726**

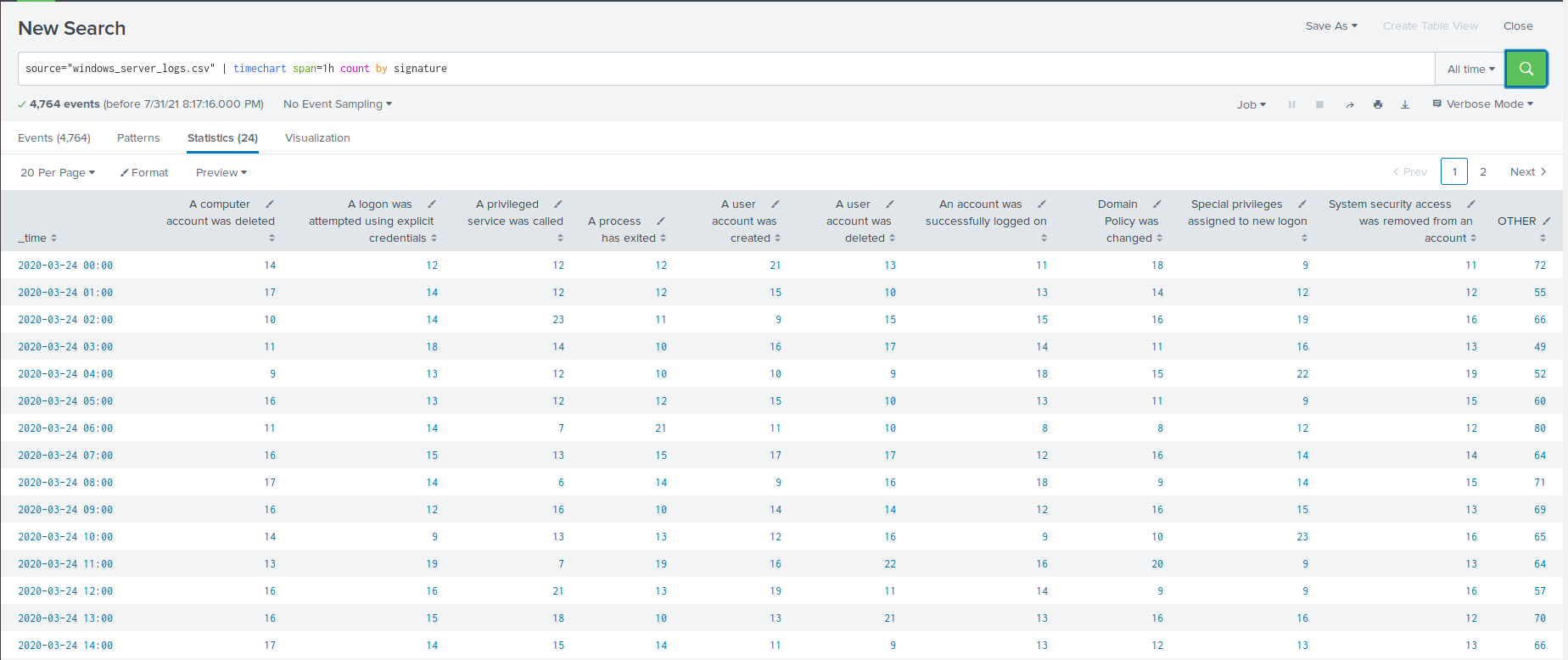


* + The average activity per hour is approximately 13 events.
  + The threshold range should be between 30-50.
  + To create alert, change the search to one hour and click Save As > Alert.
  + Set to run every hour.
  + Set alert to trigger when count is greater than chosen threshold.
  + Add action Send email to [SOC@VSI-company.com](mailto:SOC@VSI-company.com).

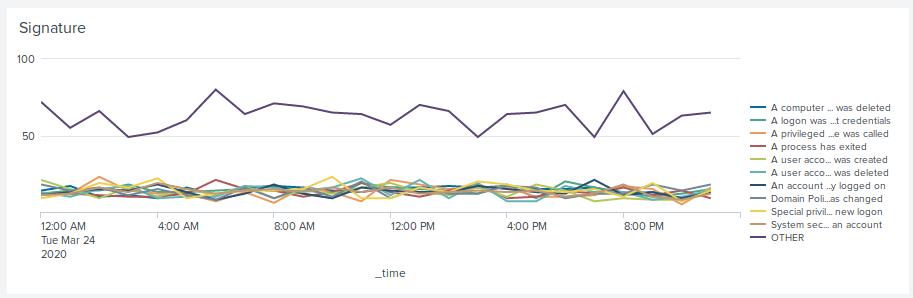


Visualizations and Dashboards: Design the following visualizations and add them to a dashboard called Windows Server Monitoring:

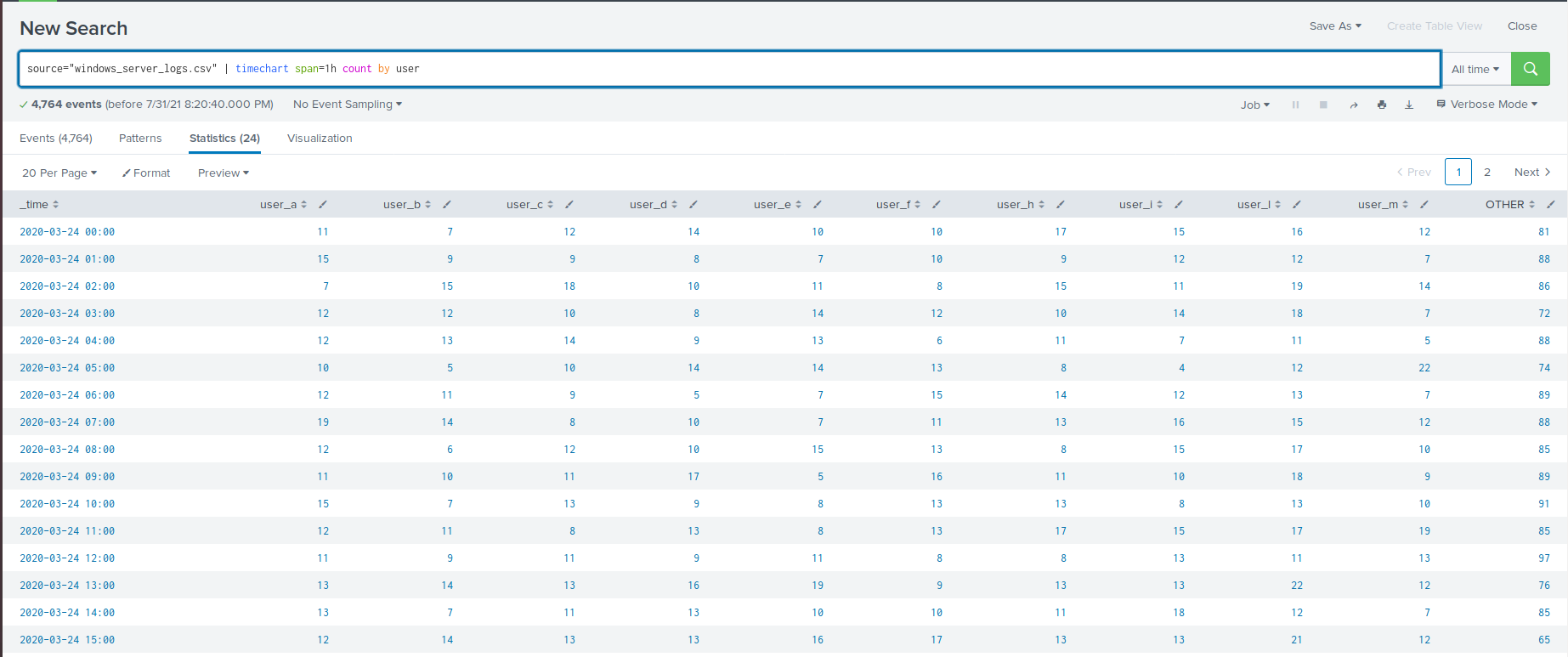
1. A line chart that displays the different signature field values over time.
   * **source="windows\_server\_logs.csv" | timechart span=1h count by signature**



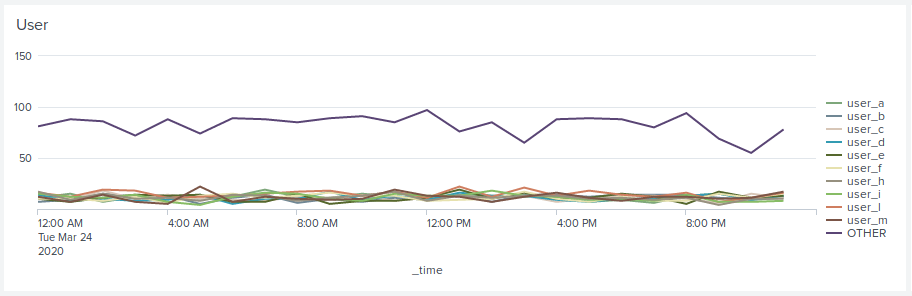
* + Select Visualizations > Line Chart.



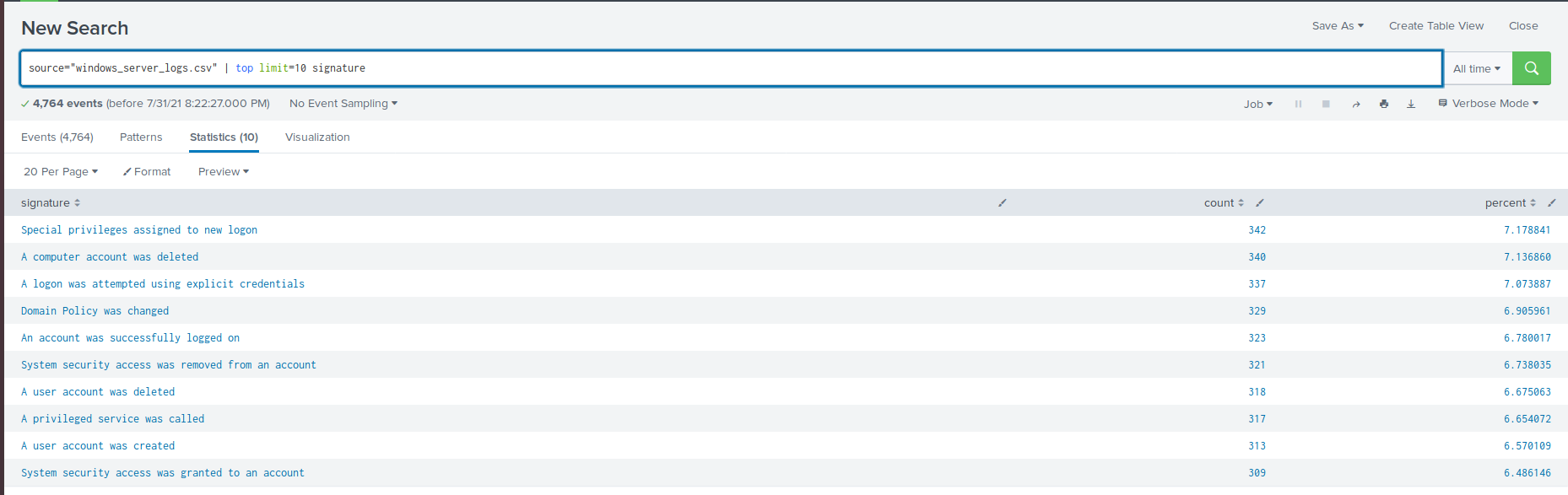
1. A line chart that displays the different user field values over time.
   * **source="windows\_server\_logs.csv" | timechart span=1h count by user**



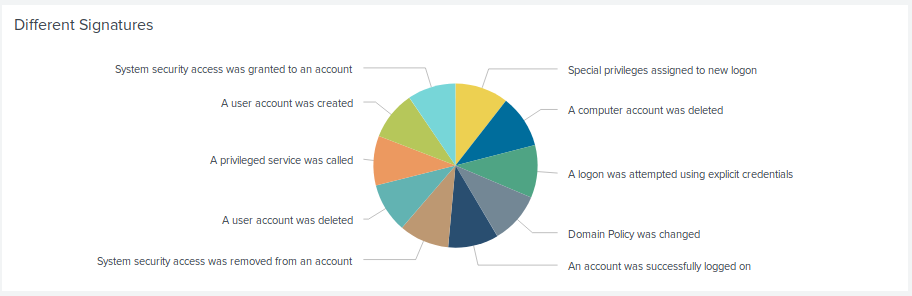
* + Select Visualizations > Line Chart.



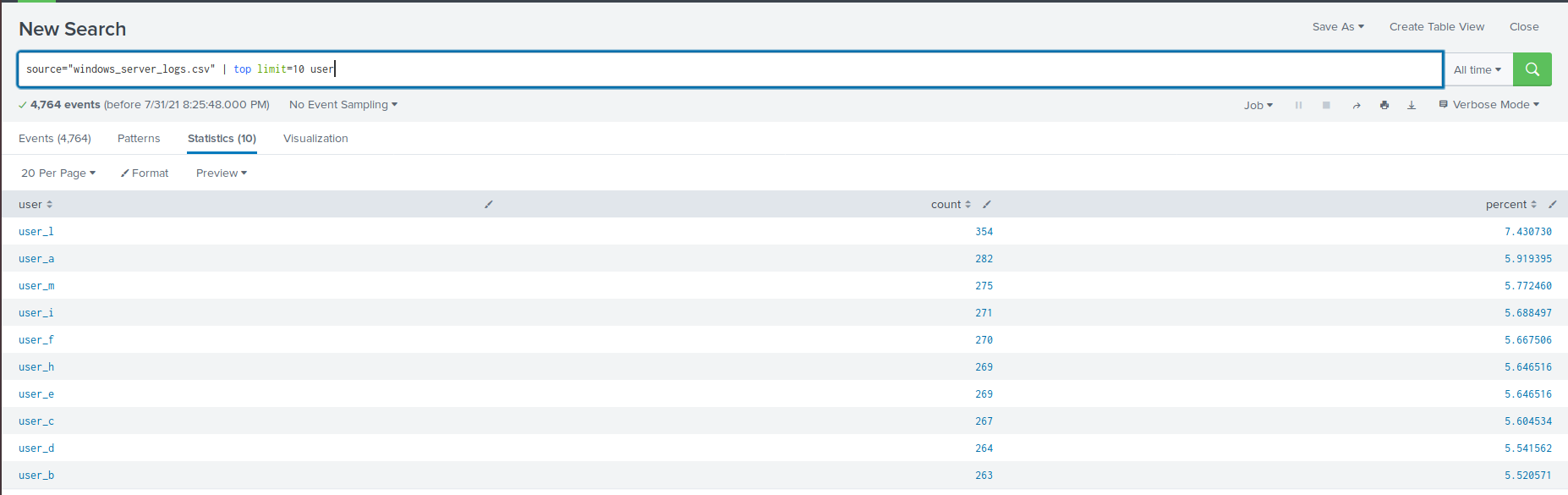
1. A bar, column, or pie chart that illustrates the count of different signatures.
   * **source="windows\_server\_logs.csv" | top limit=10 signature**



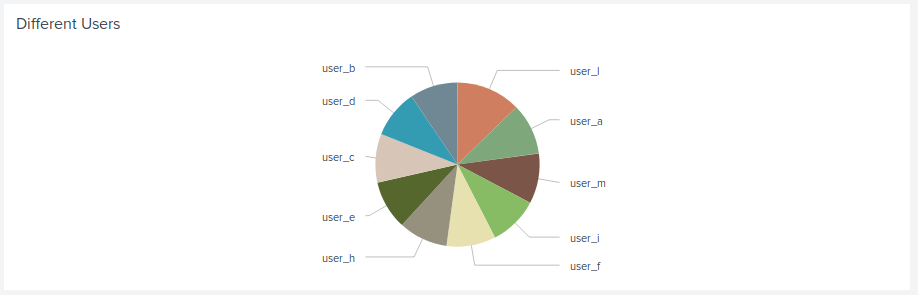
* + Select Visualizations > Bar/Column/Pie Chart.



1. A bar, column, or pie chart that illustrates the count of different users.
   * **source="windows\_server\_logs.csv" | top limit=10 user**



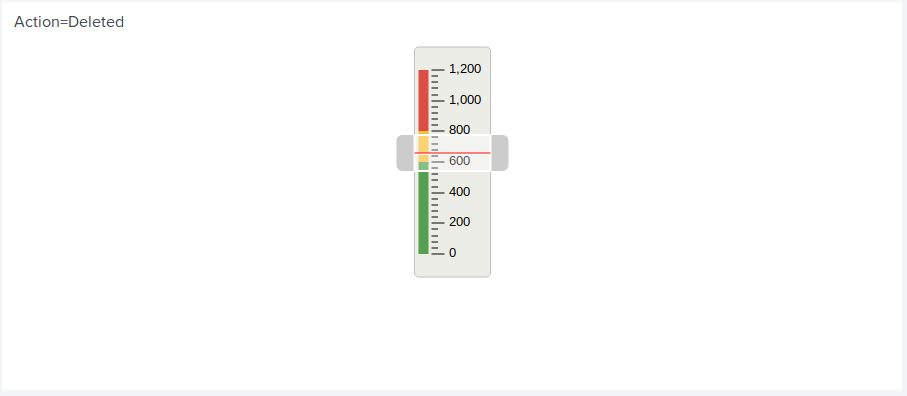
* + Select Visualizations > Bar/Column/Pie Chart.

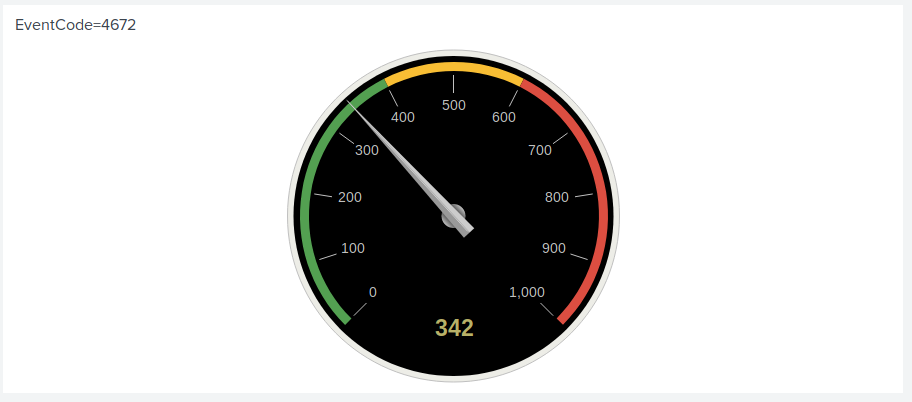


1. A statistical chart that illustrates the count of different users.
   * **source="windows\_server\_logs.csv" | top limit=10 user**

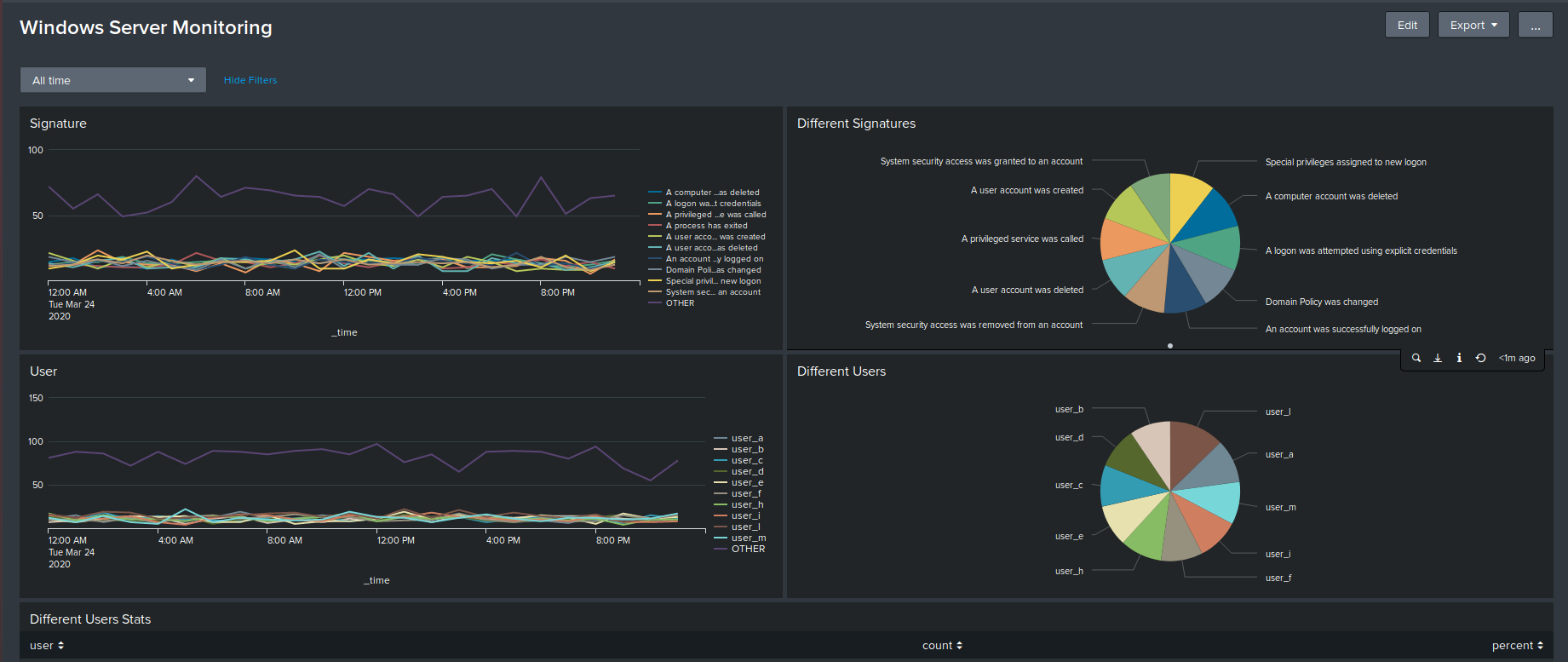


1. One single value visualization of your choice: radial gauge, marker gauge, etc.
   * Answers will vary.





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

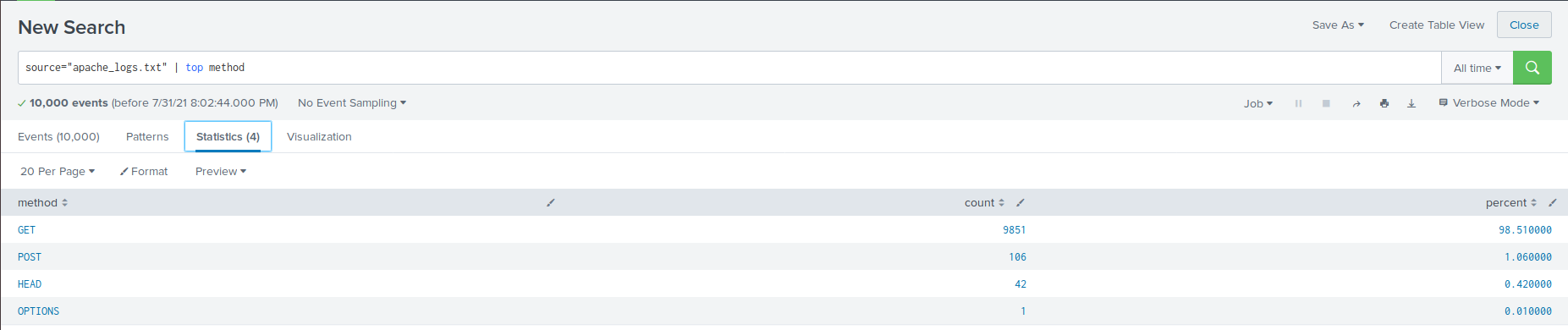


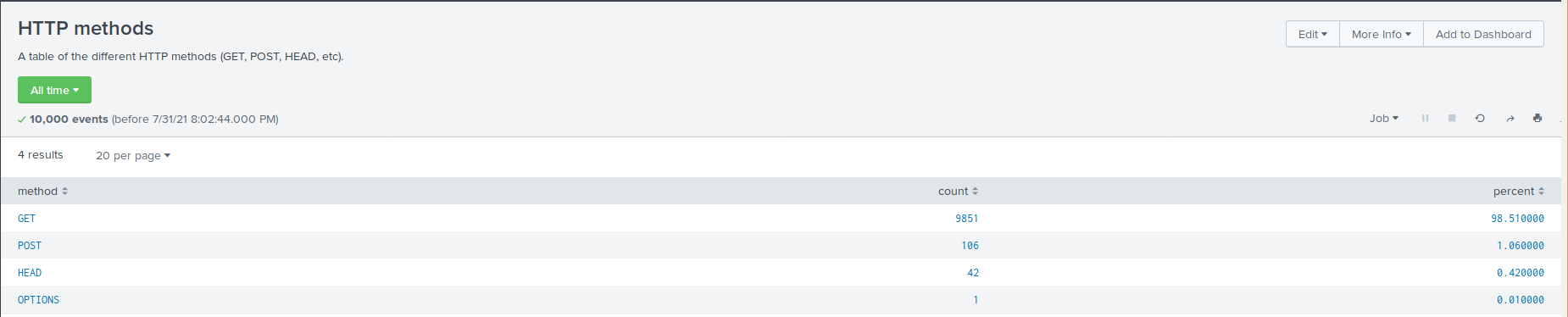
### 

### **Apache Web Server Logs**

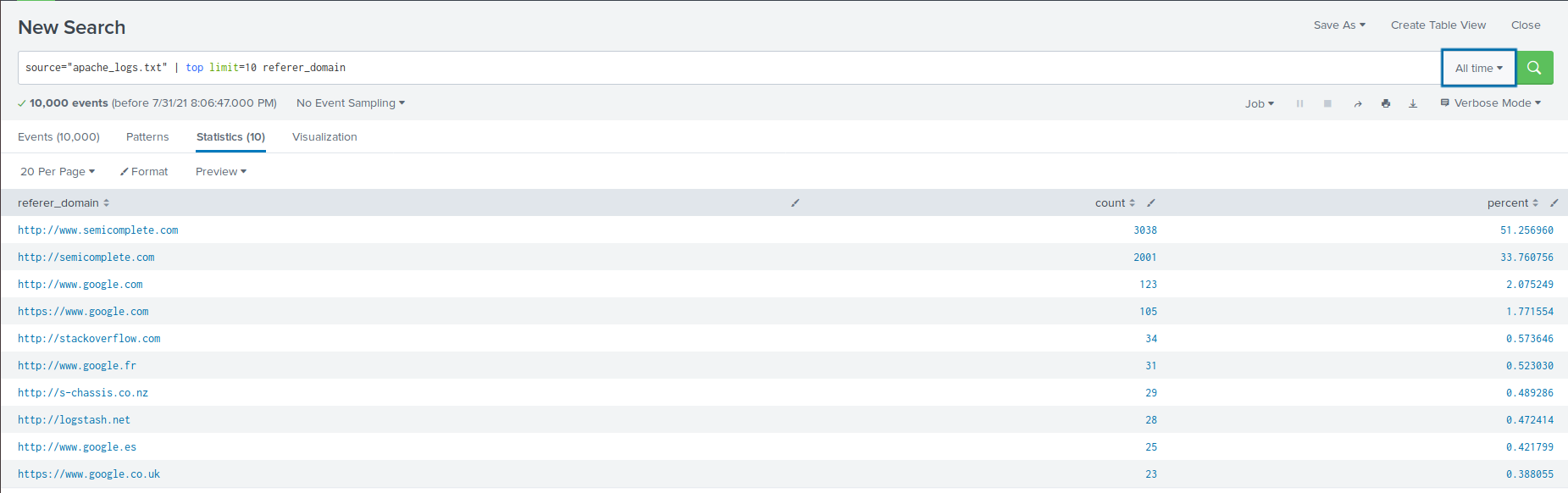
Reports: Design the following reports to assist VSI with quickly identifying specific information.

1. A report that shows a table of the different HTTP methods (GET, POST, HEAD, etc).
   * **source="apache\_logs.txt" | top method**



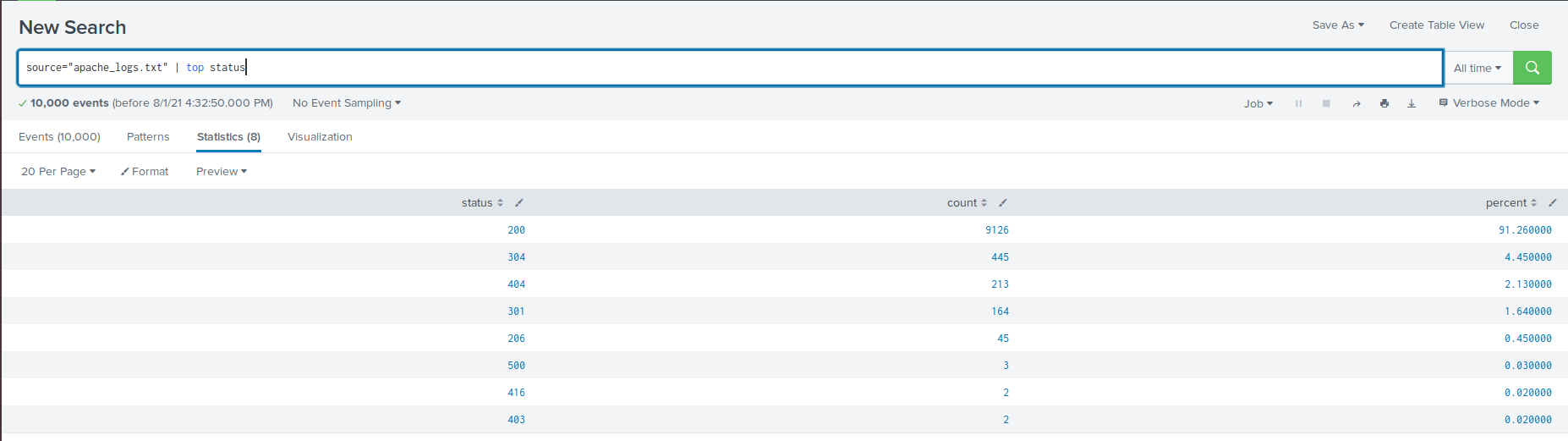


* + A report that shows the top 10 domains that referred to VSI's website.
  + **source="apache\_logs.txt" | top limit=10 referer\_domain**





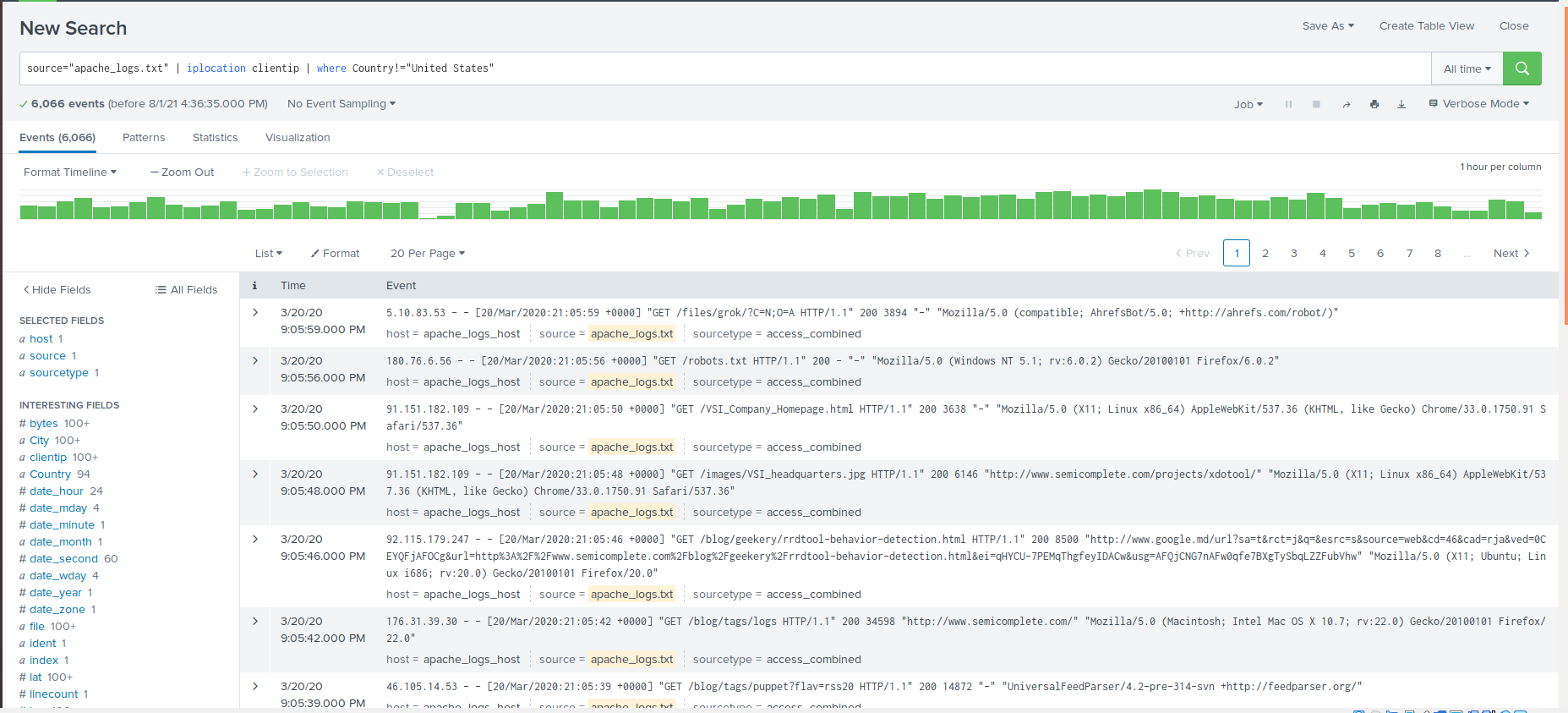
1. A report that shows the count of the HTTP response codes.
   * **source="apache\_logs.txt" | top status**



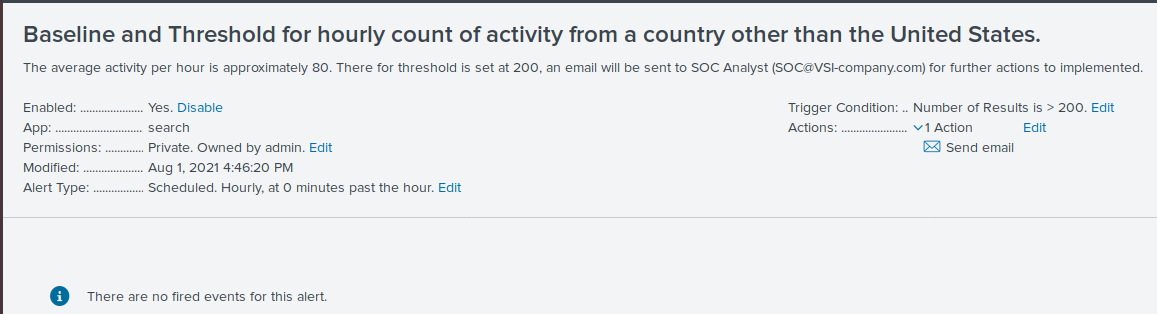


Alerts: Design the following alerts:

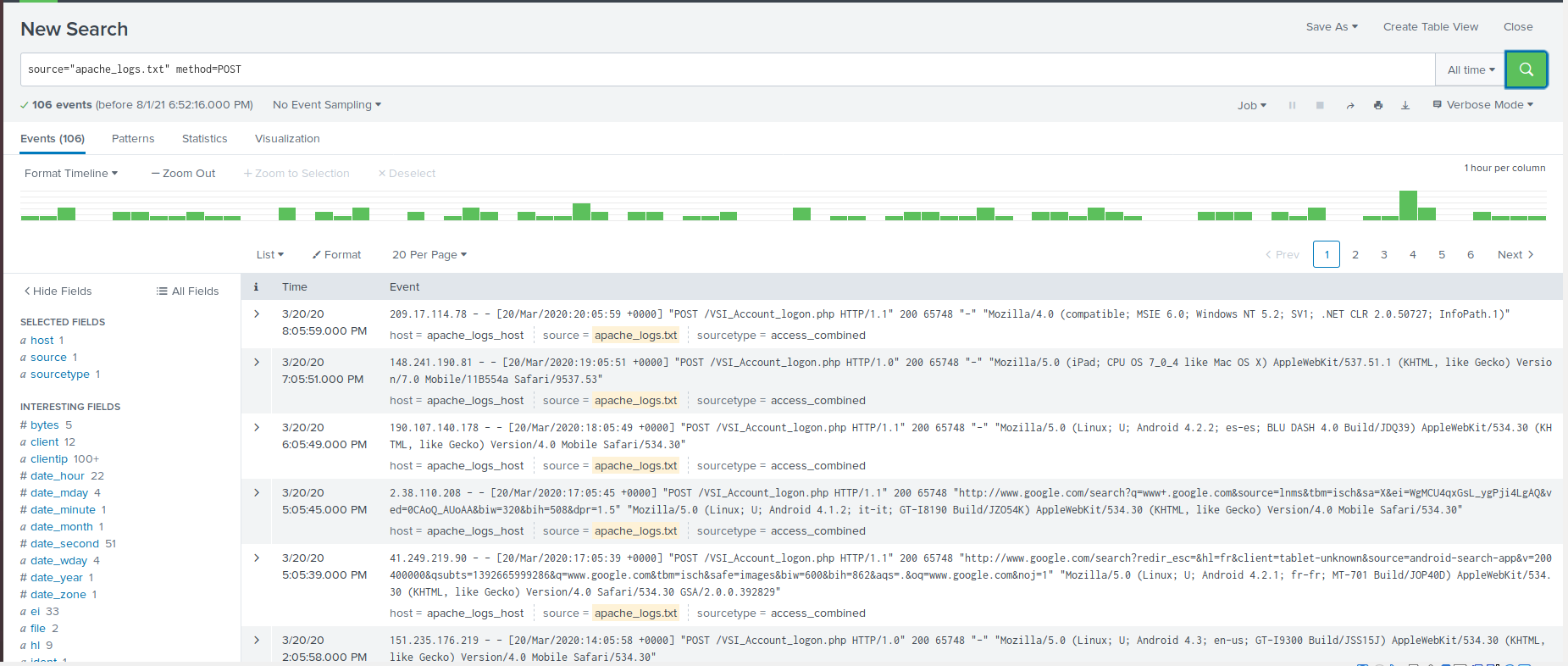
1. Determine a baseline and threshold for hourly count of activity from a country other than the United States. Create an alert to trigger when the threshold has been reached. The alert should trigger an email to SOC@VSI-company.com.
   * **source="apache\_logs.txt" | iplocation clientip | where Country!="United States"**



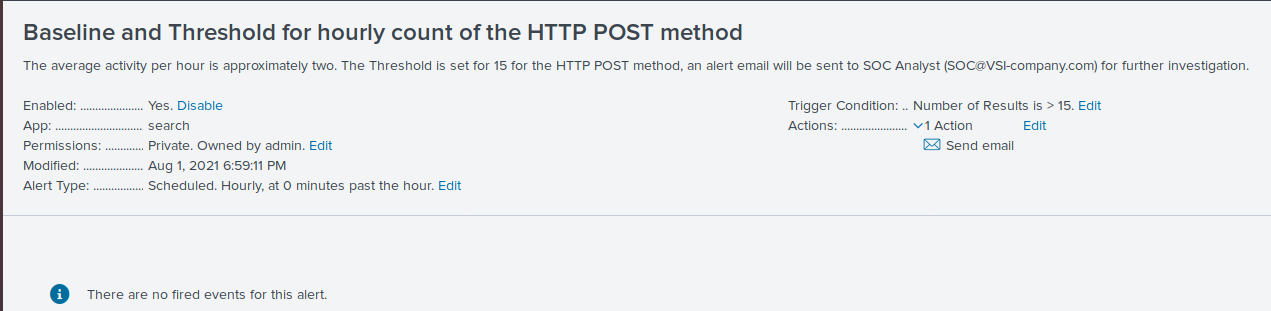
* + The average activity per hour is approximately 80.
  + The threshold should range between 170-250.
  + To create an alert, change the search to one hour.
  + Set to run every hour.
  + Set alert to trigger when count is greater than chosen threshold.
  + Add action Send email to [SOC@VSI-company.com](mailto:SOC@VSI-company.com).



1. Determine a 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.
   * **source="apache\_logs.txt" method=POST**



* + The average activity per hour is approximately two.
  + The threshold should between 12-20.
  + To create an alert, change the search to one hour.
  + Set to run every hour.
  + Set alert to trigger when count is greater than chosen threshold.
  + Add action Send email to [SOC@VSI-company.com](mailto:SOC@VSI-company.com).

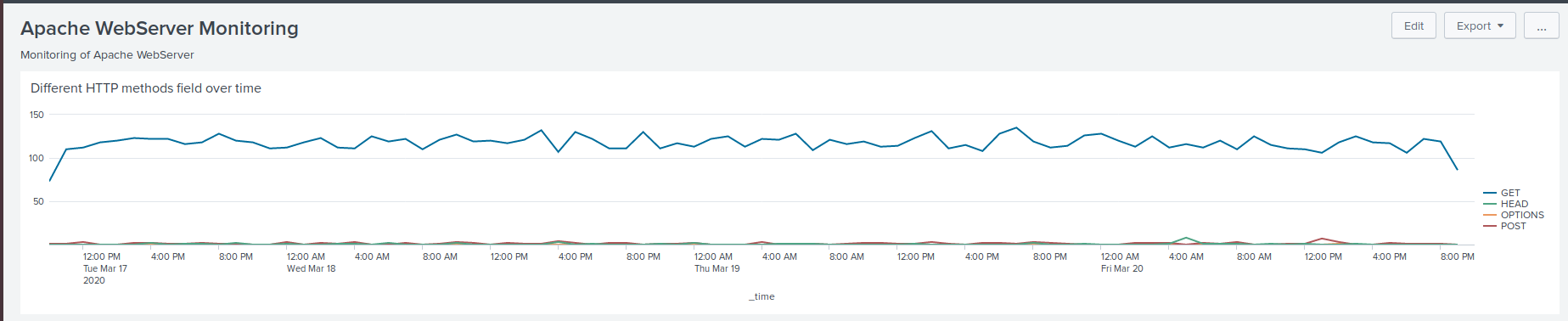


Visualizations and Dashboards: Design the following visualization and add them to a dashboard called Apache WebServer Monitoring.

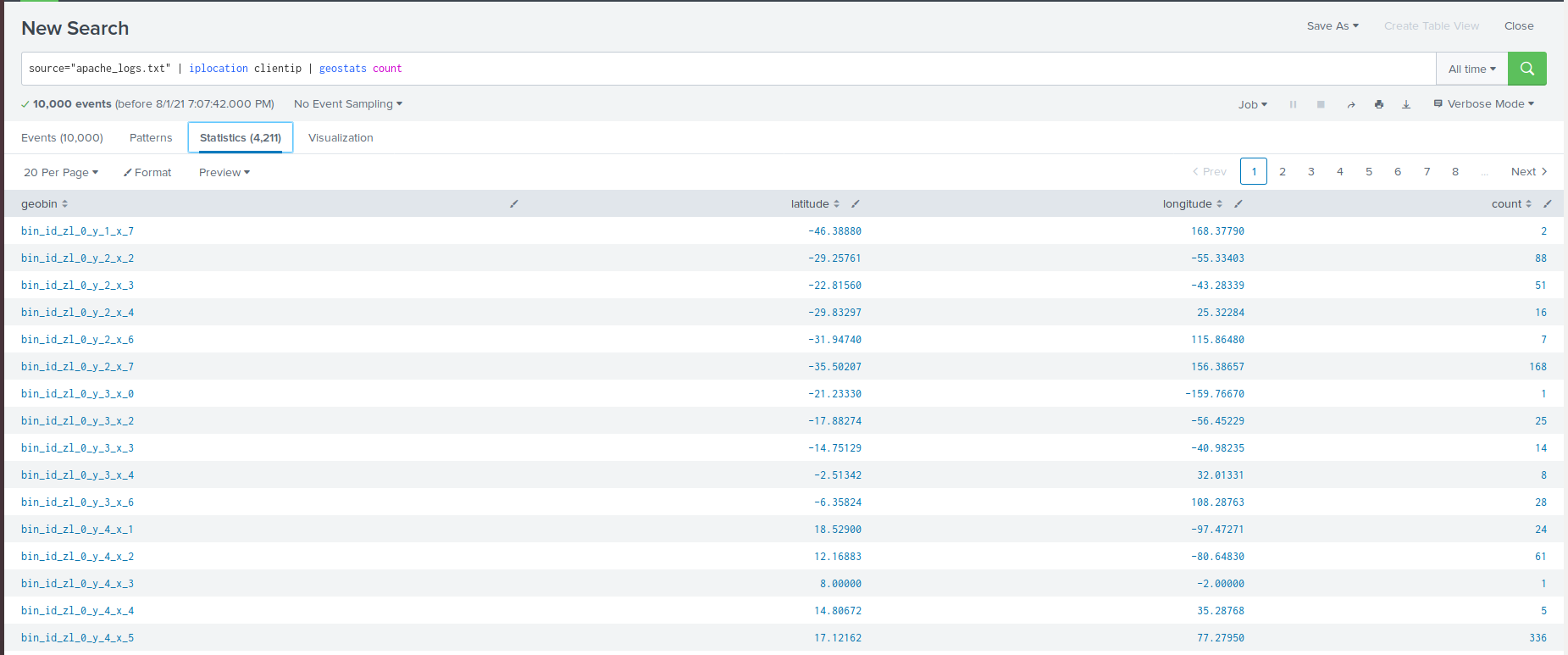
1. A line chart that displays the different HTTP methods field over time.
   * **source="apache\_logs.txt" | timechart span=1h count by method**



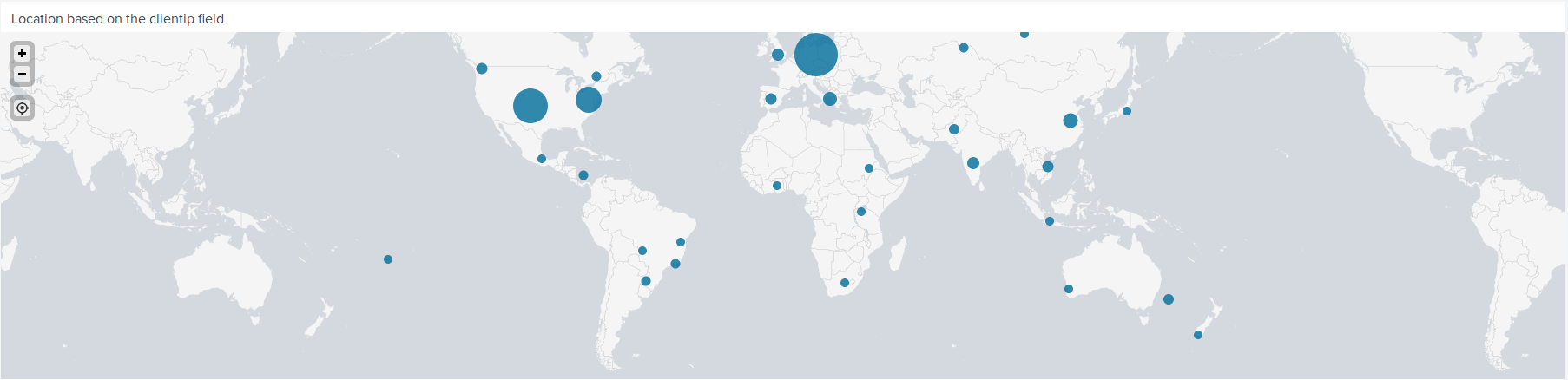
* + Select Visualizations > Line Chart.



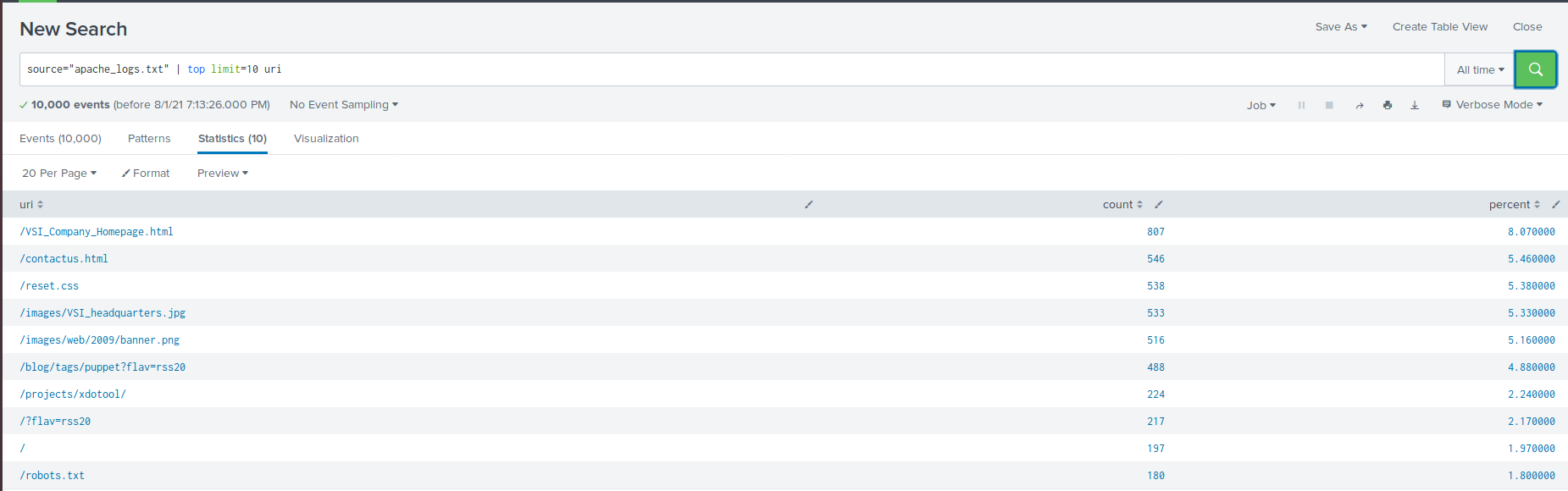
1. A geographical map showing the location based on the clientip field.
   * **source="apache\_logs.txt" | iplocation clientip | geostats count**



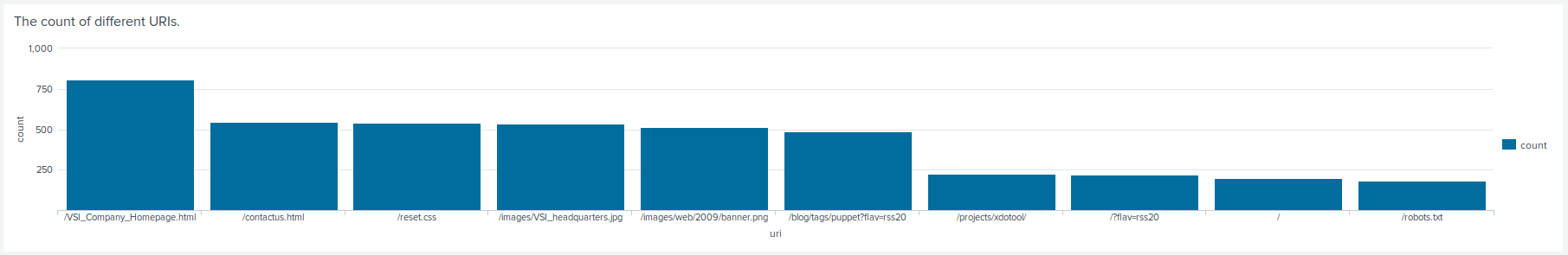
* + Select Visualizations > Line Chart.



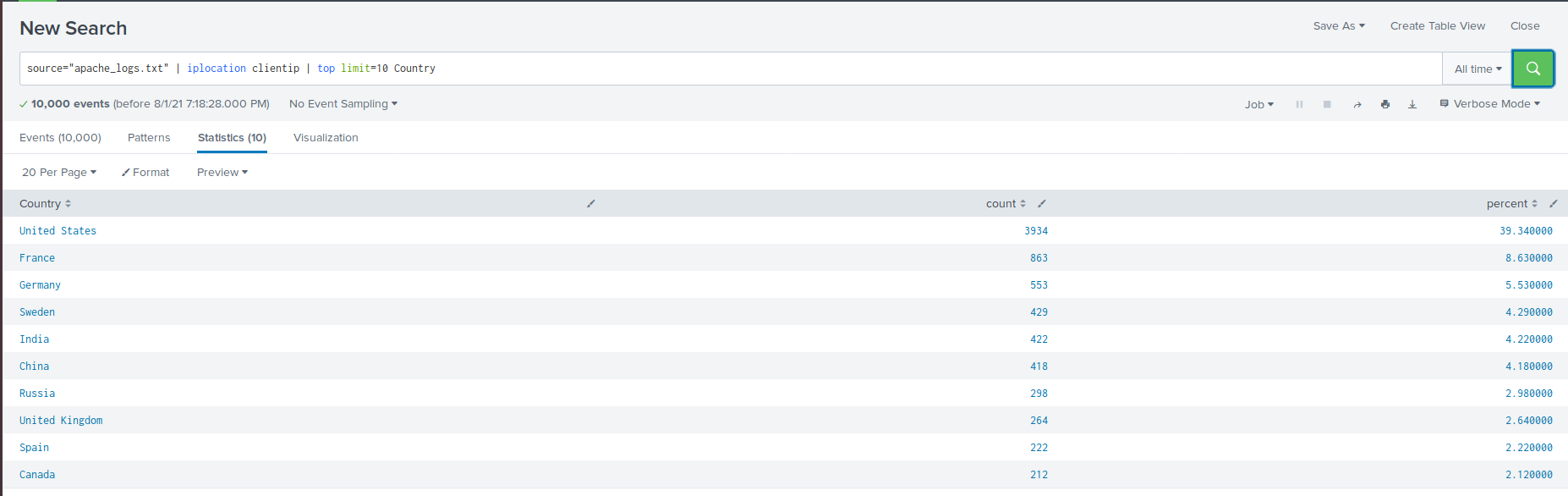
1. A bar, column, or pie chart that displays the count of different URIs.
   * **source="apache\_logs.txt" | top limit=10 uri**



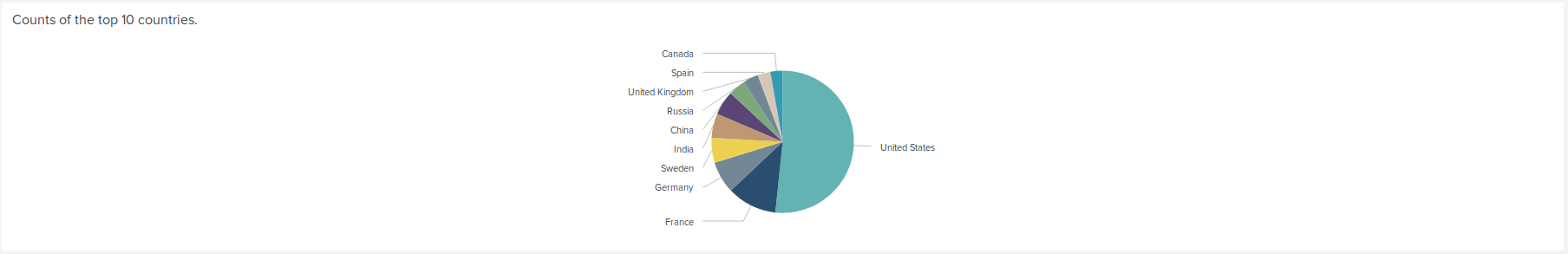
* + Select Visualizations > Bar/Column/Pie Chart.



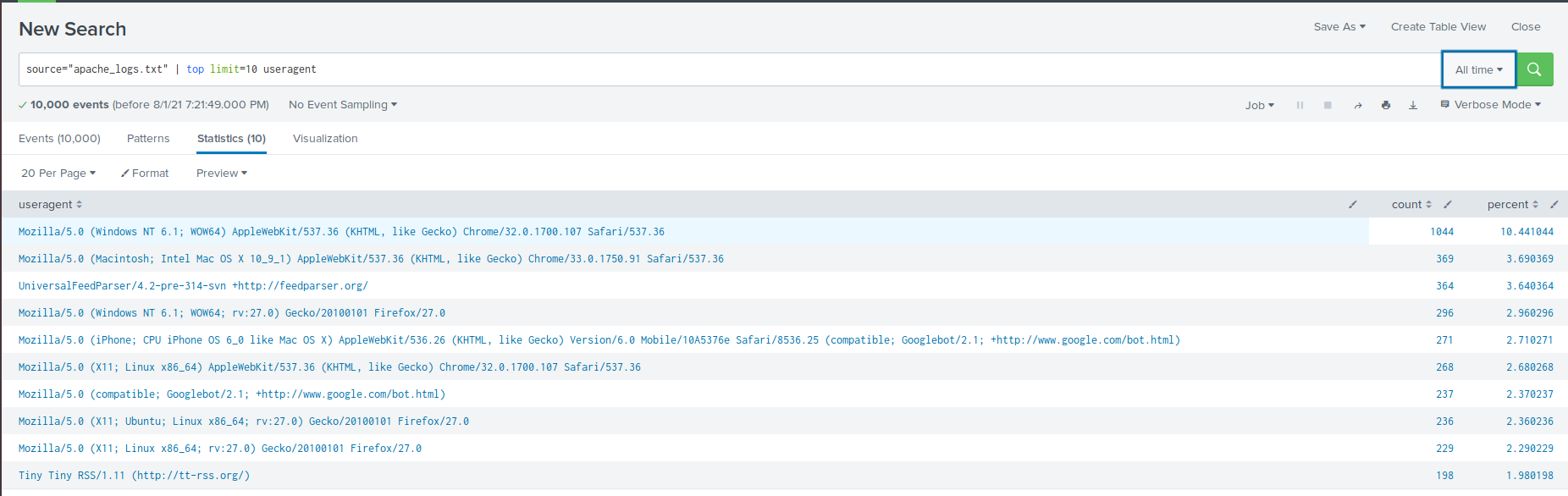
1. A bar, column, or pie chart that displays the counts of the top 10 countries.
   * **source="apache\_logs.txt" | iplocation clientip | top limit=10 Country**



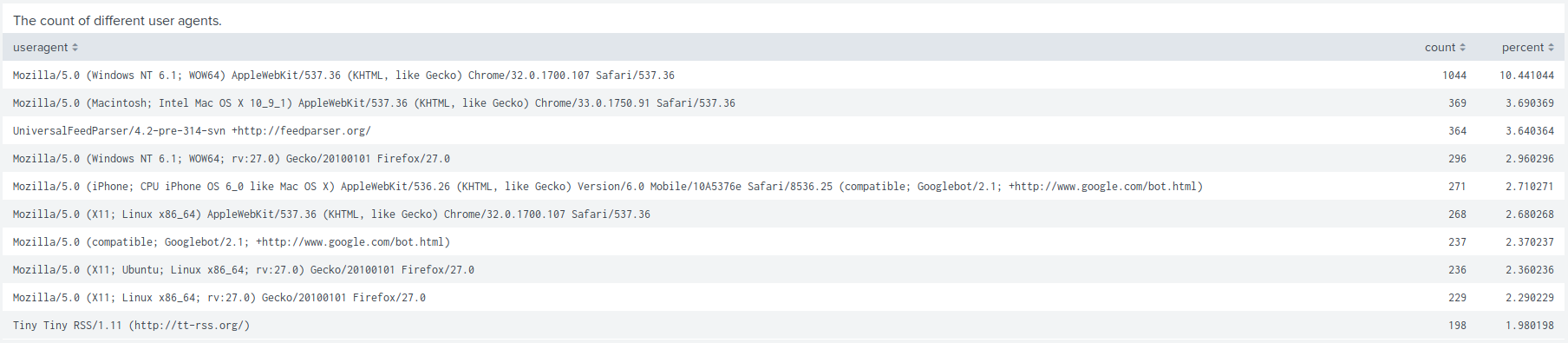
* + Select Visualizations > Bar/Column/Pie Chart.



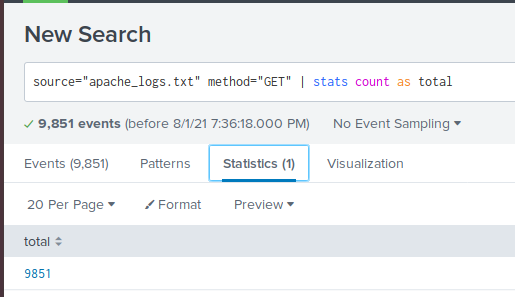
1. A statistical chart that illustrates the count of different user agents.
   * **source="apache\_logs.txt" | top limit=10 useragent**

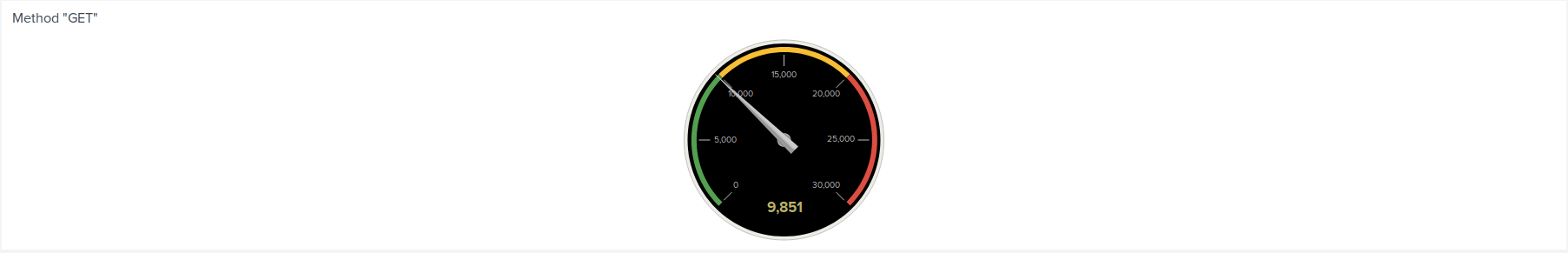


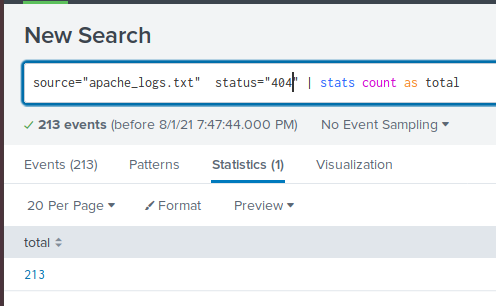
* + Click the following: Save As > Dashboard Panel > Existing > Apache WebServer Monitoring > Create Title for Panel > Save as Statistics Table

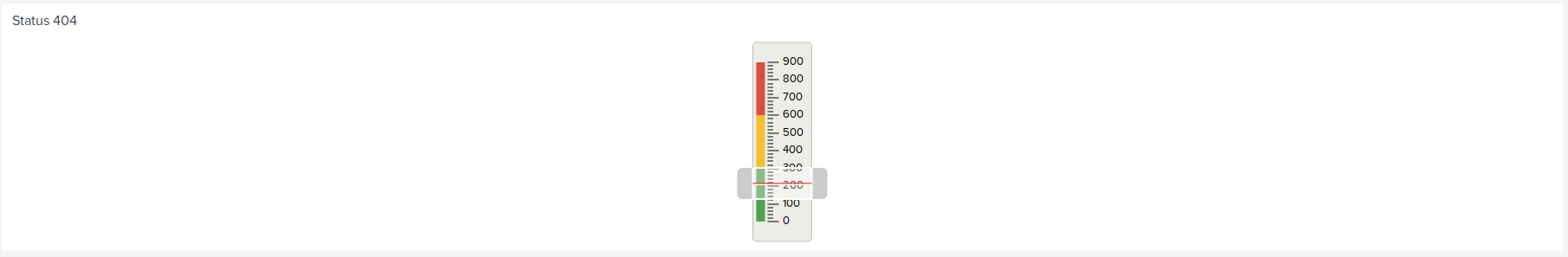


1. One single value visualization of your choice: radial gauge, marker gauge, etc.

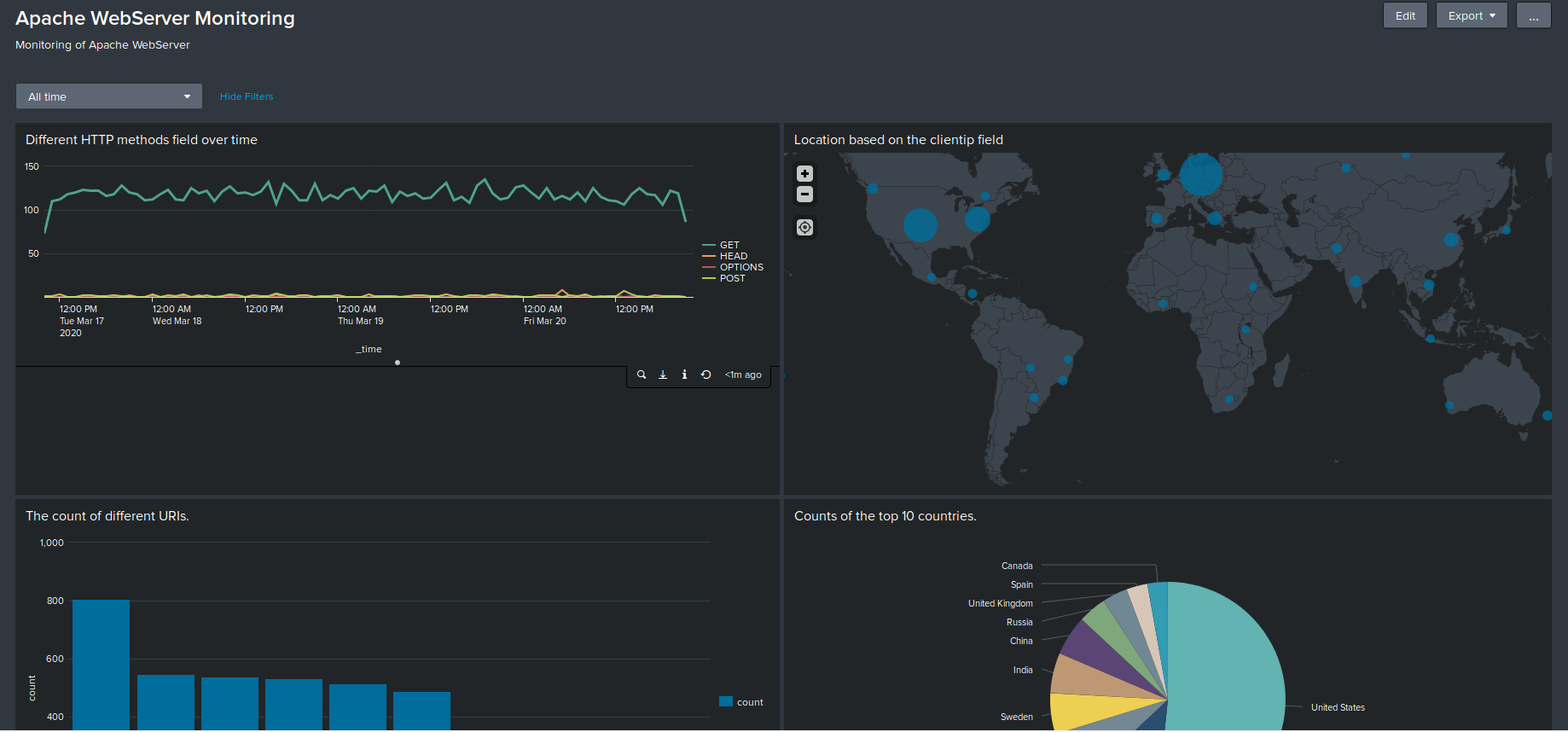








On your dashboard, add the ability to change the time range for all your visualizations.



© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.