# Splunk: Building a Secure Monitoring Solution (Part 1)

During the last several weeks of my Cybersecurity boot camp, one of our final projects was to build a secure monitoring environment for a fictitious organization called VSI (Virtual Space Industries) using Splunk Enterprise, which for those who may not know, is a SIEM (Security Information and Event Manager). SIEMs are essential tools that companies can use to detect, analyze, and respond to potential threats against their organization.

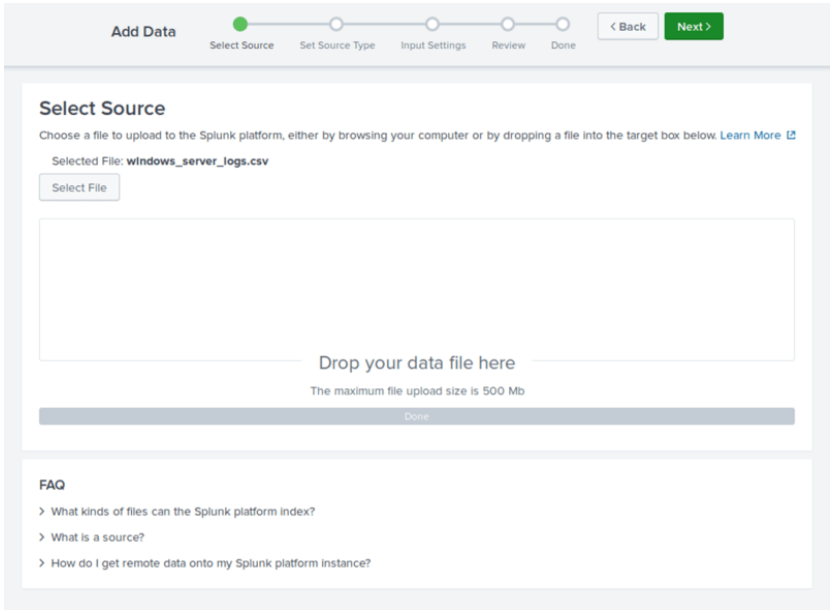
Part 1

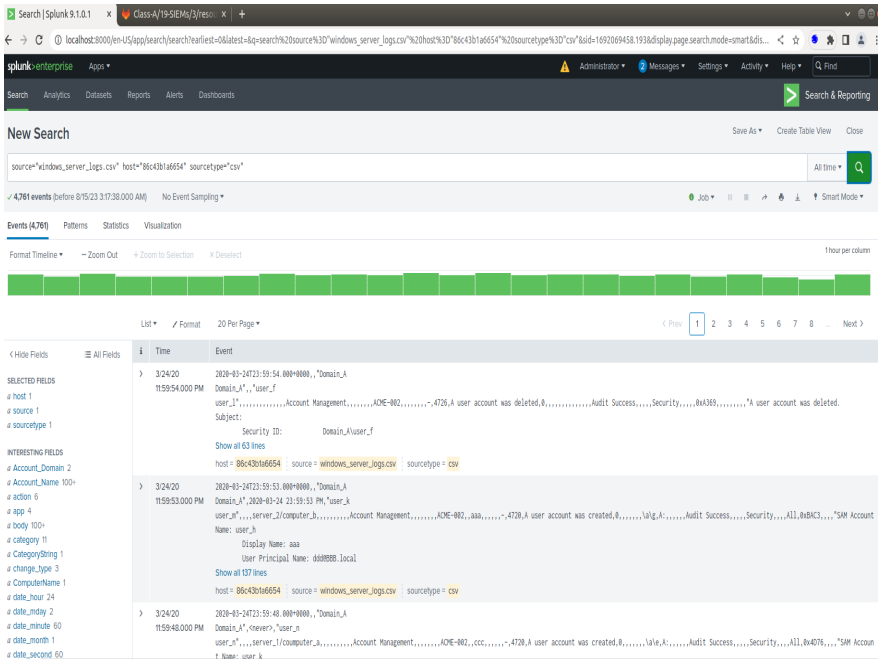
Creating Reports, Alerts, and Dashboards for Windows server log data as well as Apache webserver log data that can help point out any abnormal activity.

I started by launching Splunk, which comes pre-installed on my Ubuntu VM. I logged into the app and uploaded files that I will use to generate reports, alerts, and dashboards.

## Load and Analyze Windows Logs

1. Uploaded “windows_server_logs.csv” file in Splunk.

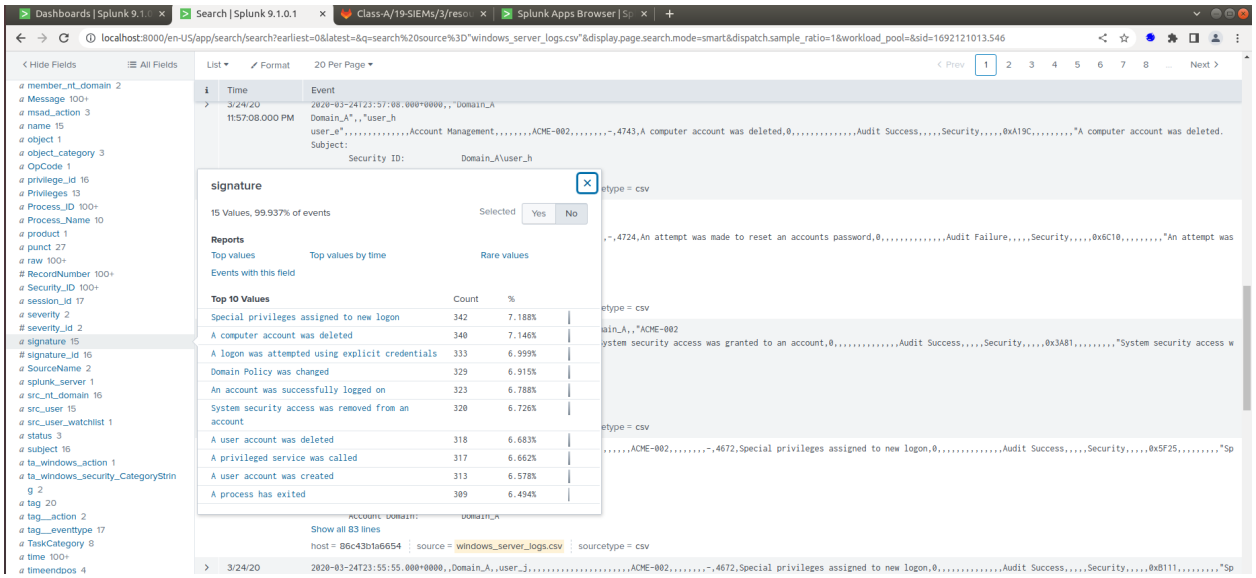


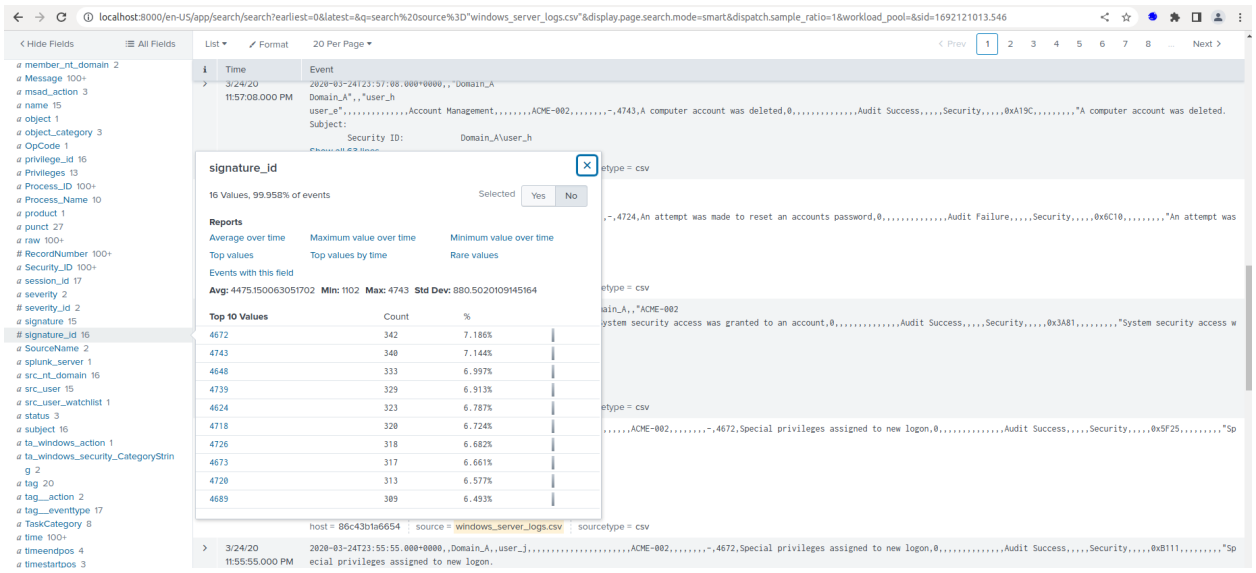

Once the logs were uploaded, I briefly took notice of and analyzed the following fields:

o signature
o signature_id
o user
o status
o severity

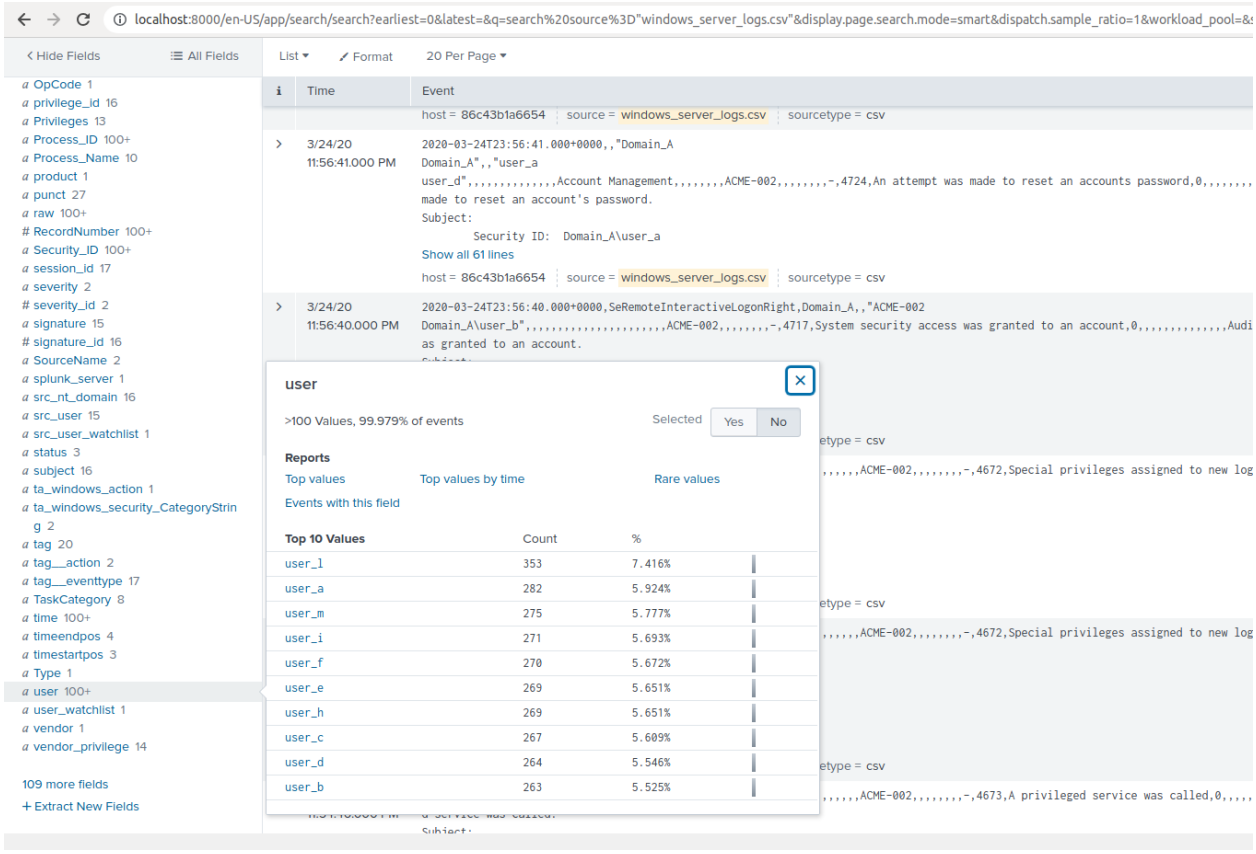
1. signature



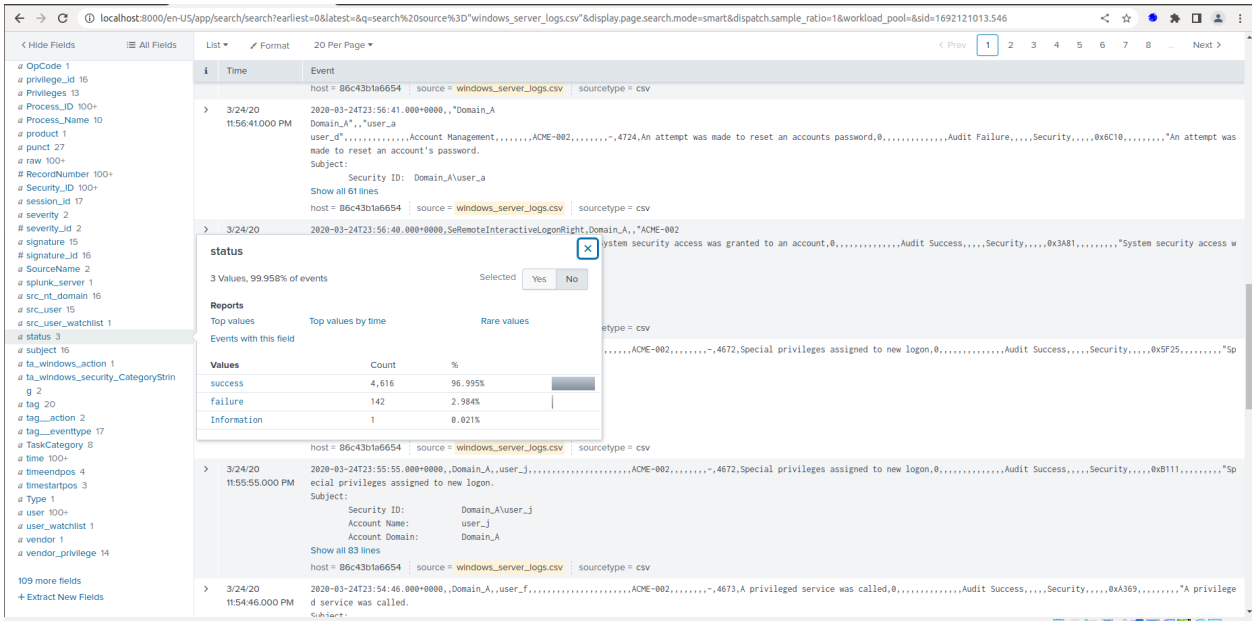

2. Signature_id



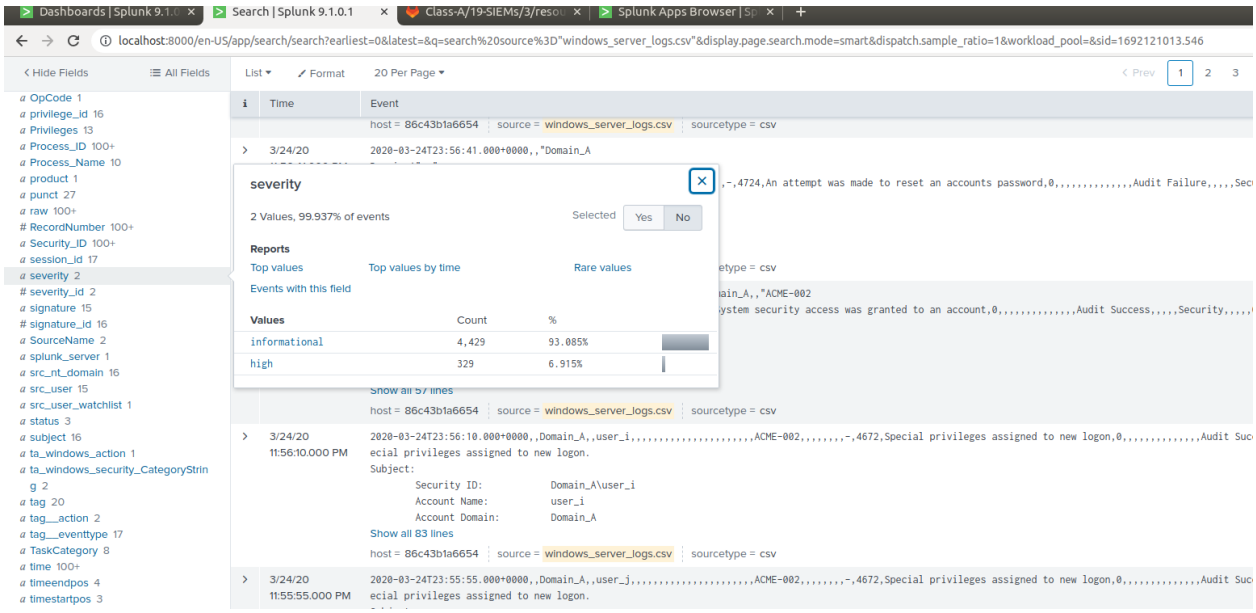

3. users


user
>100 Values, 99.979% of events
Selected
Yes
No
Reports
Top values
Top values by time
Rare values
Events with this field
Top 10 Values
Count
%
user_l 353 7.416%
user_a 282 5.924%
user_m 275 5.777%
user_i 271 5.693%
user_f 270 5.672%
user_e 269 5.651%
user_h 269 5.651%
user_c 267 5.609%
user_d 264 5.546%
user_b 263 5.525%

## 4. Status


status
3 Values, 99.958% of events
Selected
Yes
No
Reports
Top values
Top values by time
Rare values
Events with this field
Values
Count
%
success 4,616 96.995%
failure 142 2.984%
Information 1 0.021%

5. Severity

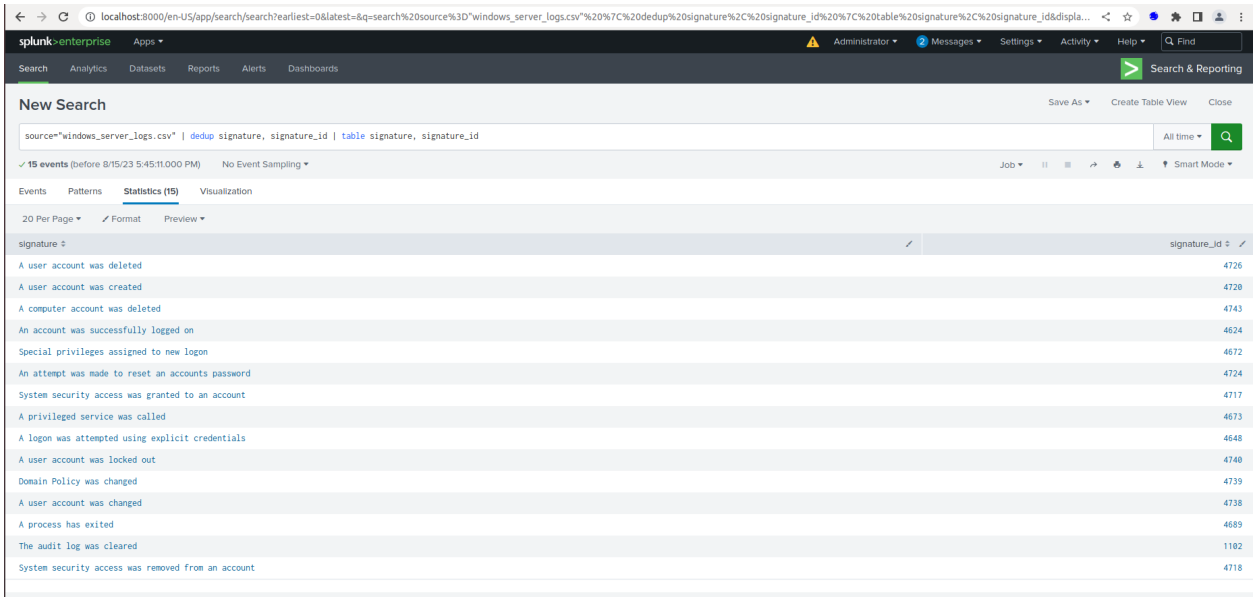



These above important points we will be focusing to creating our reports, alerts, and dashboard .

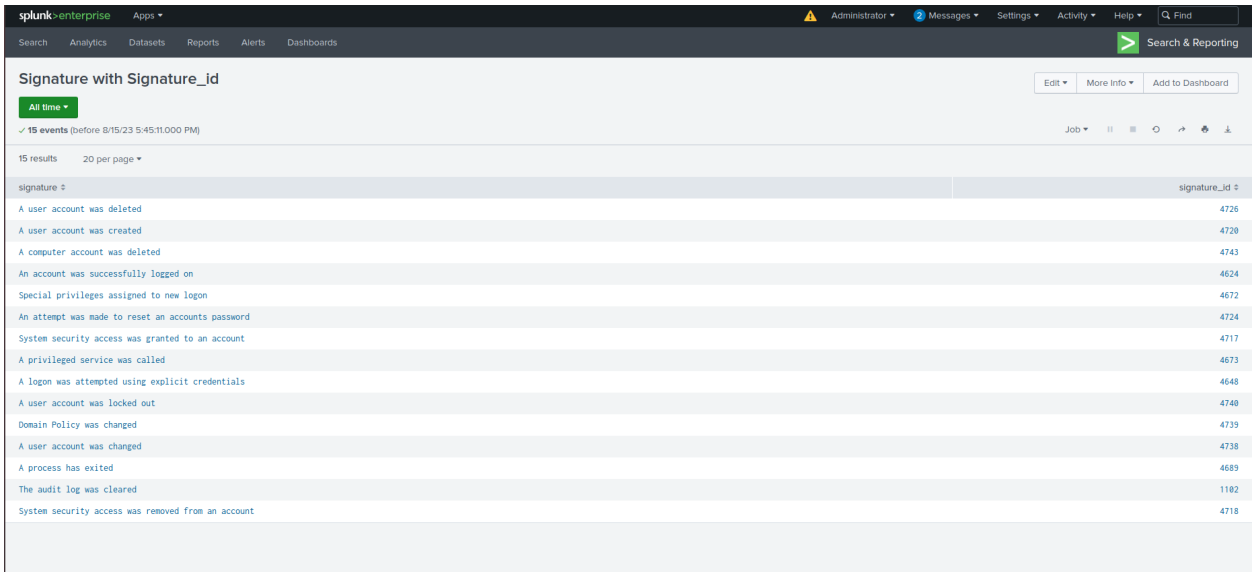
## Part 2: Create Reports, Alerts, and Dashboards for the Windows Logs

1. **Reports**: Design the following reports to assist VSI in quickly identifying specific information and **be sure to grab screenshots of each report**!
    - A report with a table of signatures and associated signature IDs.
        a. This will allow VSI to view reports that show the ID number associated with the specific signature for Windows activity.
        b. **Hint**: Research how to remove the duplicate values in your SPL search.
        c. Take a screenshot of the report.

(Search for the reports that show the ID number associated with the specific signature for Windows activity)




(Report Signature with Signature_id created )

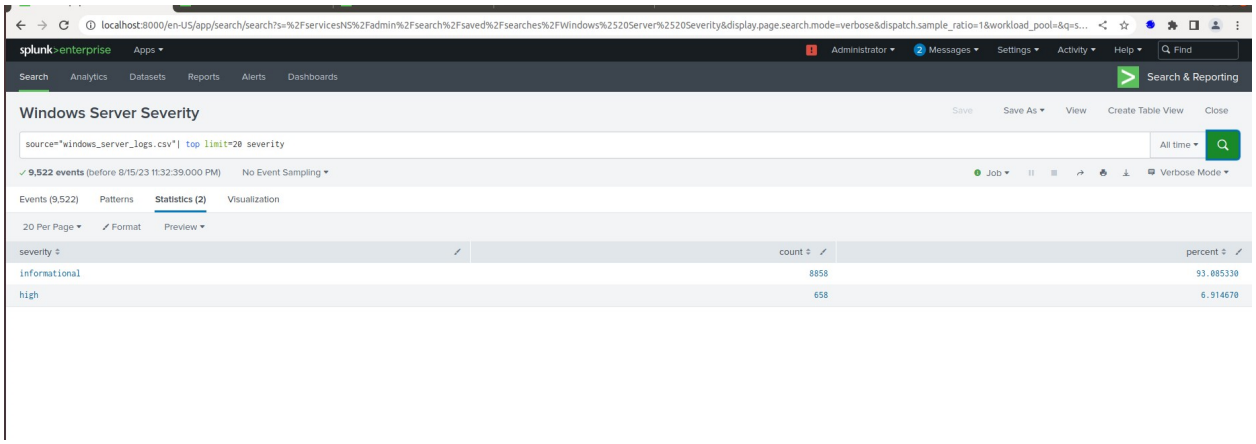



- A report that displays the severity levels, and the count and percentage of each.

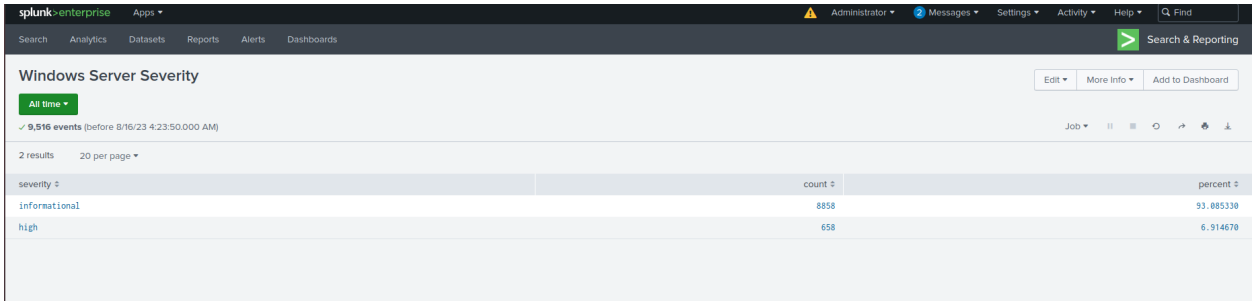
a. This will allow VSI to quickly understand the severity levels of the Windows logs being viewed.

b. Take a screenshot of the report.

(Search for the top severity level with percentage)




(Report Created Windows Server Severity)

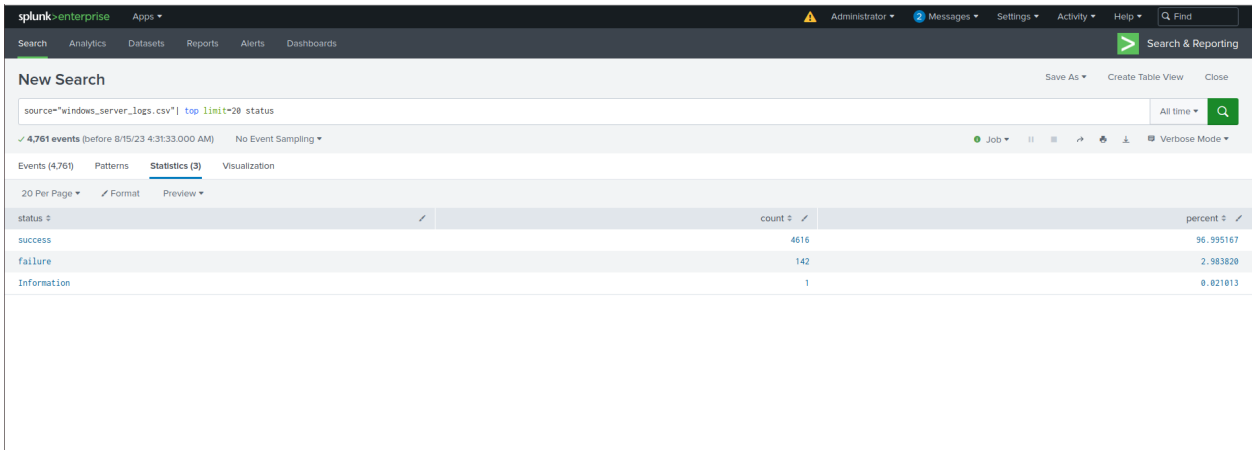


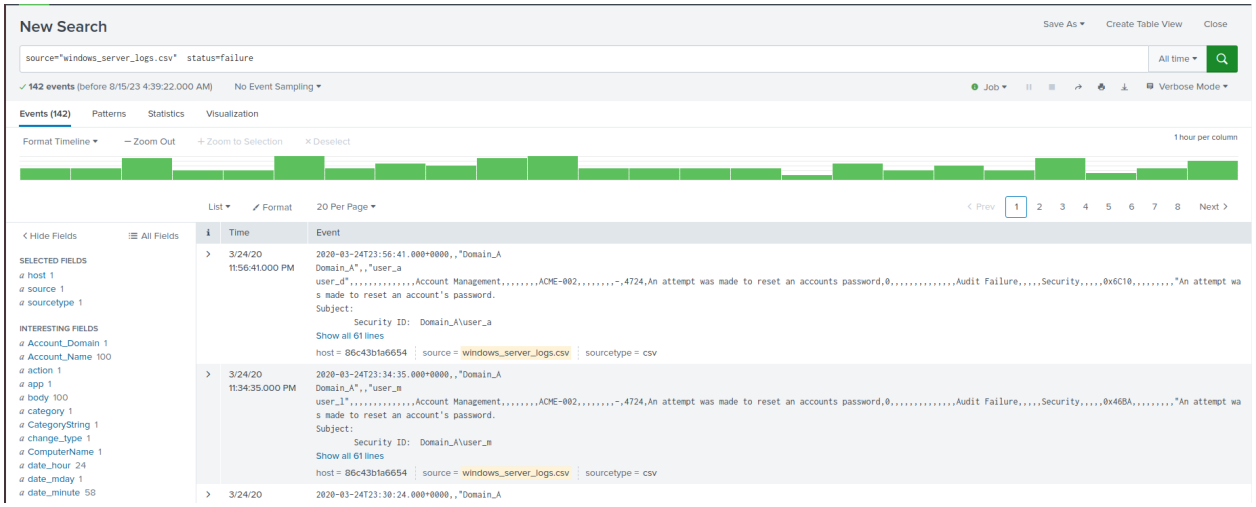

- A report that provides a comparison between the success and failure of Windows activities.

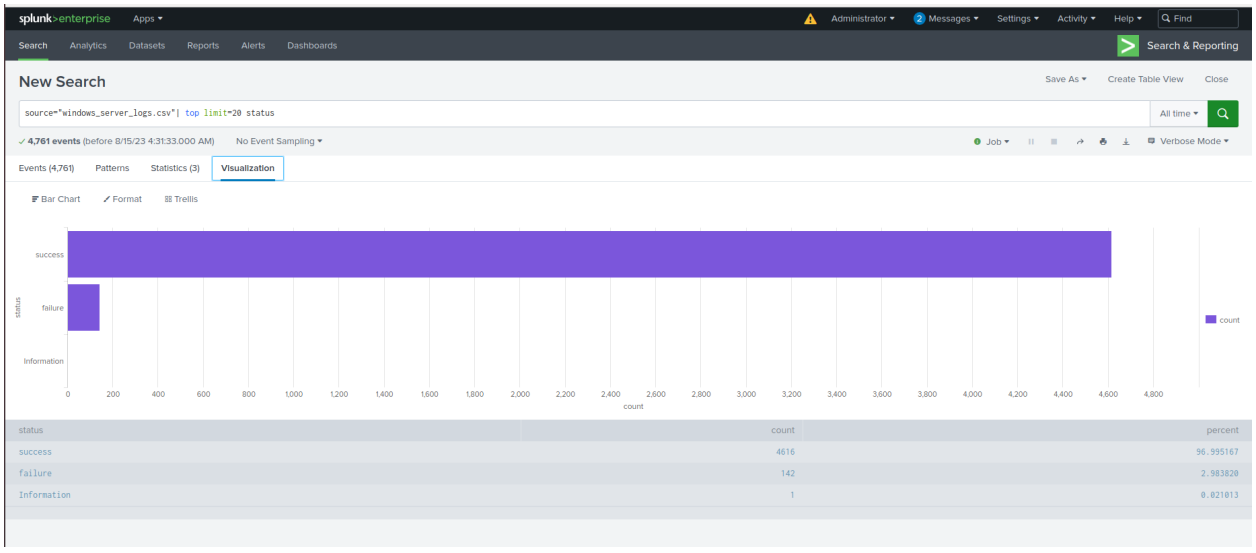
  a. This will show VSI if there is a suspicious level of failed activities on their server.

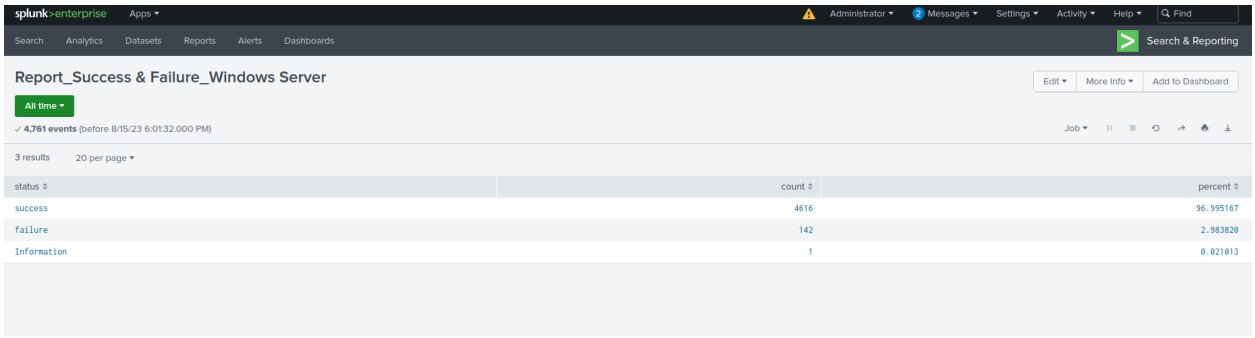
  b. **Hint**: Check the “status” field for this information.

  c. Take a screenshot of the report.


splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="windows_server_logs.csv"| top limit=20 status
All time
✓ 4,761 events (before 8/15/23 4:31:33.000 AM)
No Event Sampling
Job
Verbose Mode
Events (4,761)
Patterns
Statistics (3)
Visualization
20 Per Page
Format
Preview
status
count
percent
success 4616 96.995167
failure 142 2.983820
Information 1 0.021013

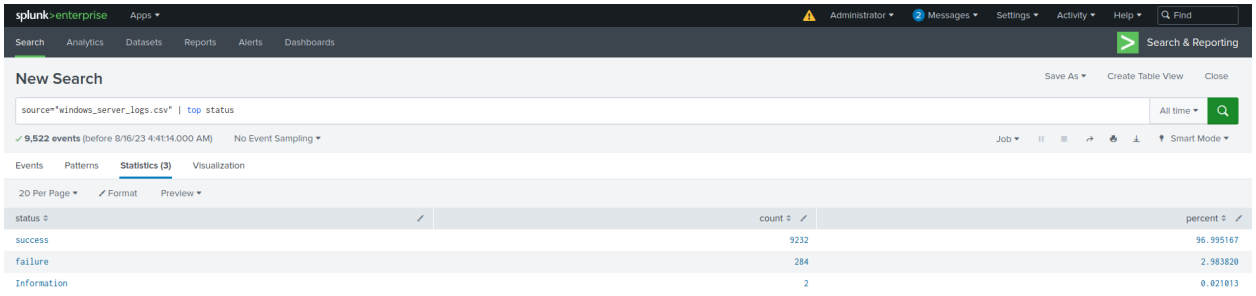

New Search
Save As
Create Table View
Close
source="windows_server_logs.csv" status=failure
All time
✓ 142 events (before 8/15/23 4:39:22.000 AM)
No Event Sampling
Job
Verbose Mode
Events (142)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
20 Per Page
Prev
1 2 3 4 5 6 7 8
Next
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
Account_Domain 1
Account_Name 100
action 1
app 1
body 100
category 1
CategoryString 1
change_type 1
ComputerName 1
date_hour 24
date_mday 1
date_minute 58
Time
Event
3/24/20 11:56:41.000 PM
2020-03-24T23:56:41.000+0000,,"Domain_A
Domain_A",,,"user_a
user_d",,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,Audit Failure,,,,Security,,,,0x6C10,,,,,,,,"An attempt was made to reset an account's password.
Subject:
Security ID: Domain_A\user_a
Show all 61 lines
host = 86c43b1a6654 source = windows_server_logs.csv sourcetype = csv
3/24/20 11:34:35.000 PM
2020-03-24T23:34:35.000+0000,,"Domain_A
Domain_A",,,"user_m
user_l",,,,,,,,,,,,,Account Management,,,,,,,,ACME-002,,,,,,,-,4724,An attempt was made to reset an accounts password,0,,,,,,,,,,,,Audit Failure,,,,Security,,,,0x46BA,,,,,,,,"An attempt was made to reset an account's password.
Subject:
Security ID: Domain_A\user_m
Show all 61 lines
host = 86c43b1a6654 source = windows_server_logs.csv sourcetype = csv
3/24/20
2020-03-24T23:30:24.000+0000,,"Domain_A


splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="windows_server_logs.csv"| top limit=20 status
All time
✓ 4,761 events (before 8/15/23 4:31:33.000 AM)
No Event Sampling
Job
Verbose Mode
Events (4,761)
Patterns
Statistics (3)
Visualization
Bar Chart
Format
Trellis
success
failure
Information
status
count
0 200 400 600 800 1,000 1,200 1,400 1,600 1,800 2,000 2,200 2,400 2,600 2,800 3,000 3,200 3,400 3,600 3,800 4,000 4,200 4,400 4,600 4,800
count
status count percent
success 4616 96.995167
failure 142 2.983820
Information 1 0.021013

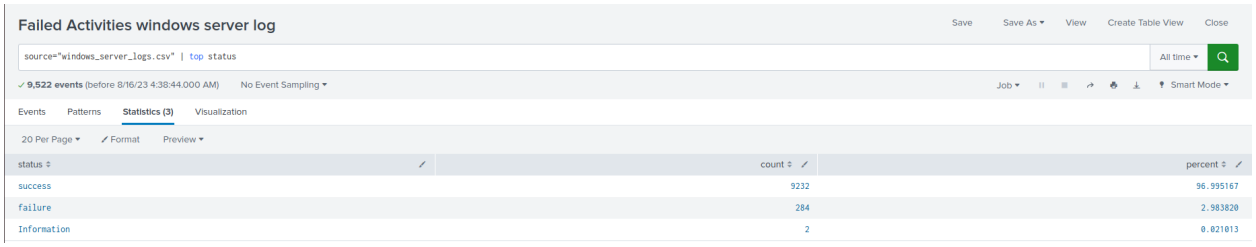


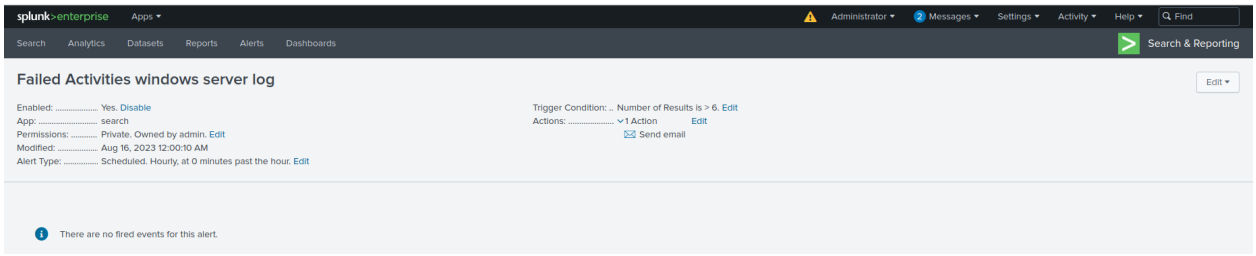

1. **Alerts**: Design the following alerts to notify VSI of suspicious activity. Keep this information on hand. You will include it in your presentation.
    - Determine a baseline and threshold for the hourly level of failed Windows activity.
        a. Create an alert that's triggered when the threshold has been reached.
        b. The alert should trigger an email to SOC@VSI-company.com.

(Search for failed Windows activity)



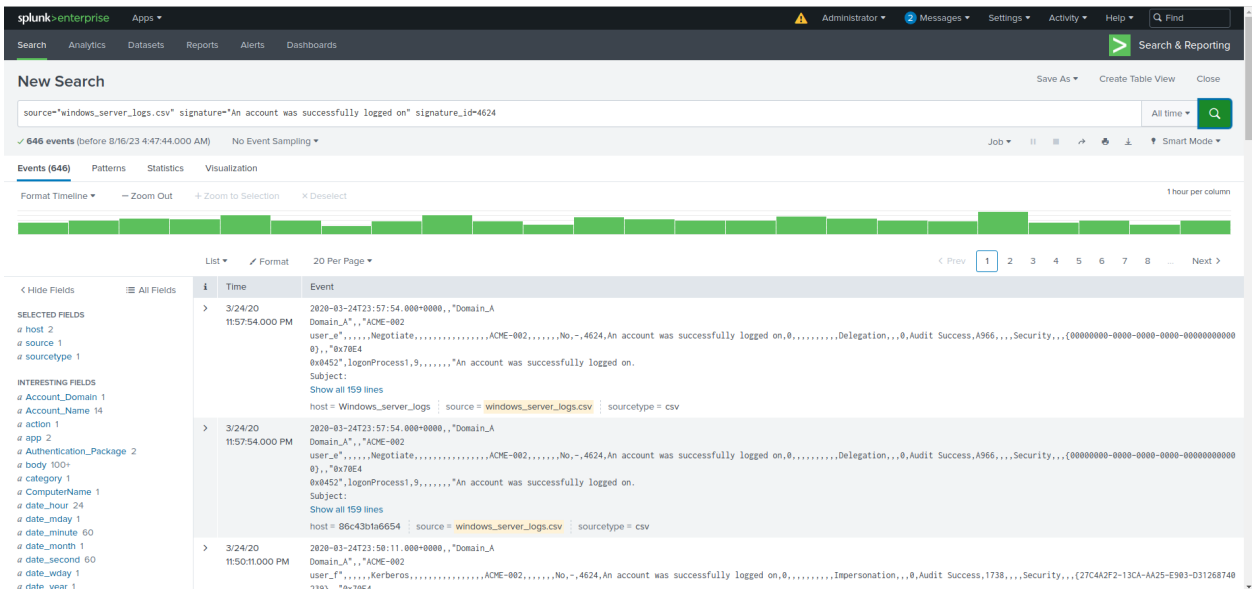

(Alert created for triggered when the level of failed Windows activity is greater than 6 per hour)



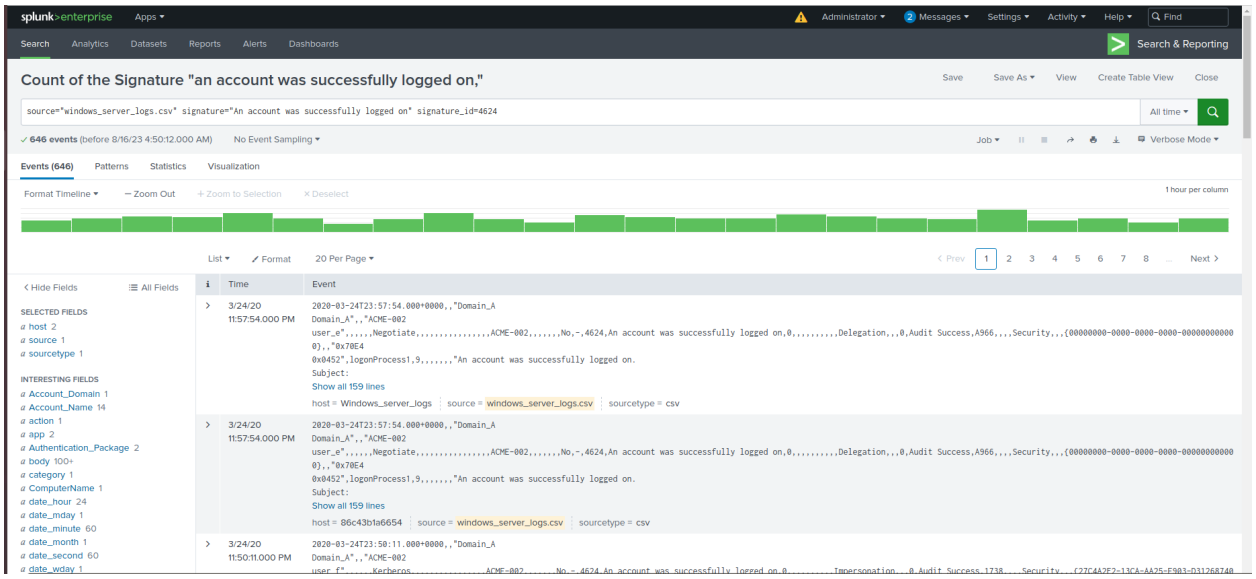


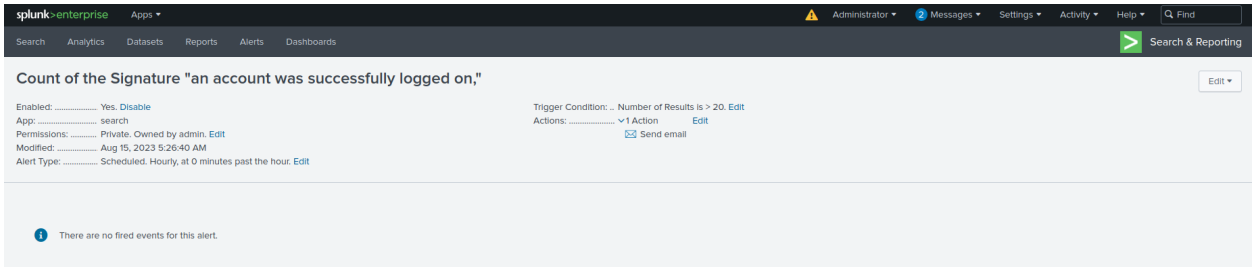

- Determine a baseline and threshold for the hourly count of the signature “an account was successfully logged on.”
    a. Create an alert that's triggered when the threshold has been reached.
    b. The alert should trigger an email to SOC@VSI-company.com.
    c. Design the alert based on the corresponding signature ID, as the signature name sometimes changes when the Windows system updates.

(Search for the signature “an account was successfully logged on”)



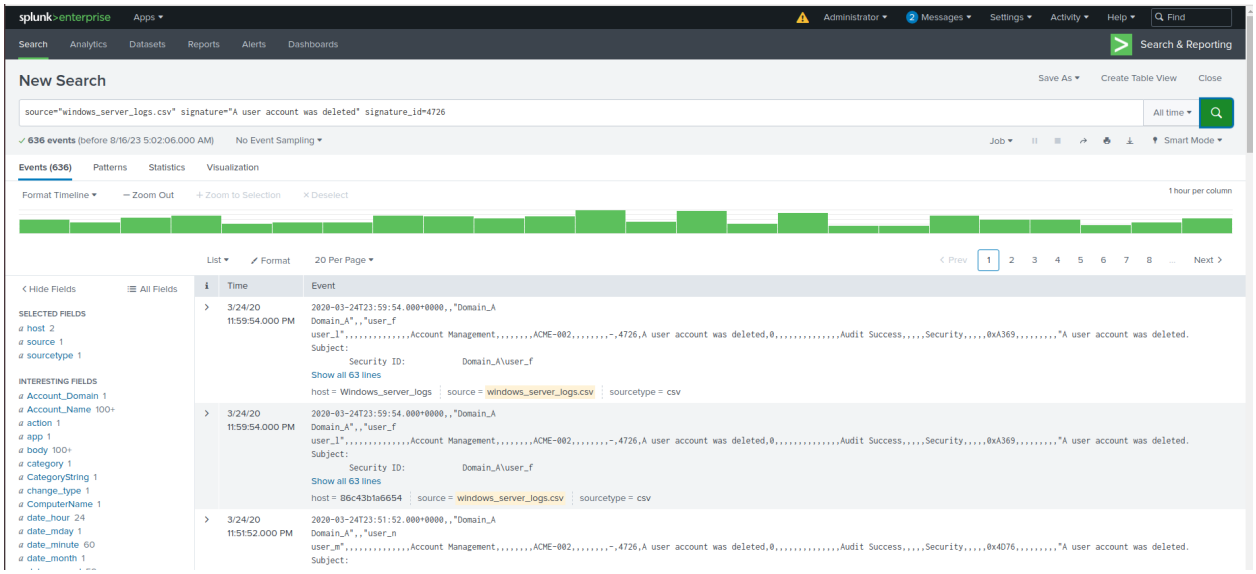

(Alert created for triggered to the signature “an account was successfully logged on is greater than 20 per hour)



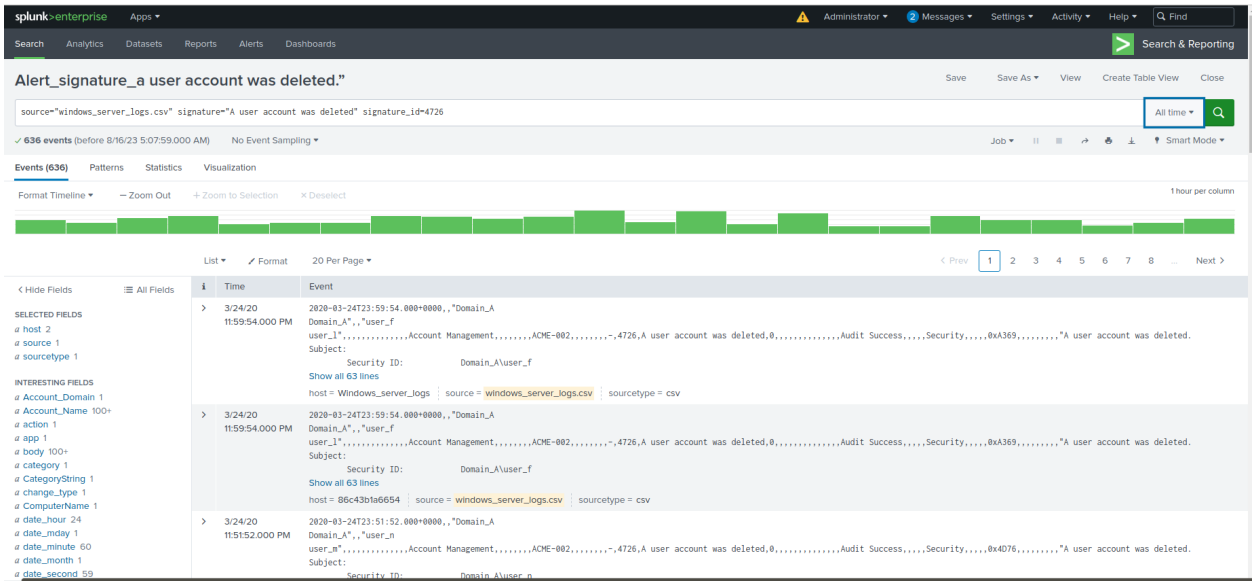



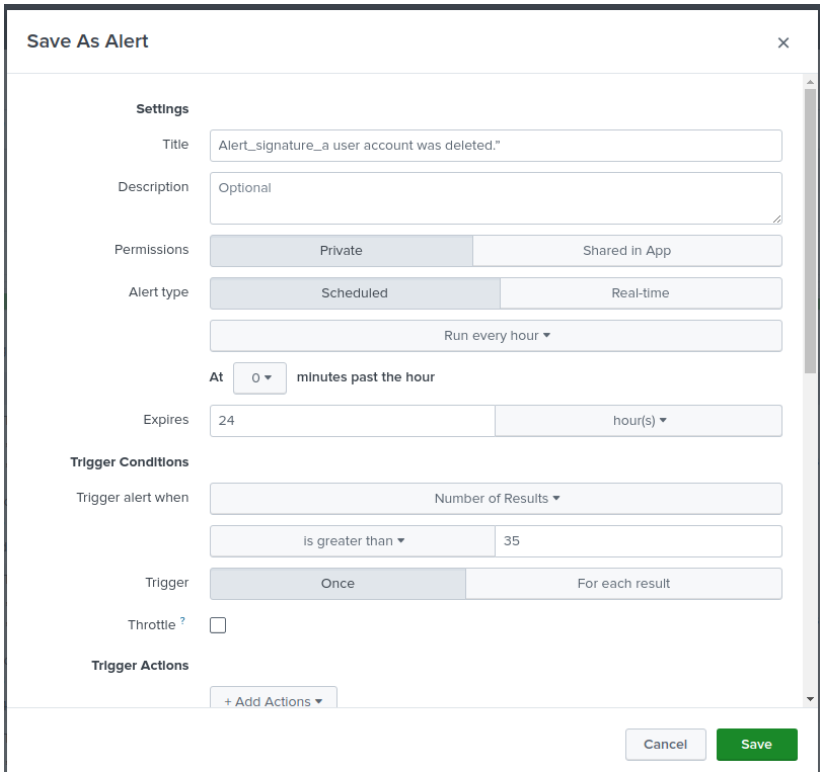

- Determine a baseline and threshold for the hourly count of the signature “a user account was deleted.”
    a. Design the alert based on the corresponding signature ID, as the signature name sometimes changes when the Windows system updates.
    b. Create an alert that's triggered when the threshold has been reached.
    c. The alert should trigger an email to SOC@VSI-company.com.

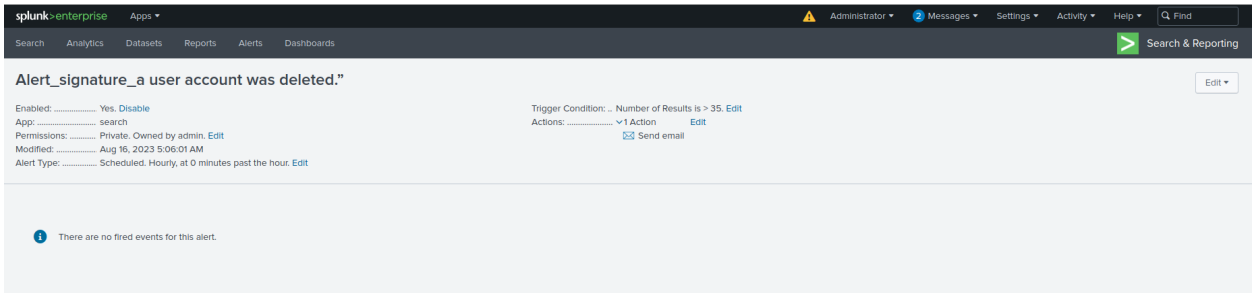
(Search for the signature “a user account was deleted”)




(Aleart created which triggered when signature “a user account was deleted” is greater than 35 per hour)

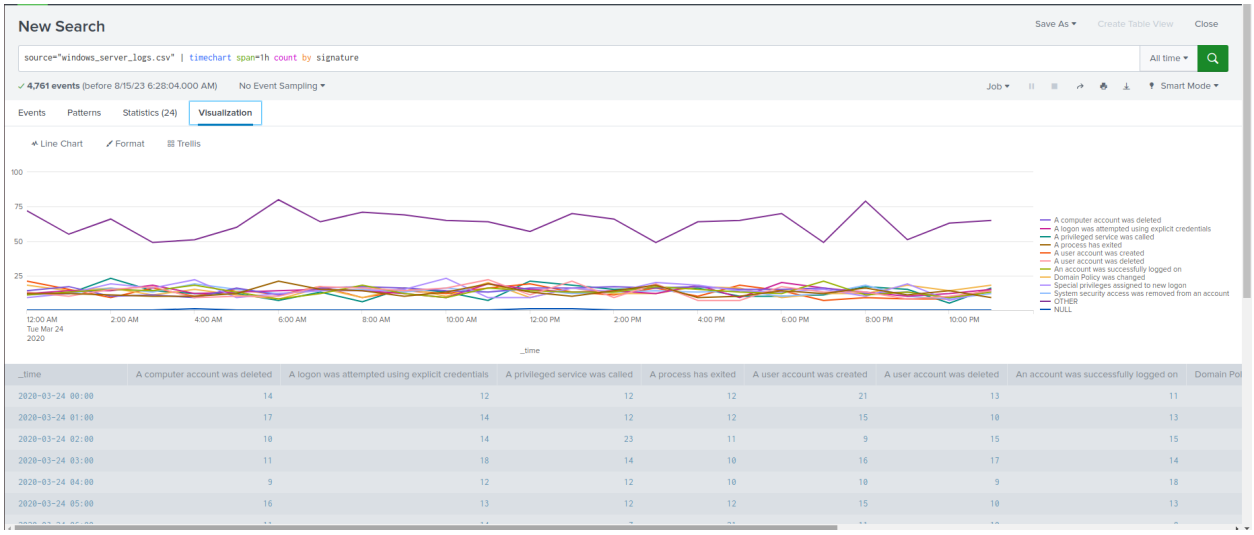




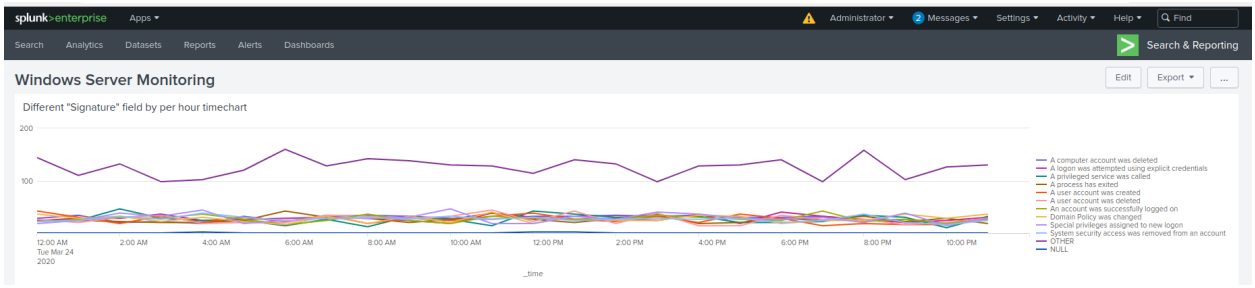




1. **Visualizations and dashboards**: Design the following visualizations, and add them to a dashboard called “Windows Server Monitoring.” Be creative with your visualizations, and make sure to grab screenshots of each!
    - A line chart that displays the different “signature” field values over time.
        a. **Hint**: Add the following after your search: `timechart span=1h count by signature`
        b. Take a screenshot of the chart.

(Search for the different “signature” field for the time chart for per hour)

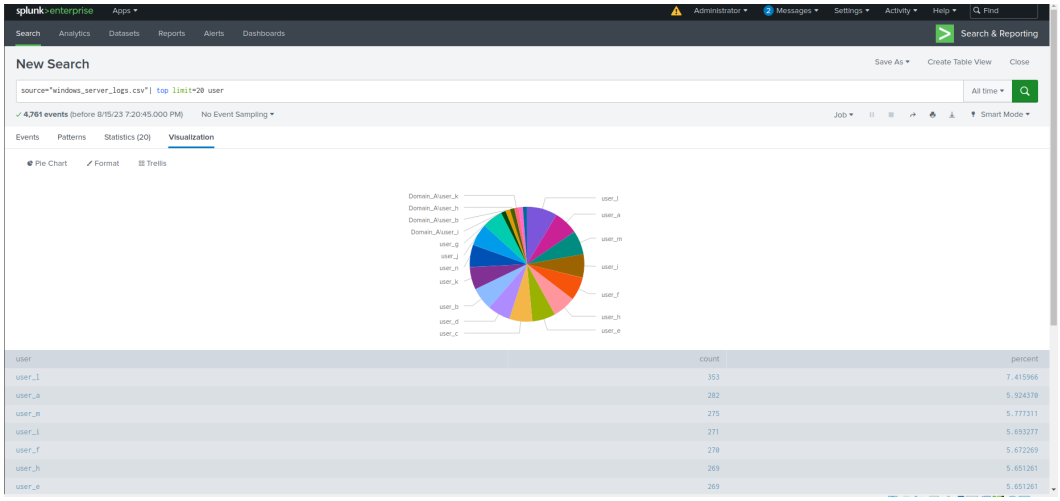



(New Dashboard created with the Different “Signature” field by per hour in the Line chart Visualization)

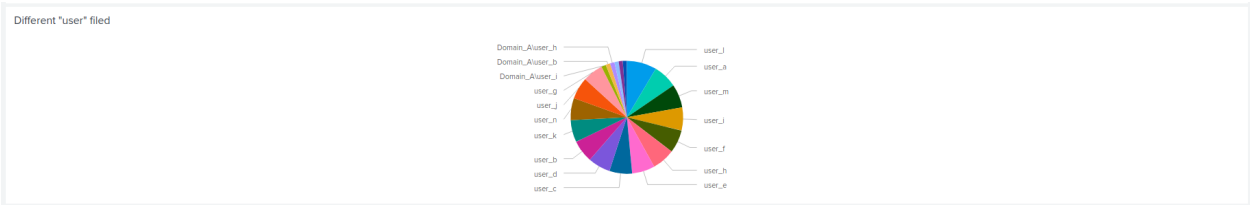



- A line chart that displays the different “user” field values over time.
    a. Take a screenshot of the chart.

(Search for the different “user” field)

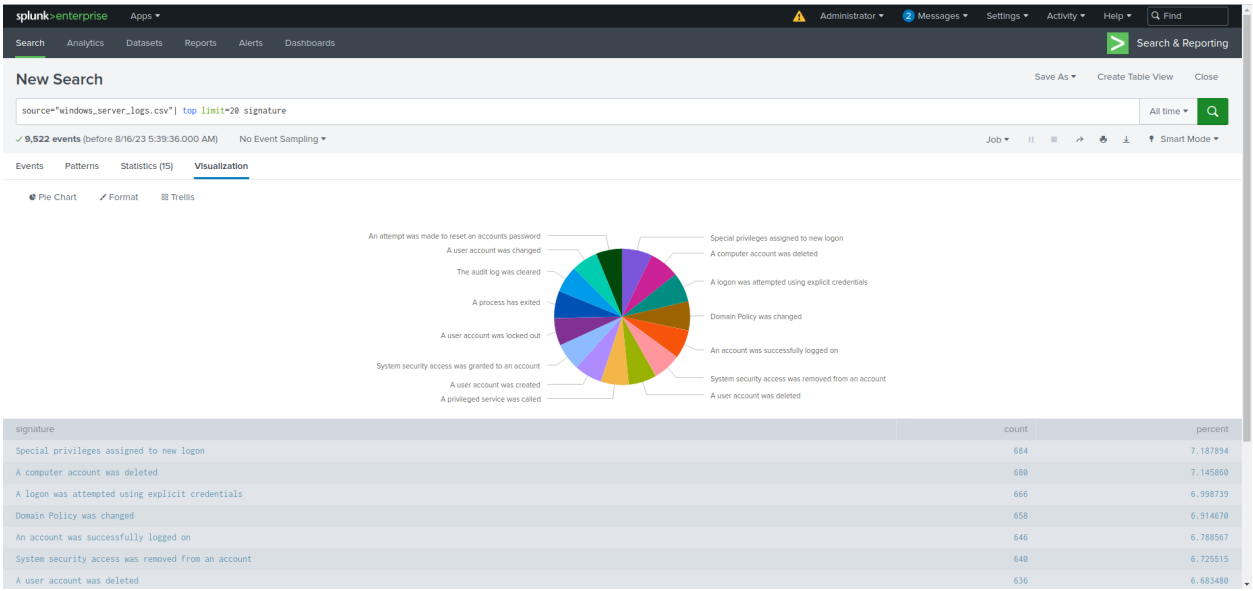


(Panel added to existing Windows Server Monitoring Dashboard with name Different “user”)

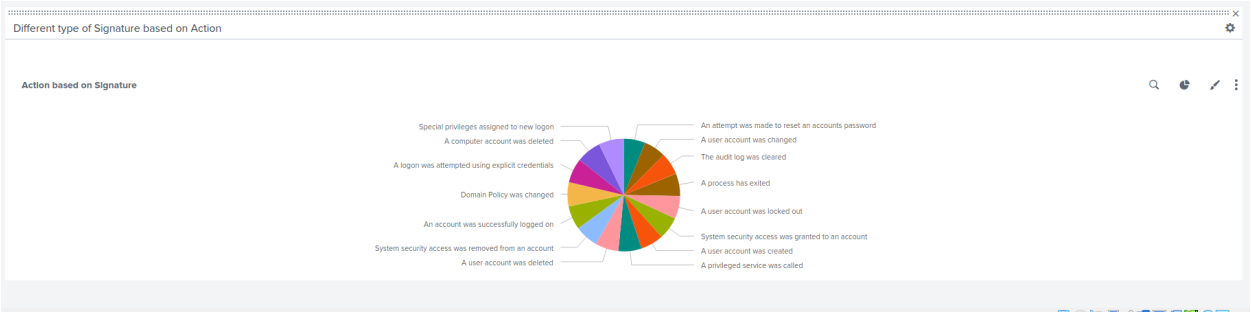



- Any visualization that illustrates the count of different signatures.
    a. **Hint**: You can add brand-new custom visualizations by accessing this page inside your VM: Additional Viz.
    b. Take a screenshot of the visualization.

(Search for the different “signature”)

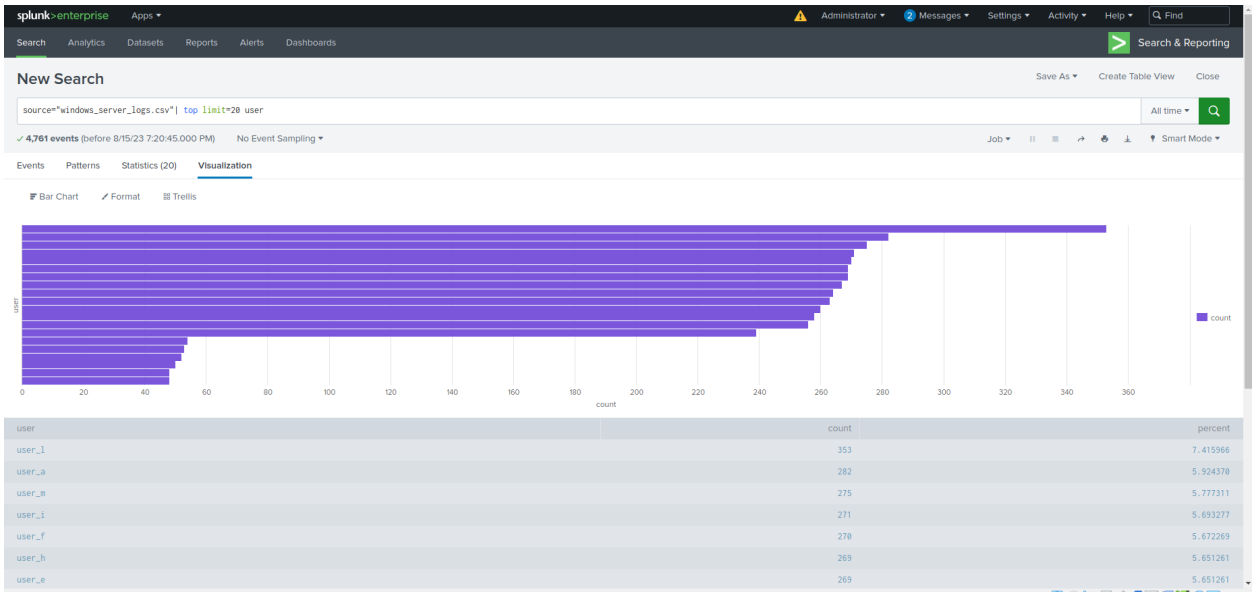



(Panel added to existing Windows Server Monitoring Dashboard)



- Any visualization that illustrates the count of different users.
    a. Take a screenshot of the visualization.

(Search for the different users)

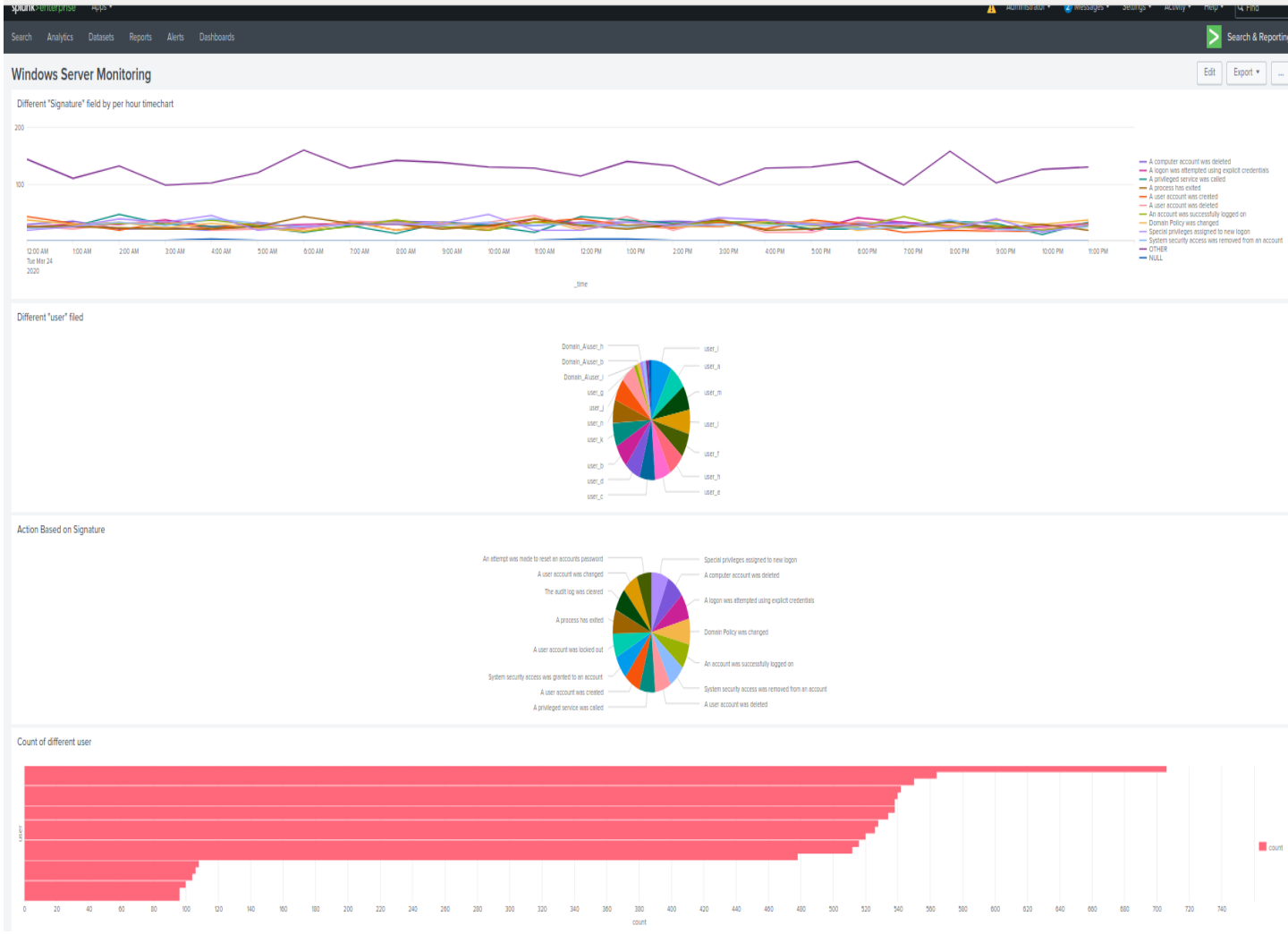



(Panel added to existing Windows Server Monitoring Dashboard)

- 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.
    a. Take a screenshot of the visualization.

4. 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.



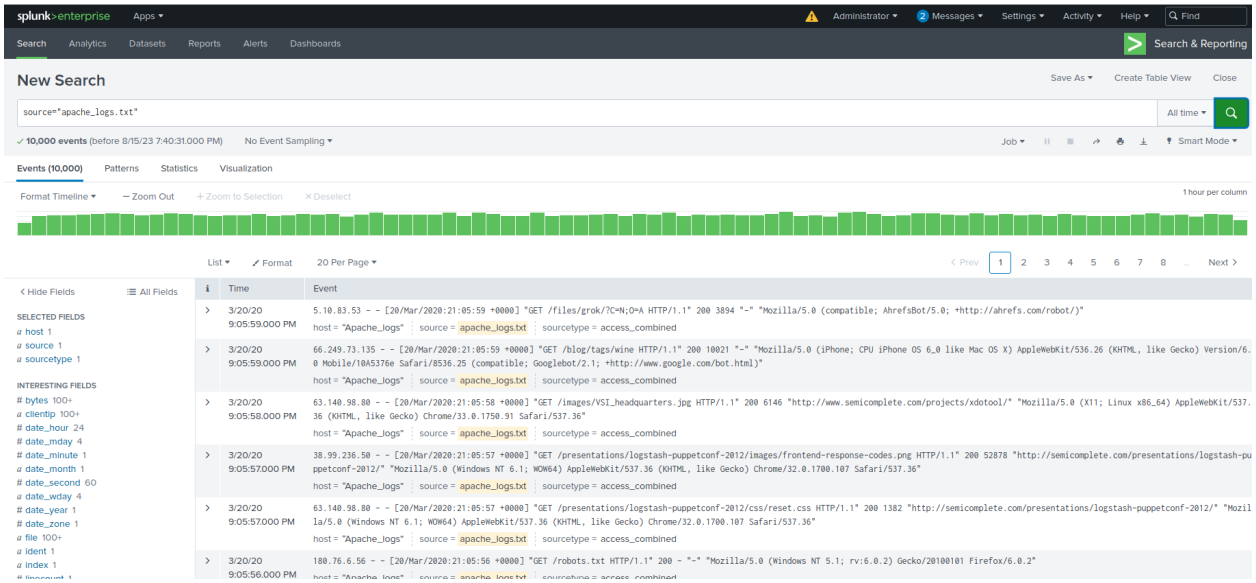

## Part 3: Load and Analyze Apache Logs

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:

1. Return to the “Add Data” option within Splunk.
2. Since you will upload the provided log file, select the “Upload” option.
    - Click “Select File.”

- Select the `apache_logs.txt` file located in the `/splunk/logs/Week-2-Day-3-Logs/` directory.
- Click the green “Next” button in the top right.

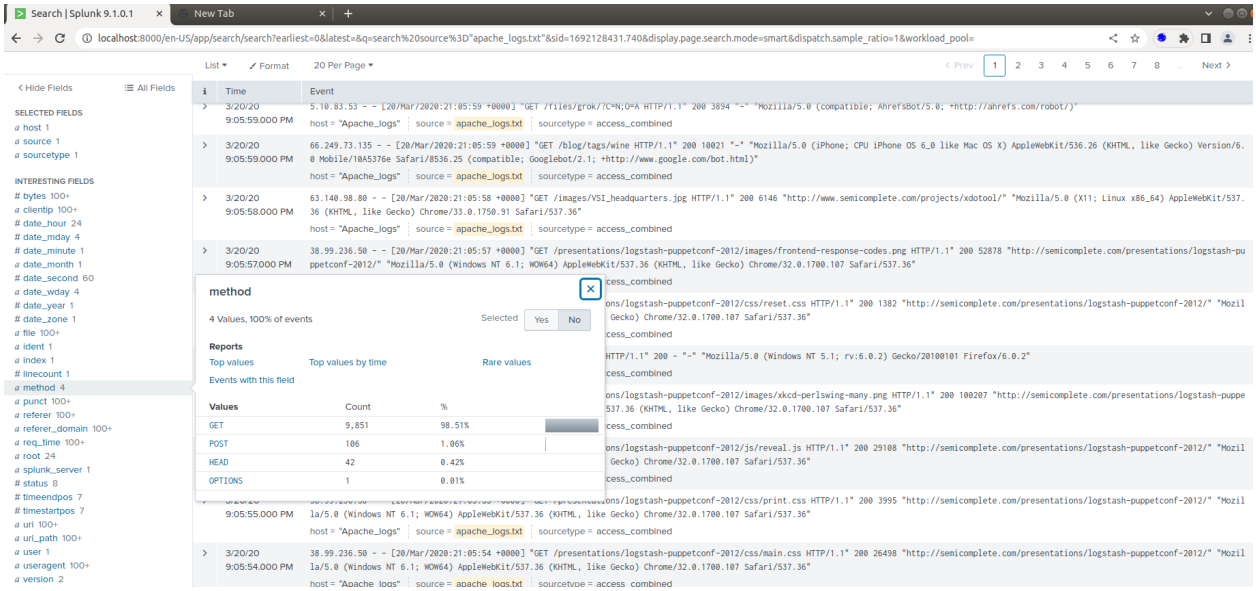
3. You will be brought to the “Set Source Type” page.
    - You don't need to change any configurations on this page.
    - Select “Next” again.
4. You'll be brought to the “Input Settings” page.
    - This page contains optional settings for how the data is input.
    - In the “Host” field, Splunk uses a random value to name the machine or device that generated the logs.
    - Update the value to “Apache_logs” and then select “Review.”
5. On the “Review” page, verify that you've chosen the correct settings, as the following image shows:
   6.
6. Once the file has successfully uploaded, a message that says “File has been uploaded successfully” will appear on the screen.
7. Select “Start Searching.”



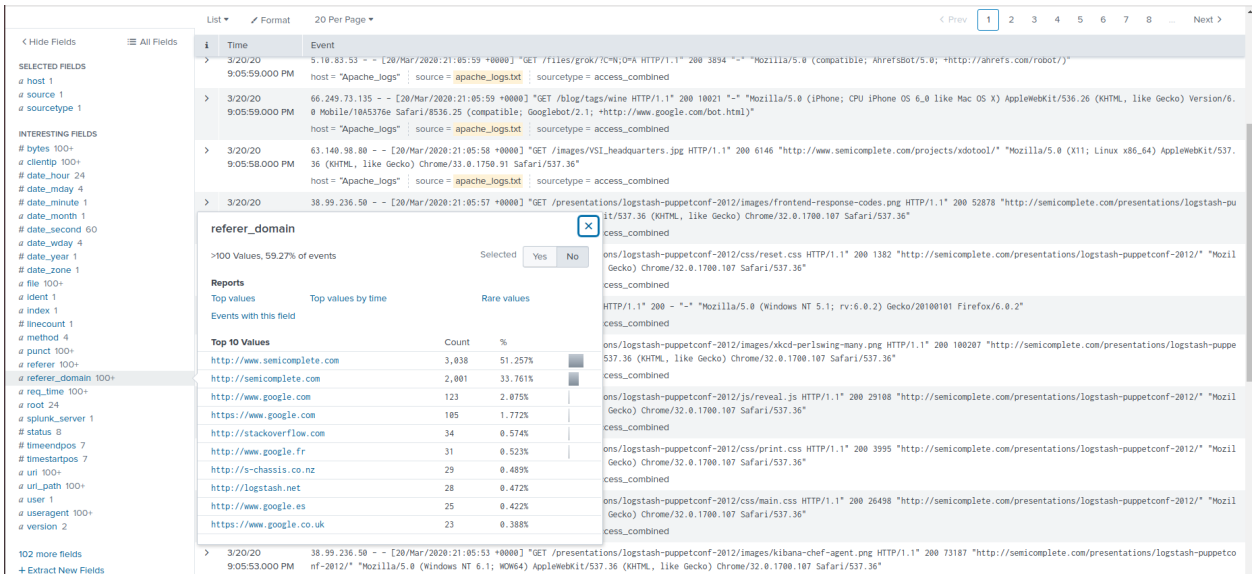

8. ⚠️ **Important**: After the data populates on the search, select “All Time” for the time range.

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

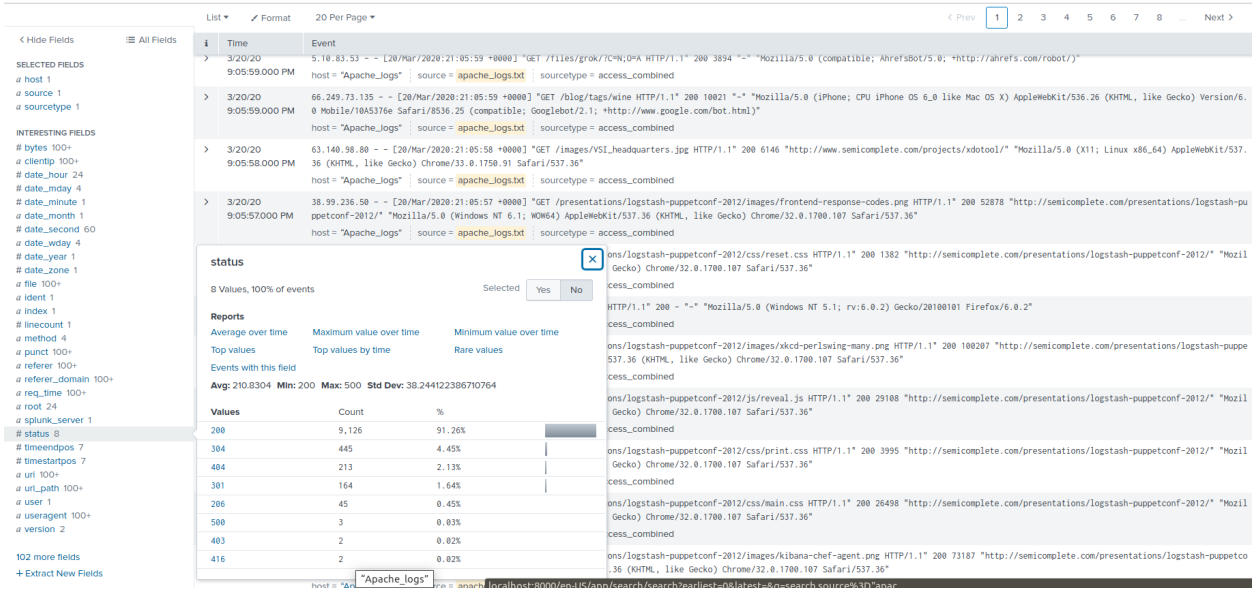
- method



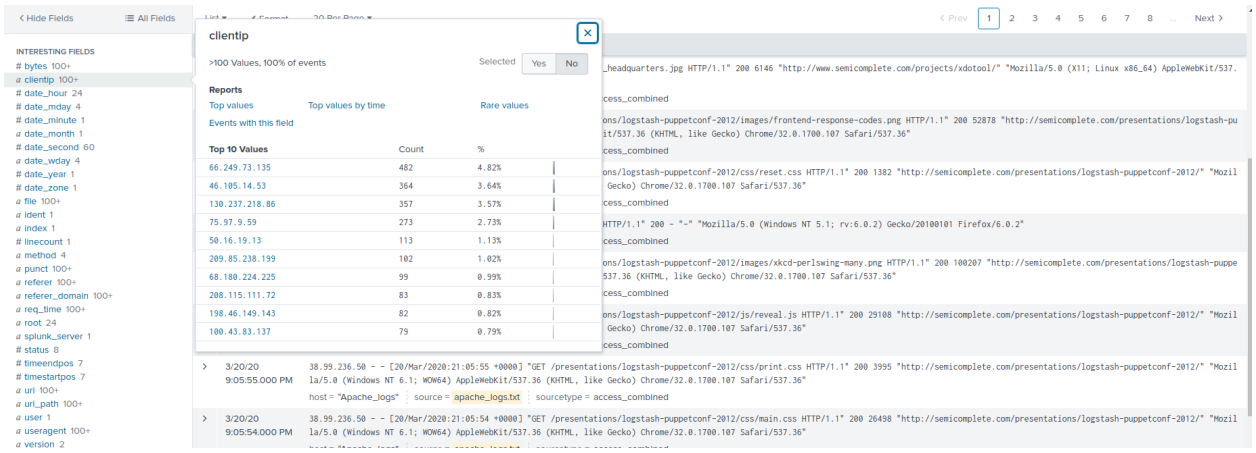

- referer_domain



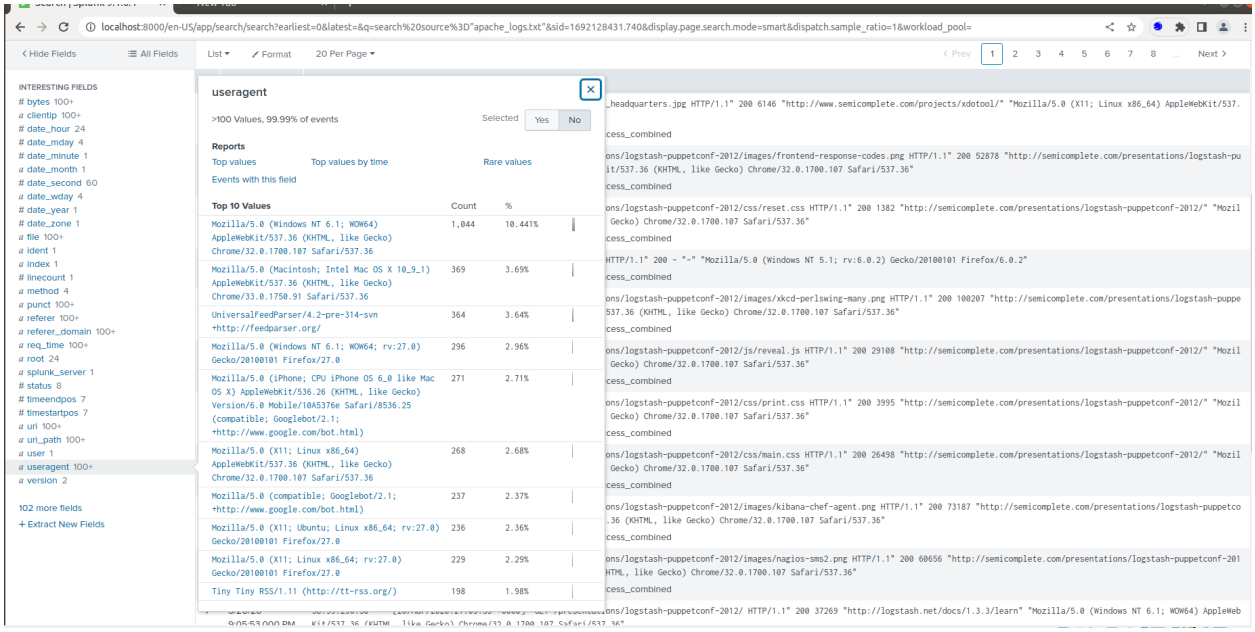

- status




- clientip




- useragent

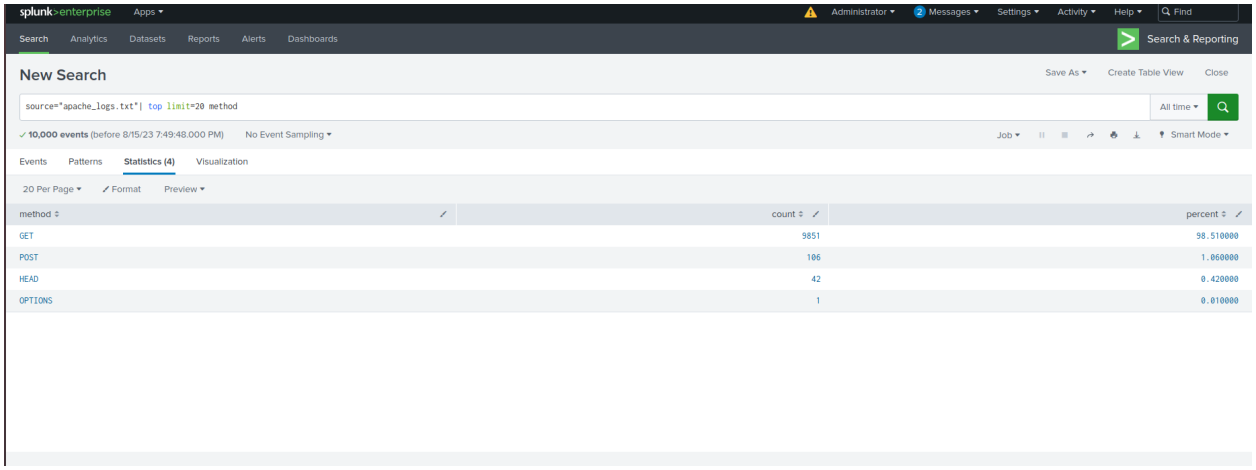



## Part 4: Create Reports, Alerts, and Dashboards for the Apache Logs

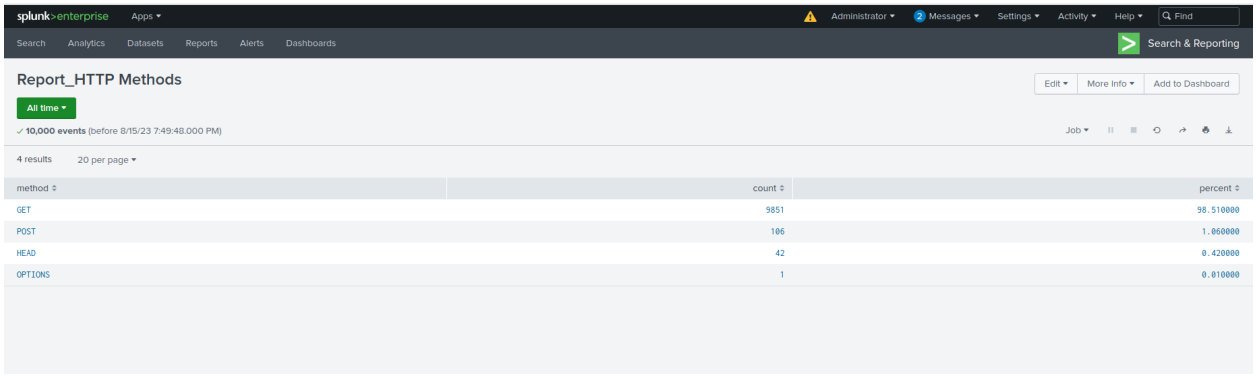
In this part, you will create reports, alerts, and dashboards to monitor for suspicious activity against VSI's Apache web server. To do so, complete the following steps:

1. 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):
        a. 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 VSI's web server.

(Search for the HTTP methods)

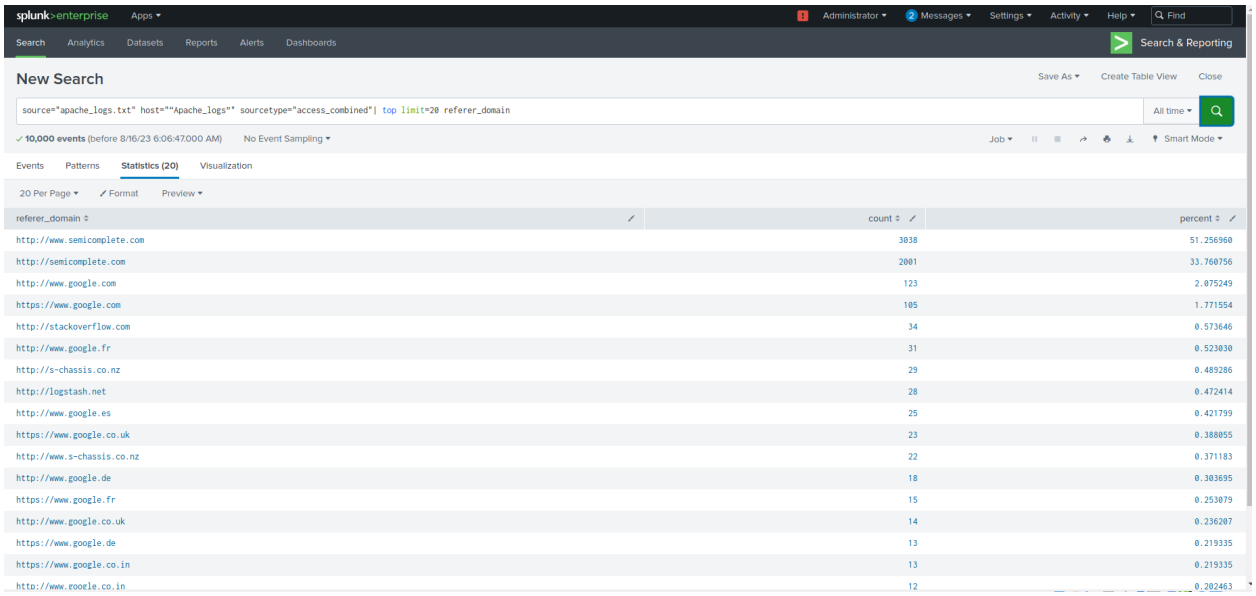



(Report created for the HTTP Methods)

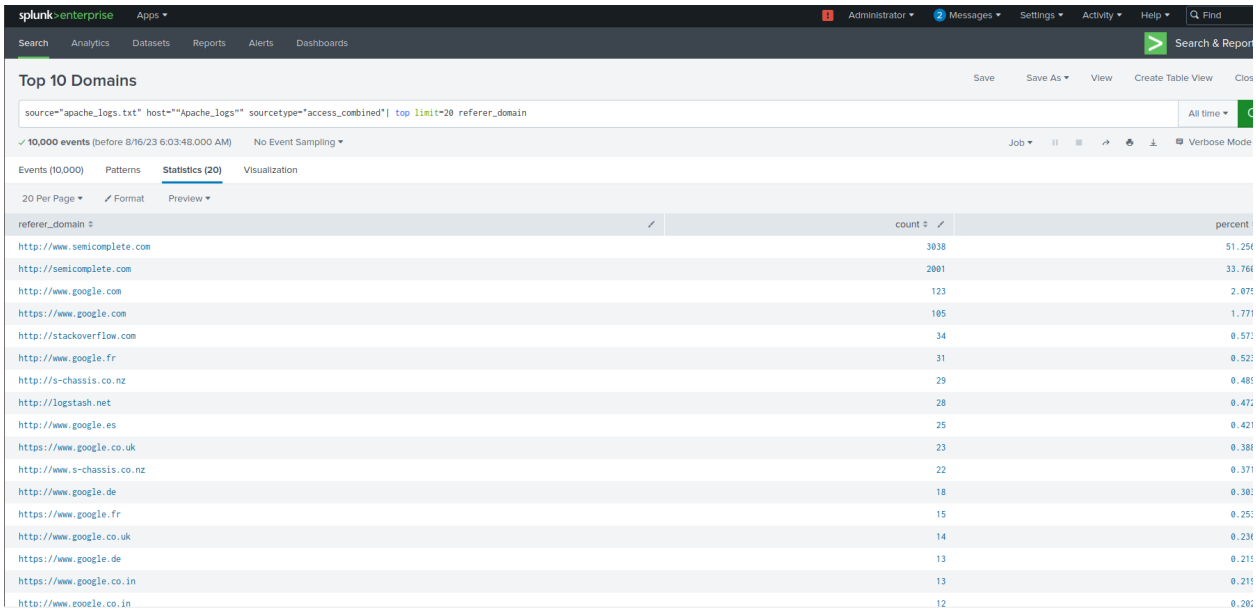



b. A report that shows the top 10 domains that refer to VSI's website.
    - This will assist VSI with identifying suspicious referrers.

(Search for the top 10 domains)

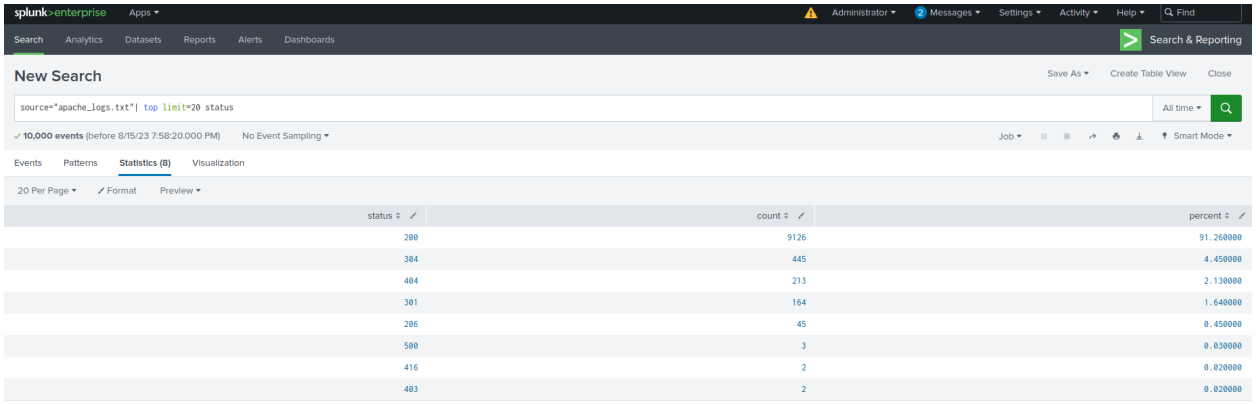


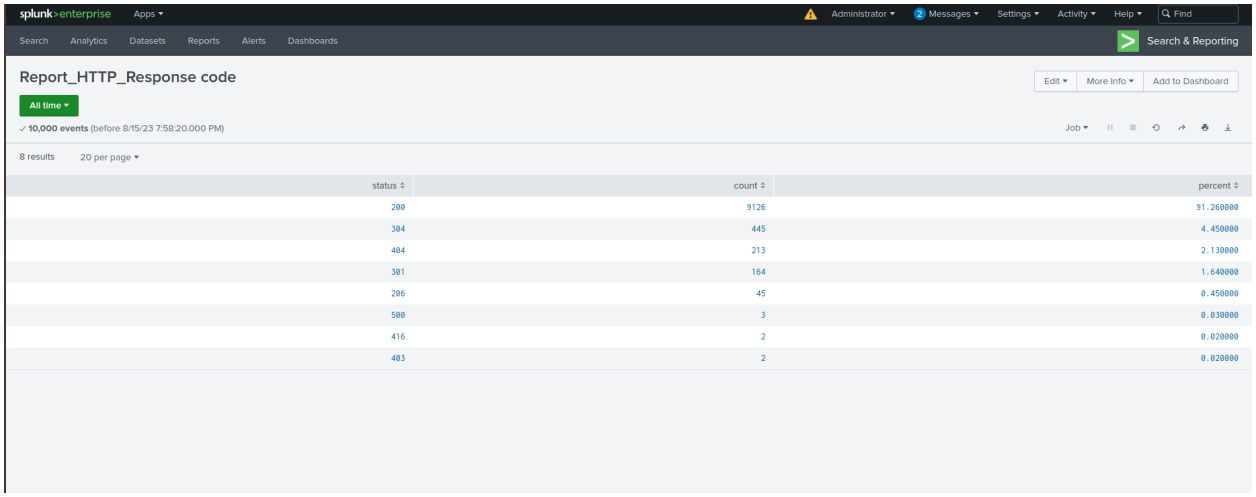

(Report created for the Top 10 Domains)



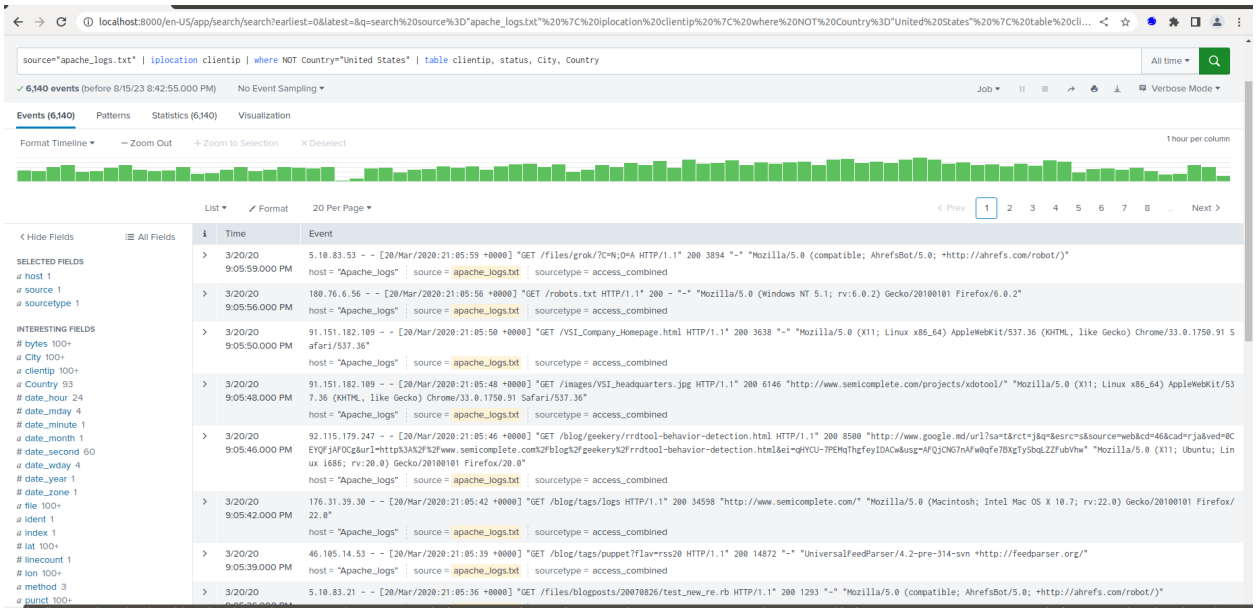

c. A report that shows the count of each HTTP response code.
    - This will provide insight into any suspicious levels of HTTP responses.

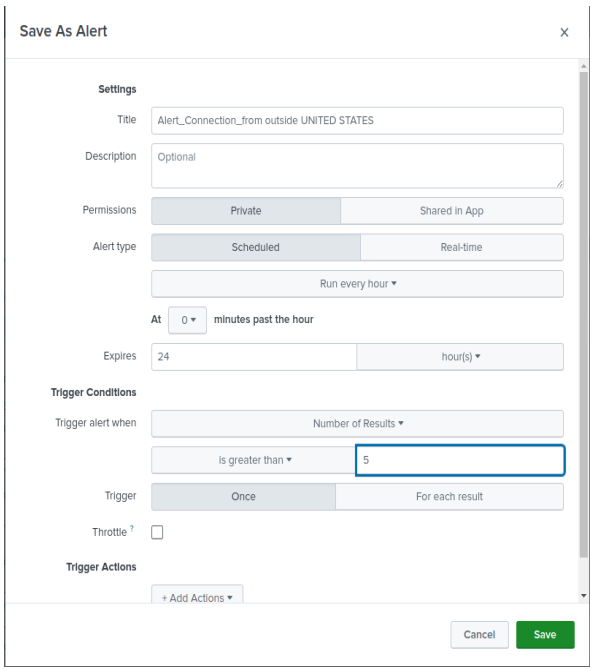
(Search for the HTTP response code)

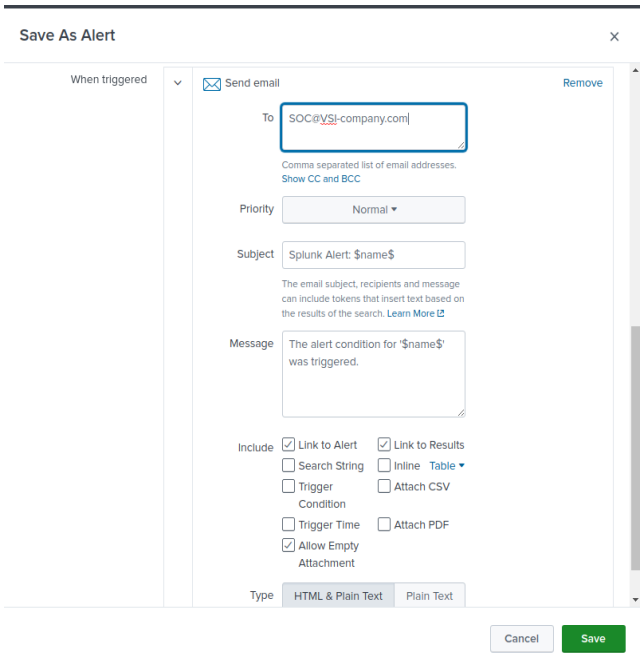


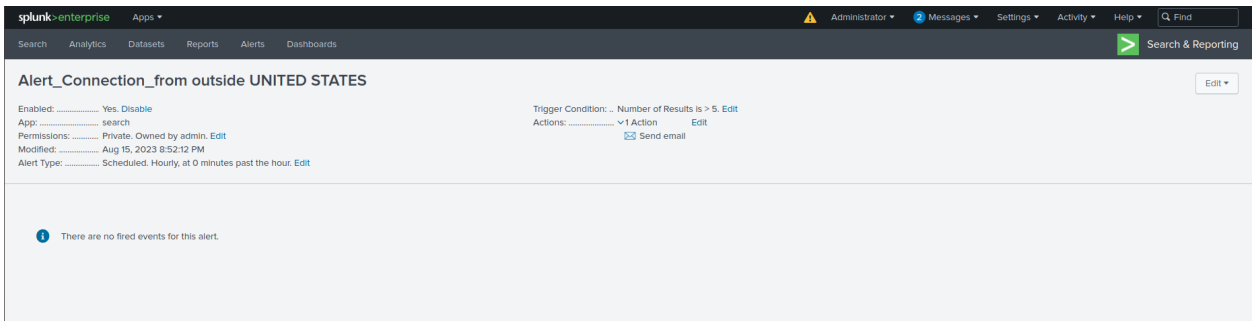




- **Alerts**: Design the following alerts:
    a. Determine a baseline and threshold for hourly activity from any country besides the United States.
        - Create an alert that's triggered when the threshold has been reached.
        - The alert should trigger an email to SOC@VSI-company.com.



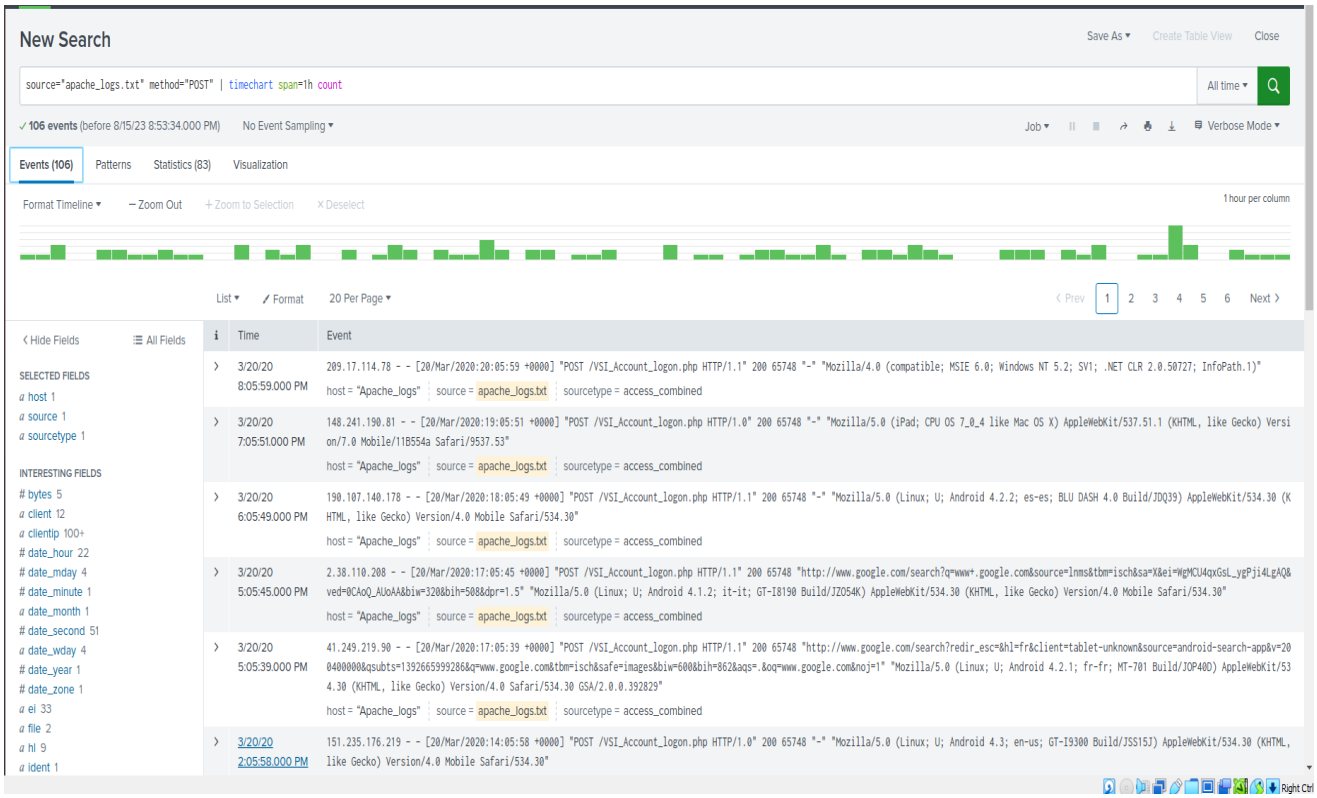



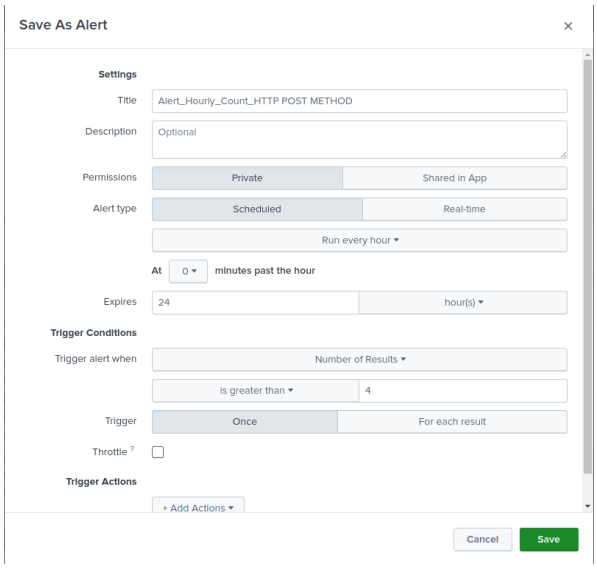



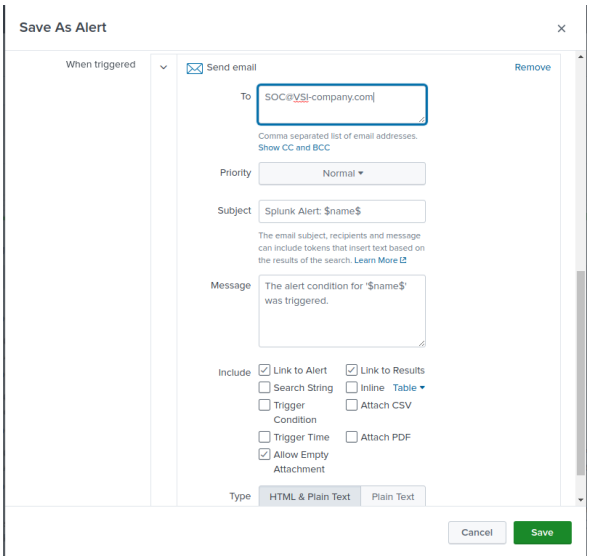



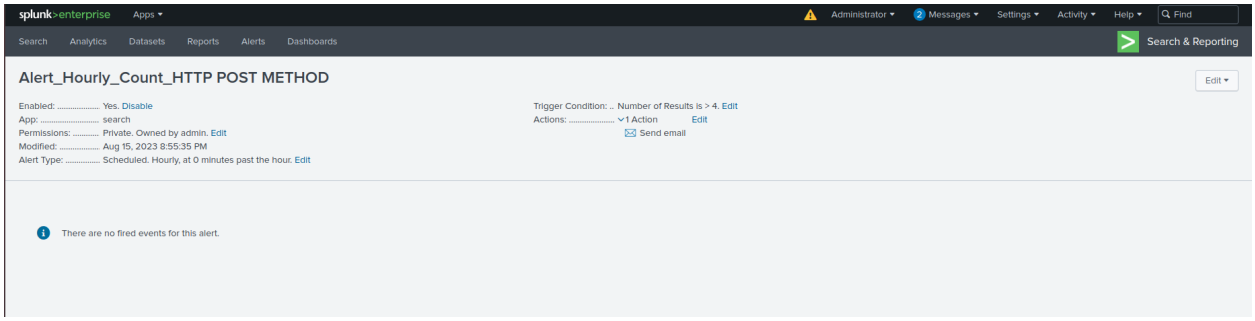

b. Determine an appropriate baseline and threshold for the hourly count of the HTTP POST method.

- Create an alert that's triggered when the threshold has been reached.
- The alert should trigger an email to SOC@VSI-company.com.

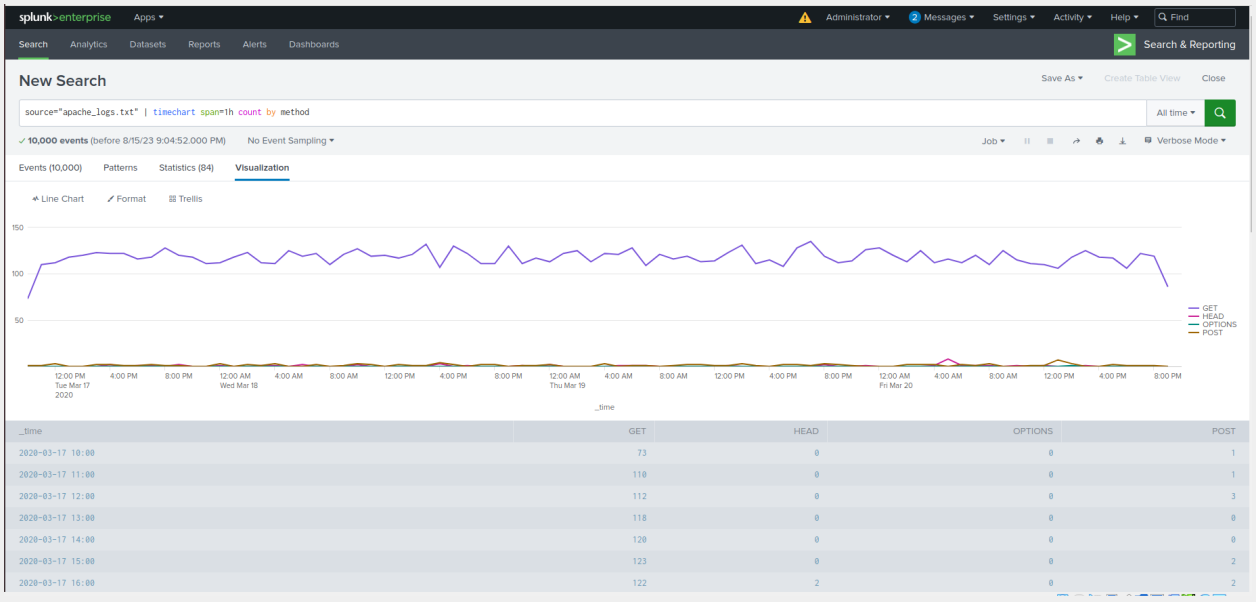


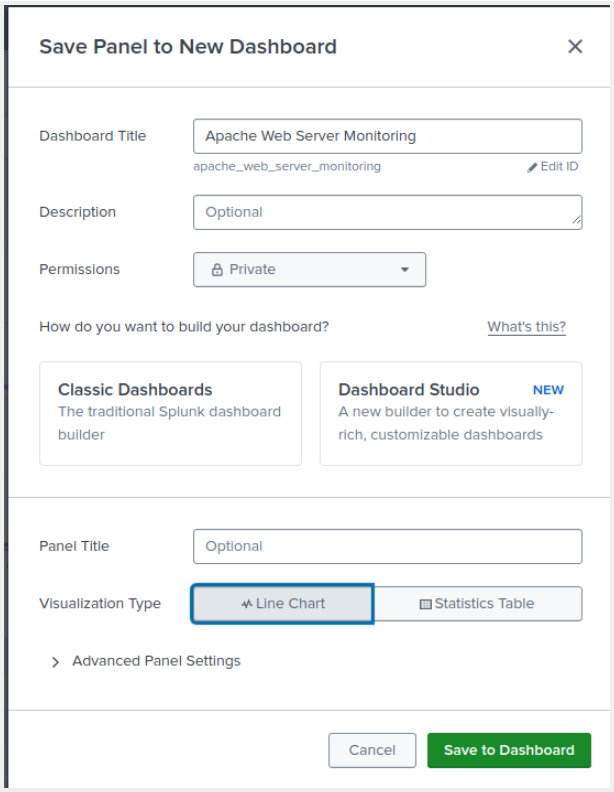


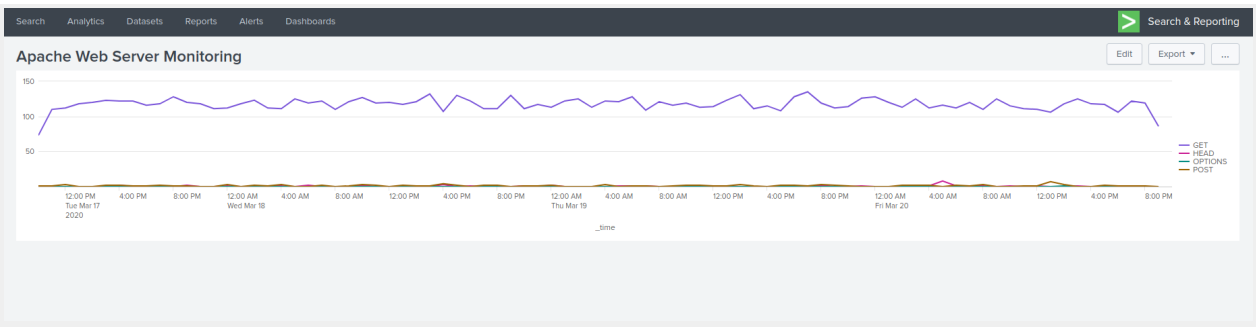



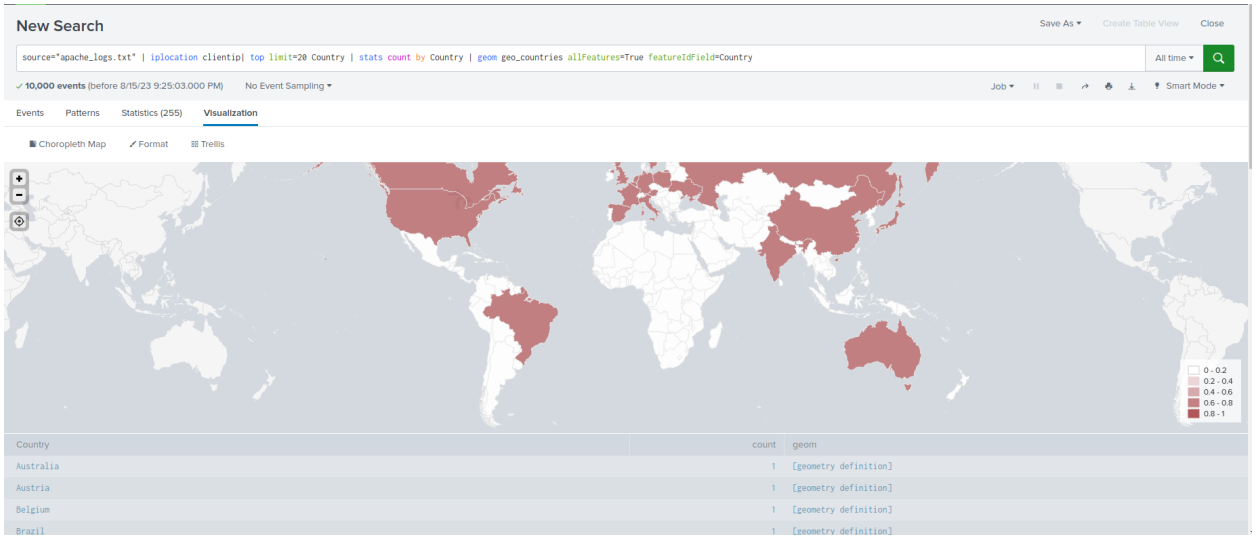

- **Visualizations and dashboards**: Design the following visualizations, and add them to a dashboard called “Apache Web Server Monitoring” (be creative with your visualizations, and make sure to grab screenshots of each):
    a. A line chart that displays the different HTTP “methods” field values over time.
        - **Hint**: Add the following after your search: `timechart span=1h count by method.`

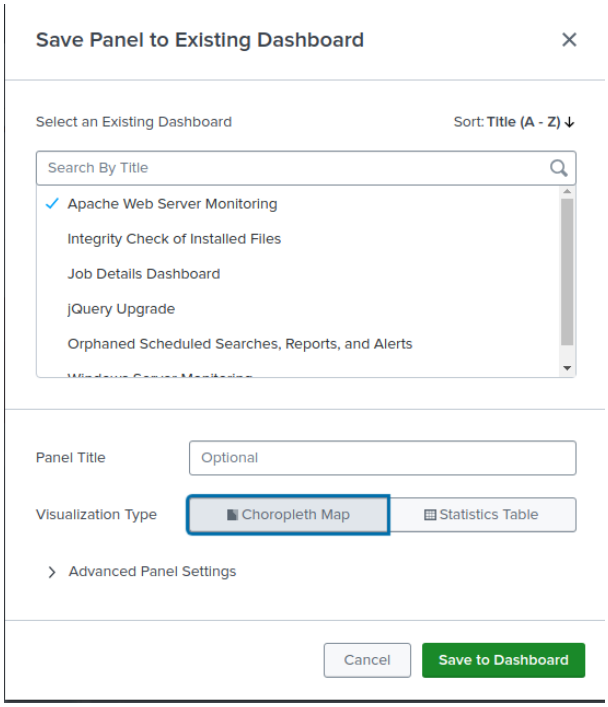

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="apache_logs.txt" | timechart span=1h count by method
All time
10,000 events (before 8/15/23 9:04:52.000 PM)
No Event Sampling
Job
Verbose Mode
Events (10,000)
Patterns
Statistics (84)
Visualization
Line Chart
Format
Trellis
150
100
50
GET
HEAD
OPTIONS
POST
12:00 PM Tue Mar 17 2020
12:00 AM Wed Mar 18
12:00 AM Thu Mar 19
12:00 AM Fri Mar 20
_time
_time
GET
HEAD
OPTIONS
POST
2020-03-17 10:00 73 0 0 1
2020-03-17 11:00 110 0 0 1
2020-03-17 12:00 112 0 0 3
2020-03-17 13:00 118 0 0 0
2020-03-17 14:00 120 0 0 0
2020-03-17 15:00 123 0 0 2
2020-03-17 16:00 122 2 0 2

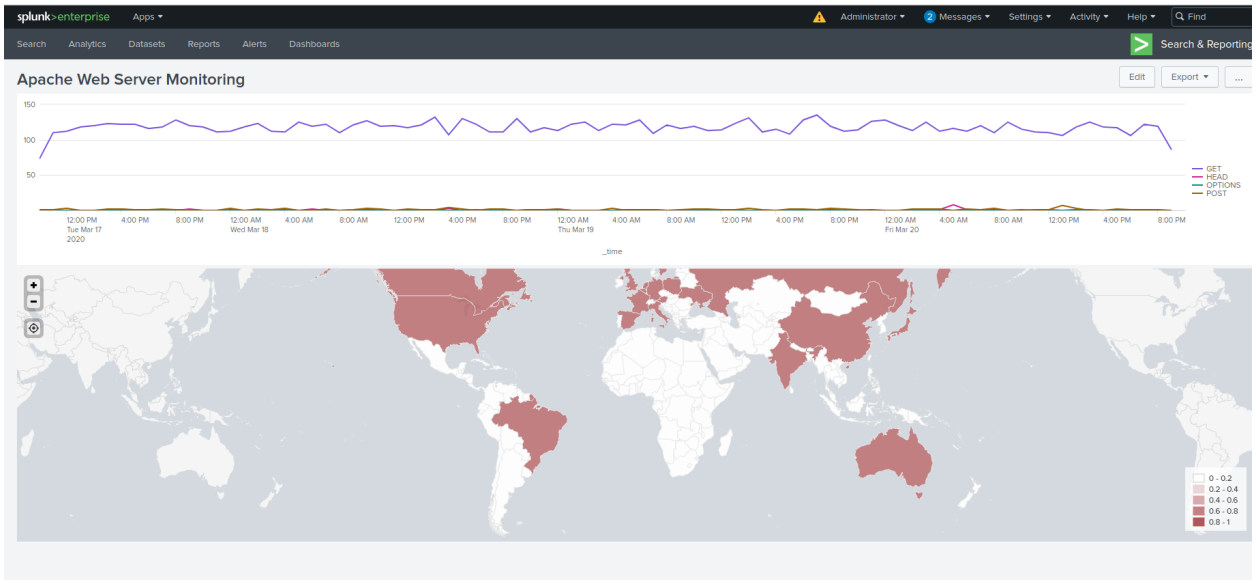

Save Panel to New Dashboard
Dashboard Title
Apache Web Server Monitoring
apache_web_server_monitoring
Edit ID
Description
Optional
Permissions
Private
How do you want to build your dashboard?
What's this?
Classic Dashboards
The traditional Splunk dashboard builder
Dashboard Studio
NEW
A new builder to create visually-rich, customizable dashboards
Panel Title
Optional
Visualization Type
Line Chart
Statistics Table
Advanced Panel Settings
Cancel
Save to Dashboard


Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Apache Web Server Monitoring
Edit
Export
150
100
50
GET
HEAD
OPTIONS
POST
12:00 PM Tue Mar 17 2020
12:00 AM Wed Mar 18
12:00 AM Thu Mar 19
12:00 AM Fri Mar 20
_time

b. A geographical map showing the location based on the “clientip” field.

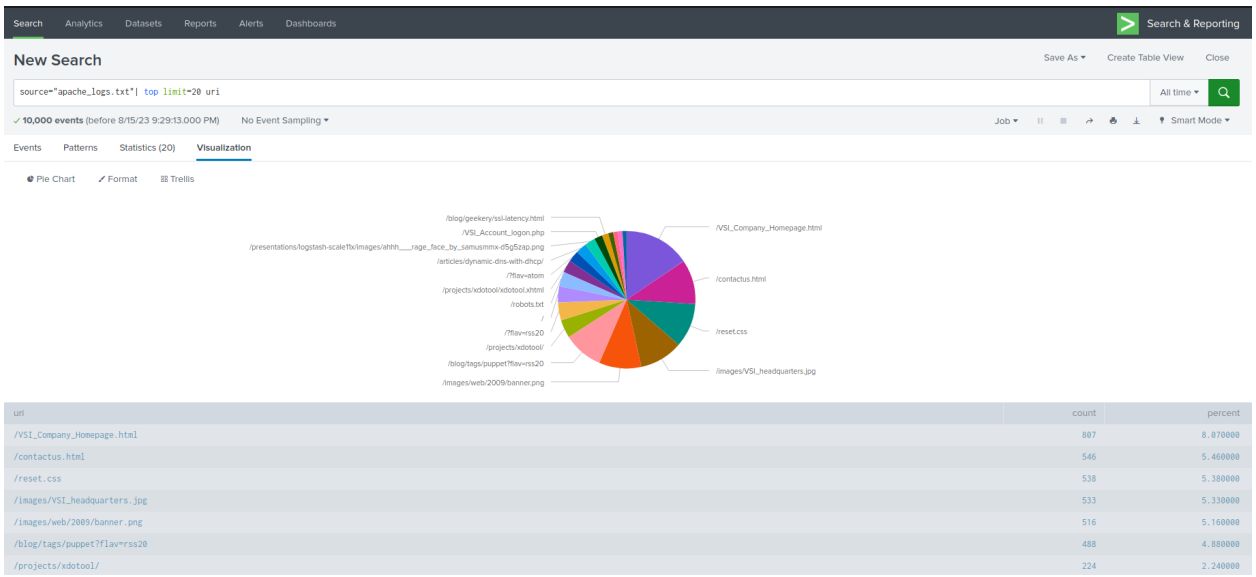


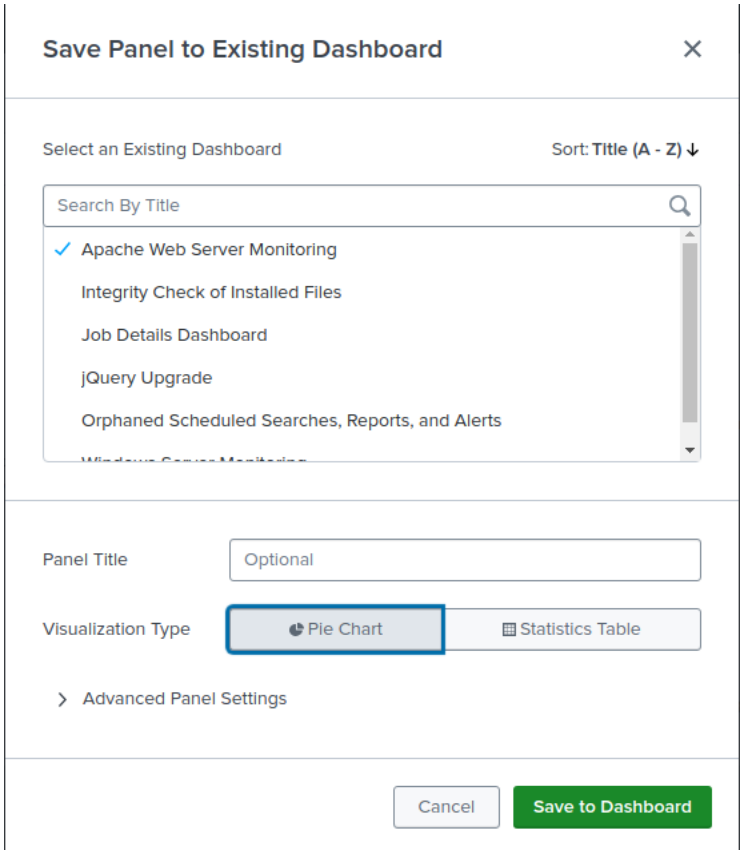



c. Any visualization of your choice that displays the number of different URIs.

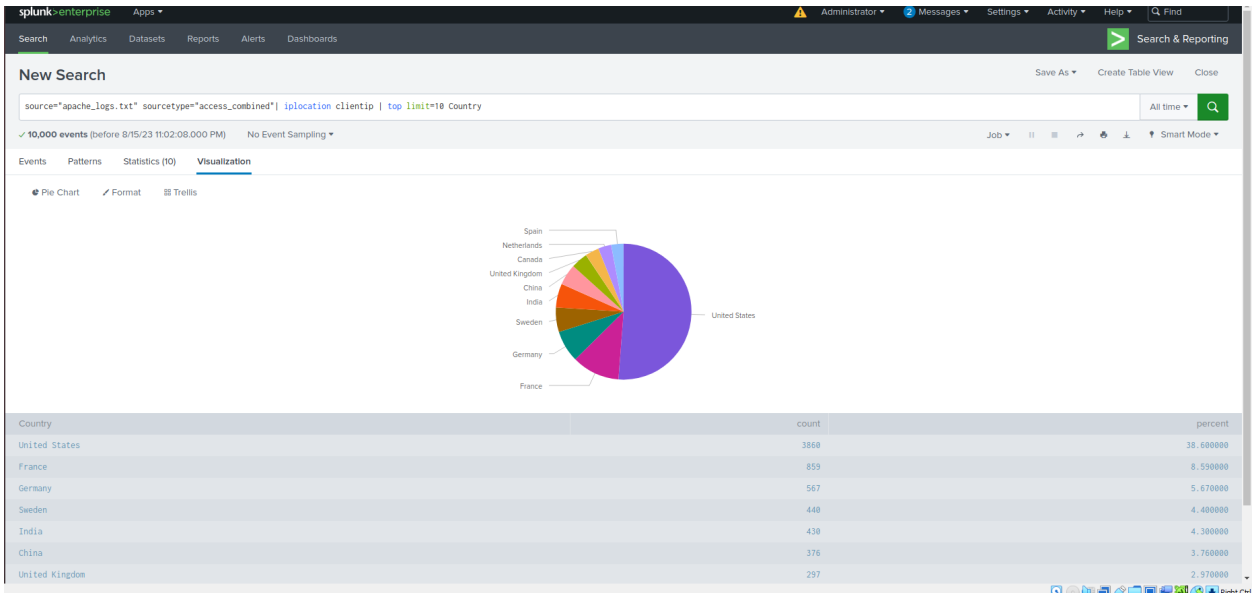
- **Hint**: You can add brand-new custom visualizations by accessing this page inside your VM: Additional Viz.

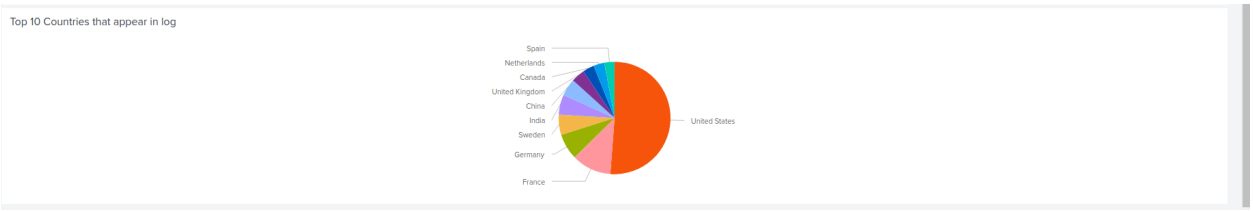



| url | count | percent |
|---|---|---|
| /VSI_Company_Homepage.html | 807 | 8.070000 |
| /contactus.html | 546 | 5.460000 |
| /reset.css | 538 | 5.380000 |
| /images/VSI_headquarters.jpg | 533 | 5.330000 |
| /images/web/2009/banner.png | 516 | 5.160000 |
| /blog/tags/puppet?flav=rss20 | 488 | 4.880000 |
| /projects/xdotool/ | 224 | 2.240000 |

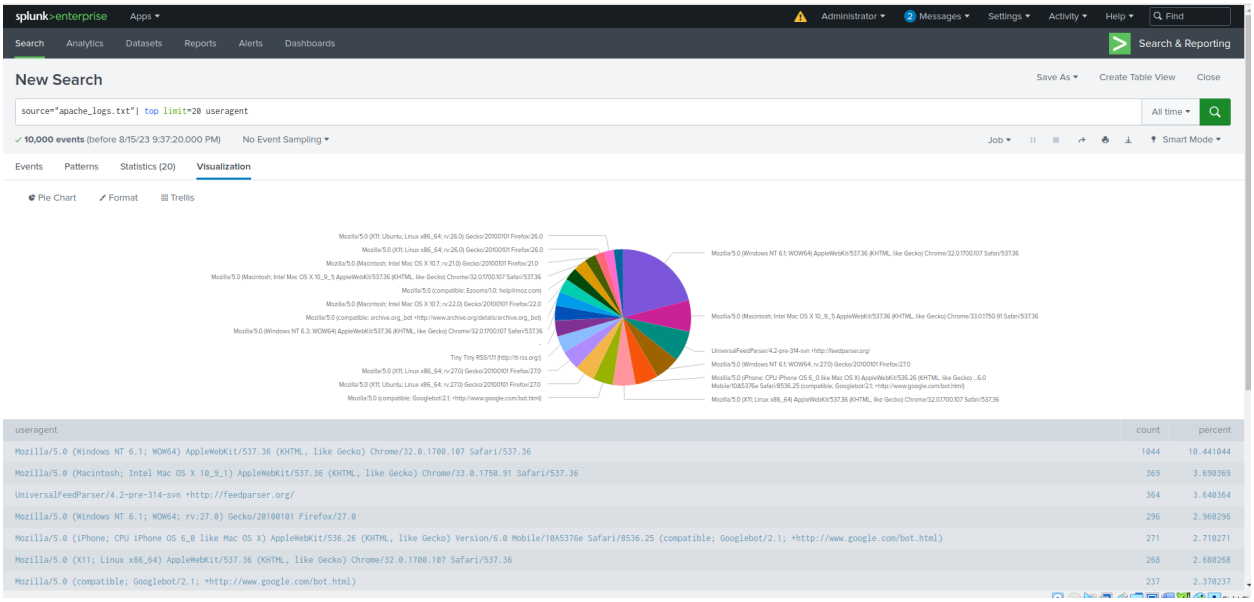


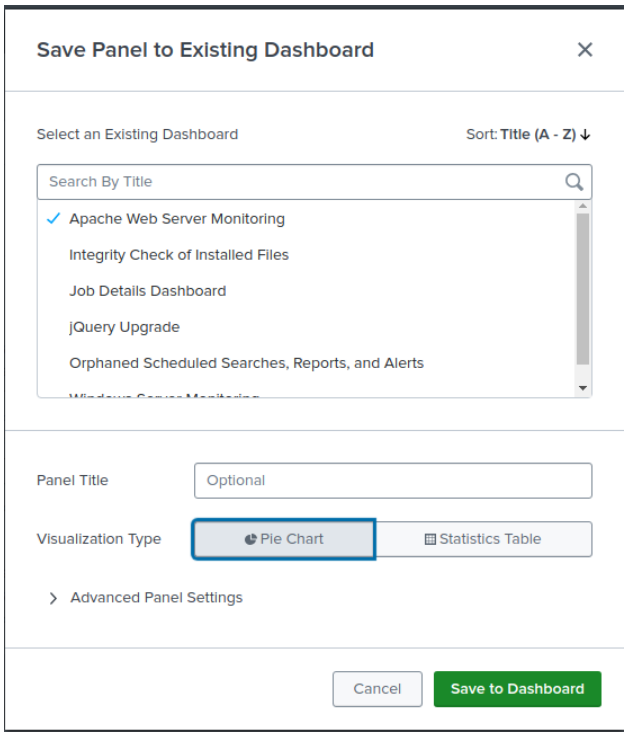

d. Any visualization of your choice that displays the count of the top 10 countries that appear in the log.

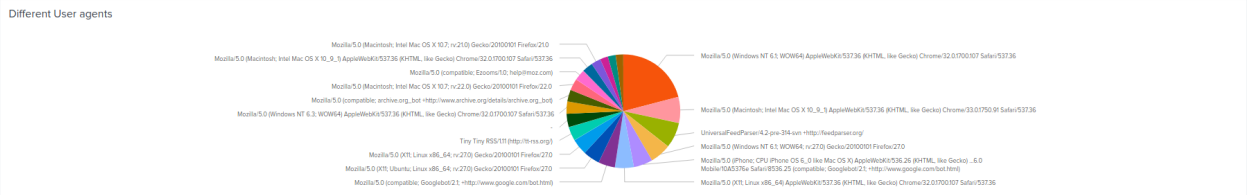




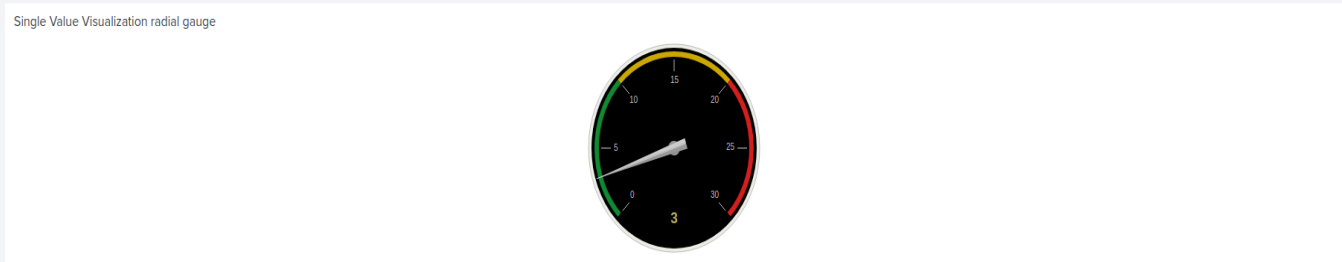

e. Any visualization that illustrates the count of different user agents.



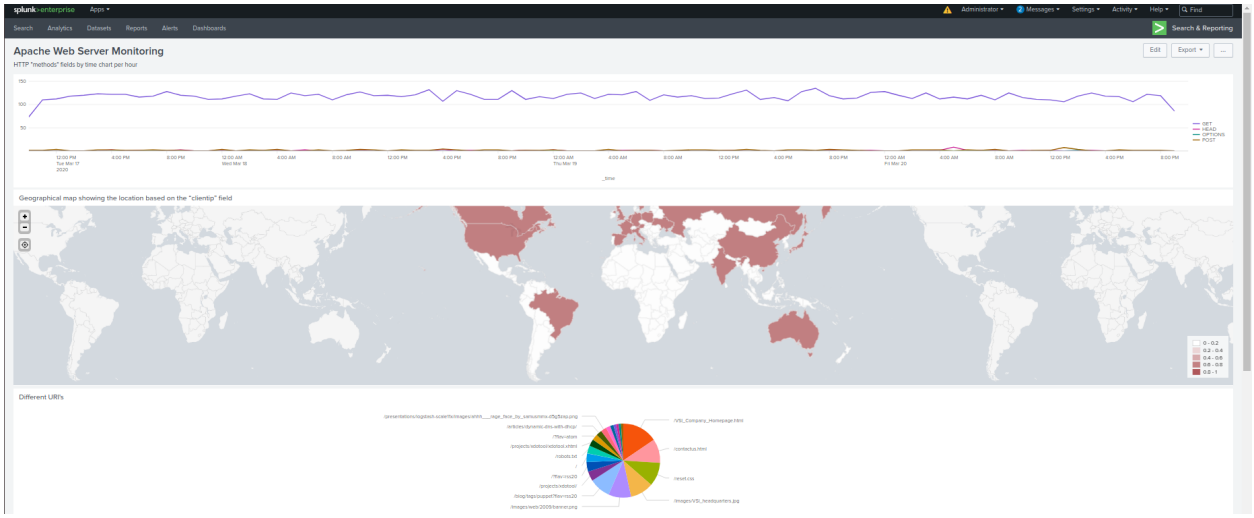



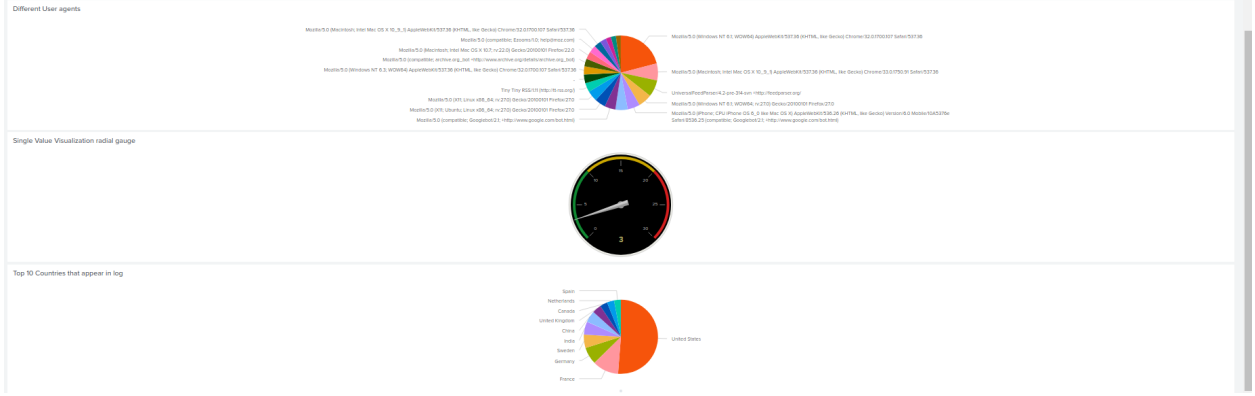



f. A single-value visualization of your choice that analyzes any single data point: e.g., radial gauge, marker gauge, or a custom visualization from http://localhost:8000/en-US/manager/search/appsremote?content=visualizations&type=app).




2. 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.


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Apache Web Server Monitoring
HTTP "methods" fields by time chart per hour
Edit
Export
GET
HEAD
OPTIONS
POST
_time
Geographical map showing the location based on the "clientip" field
0 - 0.2
0.2 - 0.4
0.4 - 0.6
0.6 - 0.8
0.8 - 1
Different URIs
/VSI_Company_Homepage.html
/contactus.html
/reset.css
/images/VSI_headquarters.jpg


Different User agents
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36
UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0


Single Value Visualization radial gauge
3


Top 10 Countries that appear in log
Spain
Netherlands
Canada
United Kingdom
China
India
Sweden
Germany
France
United States