

# **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.

Add Data

Select Source   Set Source Type   Input Settings   Review   Done   < Back   Next >

### Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. [Learn More](#)

Selected File: **windows\_server\_logs.csv**

Select File

Drop your data file here

The maximum file upload size is 500 Mb

Done

### FAQ

- > What kinds of files can the Splunk platform index?
- > What is a source?
- > How do I get remote data onto my Splunk platform instance?

Search | Splunk 5.1.0.1 x Class-A/1951EMS/3/res... x +

localhost:8000/en-US/app/search/search?earliest=&latest=&q=search%20source%3Dwindows\_server\_logs.csv%20host%3D%20&sourceType%3Dcsv&old=1692069458.193&display.page=search.mode=smart&dis...

splunk-enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Q Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

source="windows\_server\_logs.csv" host="86c43b1a654" sourcetype="csv"

4,781 events (before 01/23 3:17:38,000 AM) No Event Sampling ▾

Events [4,781] Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection X Deselect

1 hour per column

1 2 3 4 5 6 7 8 ... Next >

Time	Event
3/24/20 11:59:54,000 PM	2020-03-24T23:59:54.000+0000,,"Domain_A", "user_f", "user_e",.....Account Management.....,ADME-002,.....,4726,A user account was deleted.,.....,Audit Success,.....Security,..,0x305,.....,"A user account was deleted. Subject: Security ID: Domain_A\user_f Show all 63 lines
3/24/20 11:59:53,000 PM	2020-03-24T23:59:53.000+0000,,"Domain_A", "user_f",,2020-03-24 23:59:53 PM,"user_k" "user_h",,server_1/computer_b,.....,Account Management.....,ADME-002,aaa,.....,-,4720,A user account was created.,.....,Audit Success,.....Security,..,All,BMCS,..,"SM Account Name: user_h Display Name: aaa User Principal Name: dd088888.local Show all 137 lines
3/24/20 11:59:48,000 PM	2020-03-24T23:59:48.000+0000,,"Domain_A", "user_f",,server_1/computer_a,.....,Account Management.....,ADME-002,ccc,.....,-,4720,A user account was created.,.....,Audit Success,.....Security,..,All,0x075,..,"SM Account Name: user_k

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

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** Search | Splunk 9.1.0.1 | localhost:8000/en-US/app/search/search?earliest=0&latest=&q=search%20source%3Dwindows\_server\_logs.csv&display.page.search.mode=smart&dispatch.sample\_ratio=1&workload\_pool=&sid=1692121013.546
- Fields Panel:** Shows various fields like member\_nt\_domain, Message, msad\_action, name, object, object\_category, OpCode, privilege\_id, Privilidges, Process\_ID, Process\_Name, product, punct, raw, RecordNumber, Security\_ID, session\_id, severity, signature\_id, SourceName, splunk\_server, src\_nt\_domain, src\_user, src\_user\_watchlist, status, subject, ta\_windows\_action, ta\_windows\_security\_CategoryString, tag, tag20, tag\_action\_2, tag\_eventtype\_17, TaskCategory, time, timeendpos, and timestartpos.
- Signature Card:** Signature ID: Domain\_A\user\_h
- Event Log:** Event timestamp: 2020-03-24T23:57:08.000+0000, Domain\_A, 11:57:08.000 PM, user\_h, user\_e....., Account Management....., ACME-002....., -4743, A computer account was deleted, 0....., Audit Success, Security, 0xA19C, A computer account was deleted.
- Reports:** Top 10 Values (Count %):
  - Special privileges assigned to new logon 342 7.18%
  - A computer account was deleted 340 7.14%
  - A logon was attempted using explicit credentials 333 6.99%
  - Domain Policy was changed 329 6.91%
  - An account was successfully logged on 323 6.78%
  - System security access was removed from an account 320 6.72%
  - A user account was deleted 318 6.68%
  - A privileged service was called 317 6.62%
  - A user account was created 313 6.57%
  - A process has exited 309 6.49%
- Logs:** Shows logs for the same event with type = csv.

## 2. Signature\_id

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** Search | Splunk 9.1.0.1 | localhost:8000/en-US/app/search/search?earliest=0&latest=&q=search%20source%3Dwindows\_server\_logs.csv&display.page.search.mode=smart&dispatch.sample\_ratio=1&workload\_pool=&sid=1692121013.546
- Fields Panel:** Shows various fields like member\_nt\_domain, Message, msad\_action, name, object, object\_category, OpCode, privilege\_id, Privilidges, Process\_ID, Process\_Name, product, punct, raw, RecordNumber, Security\_ID, session\_id, severity, signature\_id, SourceName, splunk\_server, src\_nt\_domain, src\_user, src\_user\_watchlist, status, subject, ta\_windows\_action, ta\_windows\_security\_CategoryString, tag, tag20, tag\_action\_2, tag\_eventtype\_17, TaskCategory, time, timeendpos, and timestartpos.
- Signature ID Card:** Signature ID: Domain\_A\user\_h
- Event Log:** Event timestamp: 2020-03-24T23:57:08.000+0000, Domain\_A, 11:57:08.000 PM, user\_h, user\_e....., Account Management....., ACME-002....., -4743, A computer account was deleted, 0....., Audit Success, Security, 0xA19C, A computer account was deleted.
- Reports:** Top 10 Values (Avg: 4475.150063051702 Min: 1102 Max: 4743 Std Dev: 880.5020109145164):
  - 4672 342 7.18%
  - 4743 348 7.14%
  - 4648 333 6.99%
  - 4739 329 6.91%
  - 4624 323 6.78%
  - 4718 320 6.72%
  - 4726 318 6.68%
  - 4673 317 6.61%
  - 4720 313 6.57%
  - 4689 309 6.49%
- Logs:** Shows logs for the same event with type = csv.

## 3. users

localhost:8000/en-US/app/search/search?earliest=0&latest=&q=search%20source%3D"windows\_server\_logs.csv"&display.page.search.mode=smart&dispatch.sample\_ratio=1&workload\_pool=&

Hide Fields	All Fields	List	Format	20 Per Page	
<a href="#">OpCode</a> 1 <a href="#">privilege_id</a> 16 <a href="#">Privileges</a> 13 <a href="#">Process_ID</a> 100+ <a href="#">Process_Name</a> 100+ <a href="#">product</a> 1 <a href="#">punct</a> 27 <a href="#">raw</a> 100+ # RecordNumber 100+ <a href="#">Security_ID</a> 100+ <a href="#">session_id</a> 17 <a href="#">severity</a> 2 # severity_id 2 <a href="#">signature</a> 15 # signature_id 16 <a href="#">SourceName</a> 2 <a href="#">splunk_server</a> 1 <a href="#">src_nt_domain</a> 16 <a href="#">src_user</a> 15 <a href="#">src_user_watchlist</a> 1 <a href="#">status</a> 3 <a href="#">subject</a> 16 <a href="#">ta_windows_action</a> 1 <a href="#">ta_windows_security_CategoryString</a> 2 <a href="#">tag</a> 20 <a href="#">tag_action</a> 2 <a href="#">tag_eventtype</a> 17 <a href="#">TaskCategory</a> 8 <a href="#">time</a> 100+ <a href="#">timeendpos</a> 4 <a href="#">timestartpos</a> 3 <a href="#">Type</a> 1 <a href="#">user</a> 100+ <a href="#">user_watchlist</a> 1 <a href="#">vendor</a> 1 <a href="#">vendor_privilege</a> 14		<b>i</b> Time Event host = 86c43b1a6654   source = windows_server_logs.csv   sourcetype = csv > 3/24/20 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 account's password,0\....., 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 2020-03-24T23:56:40.000+0000,SeRemoteInteractiveLogonRight,Domain_A,,ACME-002 Domain_A\user_b\.....,ACME-002\.....,-4717,System security access was granted to an account,0\....., Audi			
<b>user</b> >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_1 353 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%					
109 more fields + Extract New Fields					

## 4. Status

localhost:8000/en-US/app/search/search?earliest=0&latest=&q=search%20source%3D"windows\_server\_logs.csv"&display.page.search.mode=smart&dispatch.sample\_ratio=1&workload\_pool=&sid=1692121013.546

Hide Fields	All Fields	List	Format	20 Per Page	
<a href="#">OpCode</a> 1 <a href="#">privilege_id</a> 16 <a href="#">Privileges</a> 13 <a href="#">Process_ID</a> 100+ <a href="#">Process_Name</a> 10 <a href="#">product</a> 1 <a href="#">punct</a> 27 <a href="#">raw</a> 100+ # RecordNumber 100+ <a href="#">Security_ID</a> 100+ <a href="#">session_id</a> 17 <a href="#">severity</a> 2 # severity_id 2 <a href="#">signature</a> 15 # signature_id 16 <a href="#">SourceName</a> 2 <a href="#">splunk_server</a> 1 <a href="#">src_nt_domain</a> 16 <a href="#">src_user</a> 15 <a href="#">src_user_watchlist</a> 1 <a href="#">status</a> 3 <a href="#">subject</a> 16 <a href="#">ta_windows_action</a> 1 <a href="#">ta_windows_security_CategoryString</a> 2 <a href="#">tag</a> 20 <a href="#">tag_action</a> 2 <a href="#">tag_eventtype</a> 17 <a href="#">TaskCategory</a> 8 <a href="#">time</a> 100+ <a href="#">timeendpos</a> 4 <a href="#">timestartpos</a> 3 <a href="#">Type</a> 1 <a href="#">user</a> 100+ <a href="#">user_watchlist</a> 1 <a href="#">vendor</a> 1 <a href="#">vendor_privilege</a> 14		<b>i</b> Time Event host = 86c43b1a6654   source = windows_server_logs.csv   sourcetype = csv > 3/24/20 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 account's 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 2020-03-24T23:56:40.000+0000,SeRemoteInteractiveLogonRight,Domain_A,,ACME-002 System security access was granted to an account,0\....., Audit Success\.....,Security\.....,0x3A81\.....,"System security access w			
<b>status</b> 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%					
host = 86c43b1a6654   source = windows_server_logs.csv   sourcetype = csv > 3/24/20 2020-03-24T23:55:55.000+0000,.domain_A,,user_j\.....,ACME-002\.....,-4672,Special privileges assigned to new logon,0\....., Audit Success\.....,Security\.....,0xB111\.....,"Special privileges assigned to new logon. Subject: Security ID: Domain_A\user_j Account Name: user_j Account Domain: Domain_A Show all 83 lines host = 86c43b1a6654   source = windows_server_logs.csv   sourcetype = csv > 3/24/20 2020-03-24T23:54:46.000+0000,.domain_A,,user_f\.....,ACME-002\.....,-4673,A privileged service was called,0\....., Audit Success\.....,Security\.....,0xA369\.....,"A privilege					
109 more fields + Extract New Fields					

## 5. Severity

The screenshot shows a Splunk search interface with multiple tabs at the top: Dashboards, Search, Class-A/19-SIEMs/3/resources, and Splunk Apps Browser. The main area displays a search result for 'windows\_server\_logs.csv' with 20 events per page. A modal window is open over the results, titled 'severity'. It shows '2 Values, 99.937% of events' with 'Selected Yes' checked. Below this, there are three tabs: 'Top values', 'Top values by time', and 'Rare values'. The 'Top values' tab is selected, showing two rows: 'informational' with a count of 4,429 (93.085%) and 'high' with a count of 329 (6.915%). At the bottom of the modal, there are buttons for 'Show all 83 lines' and 'Show all 57 lines'.

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)

signature	signature_id
A user account was deleted	4726
A user account was created	4728
A computer account was deleted	4743
An account was successfully logged on	4624
Special privileges assigned to new logon	4672
An attempt was made to reset an accounts password	4724
System security access was granted to an account	4717
A privileged service was called	4673
A logon was attempted using explicit credentials	4648
A user account was locked out	4740
Domain Policy was changed	4739
A user account was changed	4738
A process has exited	4689
The audit log was cleared	1102
System security access was removed from an account	4718

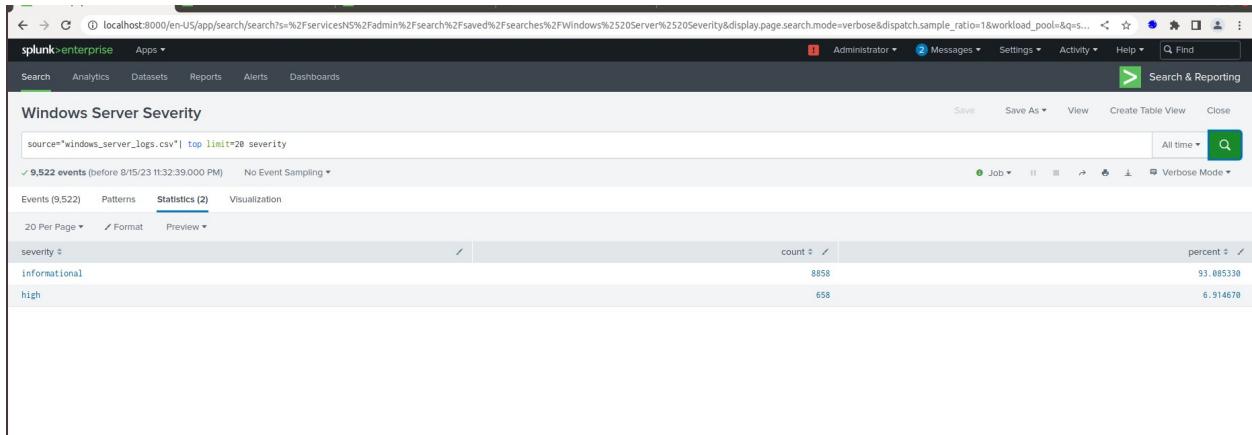
(Report Signature with Signature\_id created )

signature	signature_id
A user account was deleted	4726
A user account was created	4728
A computer account was deleted	4743
An account was successfully logged on	4624
Special privileges assigned to new logon	4672
An attempt was made to reset an accounts password	4724
System security access was granted to an account	4717
A privileged service was called	4673
A logon was attempted using explicit credentials	4648
A user account was locked out	4740
Domain Policy was changed	4739
A user account was changed	4738
A process has exited	4689
The audit log was cleared	1102
System security access was removed from an account	4718

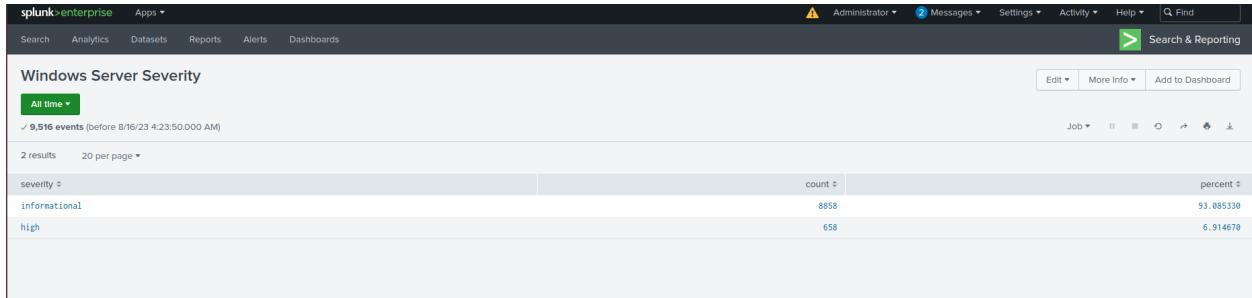
- A report that displays the severity levels, and the count and percentage of each.

- 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)



- o 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.

**New Search**

source="windows\_server\_logs.csv" | top limit=20 status

✓ 4,761 events (before 8/15/23 4:31:33.000 AM) No Event Sampling ▾

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**

source="windows\_server\_logs.csv" status=failure

✓ 142 events (before 8/15/23 4:39:22.000 AM) No Event Sampling ▾

Events (142) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 hour per column

List ▾ Format 20 Per Page ▾

◀ Hide Fields ▶ All Fields

Time	Event
3/24/20 11:56:41:000 PM	2020-03-24T23:56:41.000+0000,,Domain_A user,_A,,user,_a user,_d,,Account Management,,ADHE-002,,,-4724,An attempt was made to reset an account's password.,,,Audit Failure,,,Security,,,0x6C10,,,"An attempt was made to reset an account's password. Subject: Security ID: Domain_Auser_a Show all 61 lines host= 86c4301a6654   source = windows_server_logs.csv   sourcetype = csv
3/24/20 11:34:35.000 PM	2020-03-24T23:34:35.000+0000,,Domain_A user,_A,,user,_B user,_1,,Account Management,,ADHE-002,,,-4724,An attempt was made to reset an account's password.,,,Audit Failure,,,Security,,,0x468A,,,"An attempt was made to reset an account's password. Subject: Security ID: Domain_Auser_m Show all 61 lines host= 86c4301a6654   source = windows_server_logs.csv   sourcetype = csv
3/24/20 2020-03-24T23:30:24.000+0000,,Domain_A	

◀ Prev 1 2 3 4 5 6 7 8 Next ▾

**New Search**

source="windows\_server\_logs.csv" | top limit=20 status

✓ 4,761 events (before 8/15/23 4:31:33.000 AM) No Event Sampling ▾

Events (4,761) Patterns Statistics (3) **Visualization**

Bar Chart ▾ Format Trellis ▾

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)



**Failed Activities windows server log**

Enabled: Yes. Disable  
App: search  
Permissions: Private. Owned by admin, Edit  
Modified: Aug 16, 2023 12:00:10 AM  
Alert Type: Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: Number of Results is > 6. Edit  
Actions: 1 Action Edit  
Send email

There are no fired events for this alert.

- 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](mailto: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”)

New Search

source="windows\_server\_logs.csv" signature="An account was successfully logged on" signature\_id=4624

✓ 646 events (before 8/16/23 4:47:44.000 AM) No Event Sampling

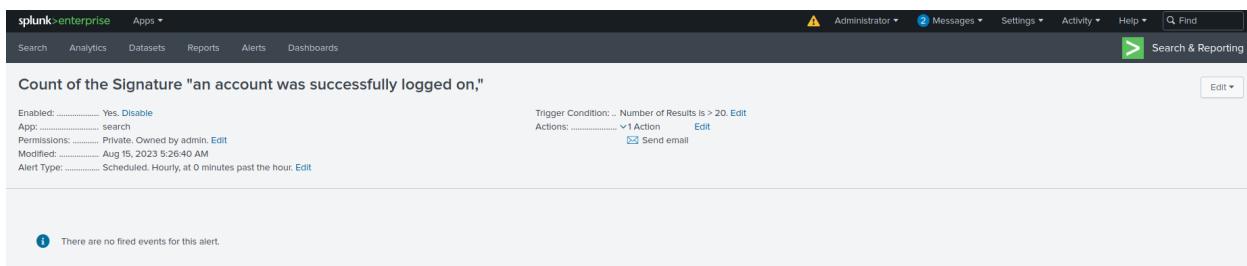
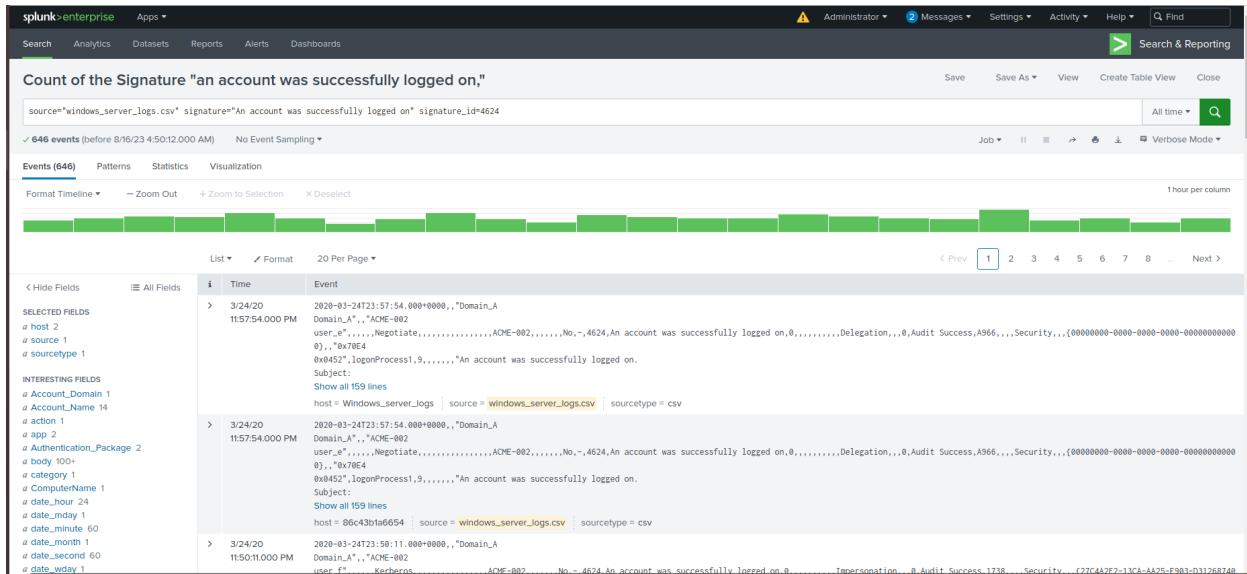
Events (646) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection X Deselect

1 hour per column

Time	Event
3/24/20 11:57:54:000 PM	2020-03-24T23:57:54.000+0000,,Domain_A user_e\.....,ACME-002,.....,No,-,4624,An account was successfully logged on.0.,.....,Delegation,,0,Audit Success,A966,,,Security,,,(00000000-0000-0000-0000-000000000000 0),,0x70E4 0x452*,logonProcess1,9,.....,"An account was successfully logged on. Subject: Show all 159 lines host = Windows_server_logs   source = windows_server_logs.csv   sourcetype = csv
3/24/20 11:57:54:000 PM	2020-03-24T23:57:54.000+0000,,Domain_A user_e\.....,ACME-002,.....,No,-,4624,An account was successfully logged on.0.,.....,Delegation,,0,Audit Success,A966,,,Security,,,(00000000-0000-0000-0000-000000000000 0),,0x70E4 0x452*,logonProcess1,9,.....,"An account was successfully logged on. Subject: Show all 159 lines host = 86c43bfa654   source = windows_server_logs.csv   sourcetype = csv
3/24/20 11:50:11:000 PM	2020-03-24T23:50:11.000+0000,,Domain_A user_e\.....,ACME-002,.....,No,-,4624,An account was successfully logged on.0.,.....,Impersonation,,0,Audit Success,1738,,,Security,,,(27C4A2F2-13CA-AA25-E983-031268740 0),,0x452*,Kerberos,.....,"An account was successfully logged on.0.,.....,Impersonation,,0,Audit Success,1738,,,Security,,,(27C4A2F2-13CA-AA25-E983-031268740

(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](mailto:SOC@VSI-company.com).

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

**New Search**

source="windows\_server\_logs.csv" signature="A user account was deleted" signature\_id=4726

636 events (before 8/16/23 5:02:06.000 AM) No Event Sampling

Events (636) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection X Deselect

1 hour per column

List ✓ Format 20 Per Page ▾

Time	Event
3/24/20 11:59:54.000 PM	2020-03-24T23:59:54.000+0000,,Domain_A Domain_A,"user_f user_1",.....,Account Management,.....,ACME-002,.....,-4726,A user account was deleted.0,.....,Audit Success,....,Security,....,0xA369,.....,"A user account was deleted. Subject: Security ID: Domain_A\user_f Show all 63 lines host = Windows_server_logs   source = windows_server_logs.csv   sourcetype = csv
3/24/20 11:59:54.000 PM	2020-03-24T23:59:54.000+0000,,Domain_A Domain_A,"user_f user_1",.....,Account Management,.....,ACME-002,.....,-4726,A user account was deleted.0,.....,Audit Success,....,Security,....,0xA369,.....,"A user account was deleted. Subject: Security ID: Domain_A\user_f Show all 63 lines host = 86c43ba6654   source = windows_server_logs.csv   sourcetype = csv
3/24/20 11:51:52.000 PM	2020-03-24T23:51:52.000+0000,,Domain_A Domain_A,"user_n user_m",.....,Account Management,.....,ACME-002,.....,-4726,A user account was deleted.0,.....,Audit Success,....,Security,....,0x4076,.....,"A user account was deleted. Subject:

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

**Alert\_signature\_a user account was deleted."**

source="windows\_server\_logs.csv" signature="A user account was deleted" signature\_id=4726

636 events (before 8/16/23 5:07:59.000 AM) No Event Sampling

Events (636) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection X Deselect

1 hour per column

List ✓ Format 20 Per Page ▾

Time	Event
3/24/20 11:59:54.000 PM	2020-03-24T23:59:54.000+0000,,Domain_A Domain_A,"user_f user_1",.....,Account Management,.....,ACME-002,.....,-4726,A user account was deleted.0,.....,Audit Success,....,Security,....,0xA369,.....,"A user account was deleted. Subject: Security ID: Domain_A\user_f Show all 63 lines host = Windows_server_logs   source = windows_server_logs.csv   sourcetype = csv
3/24/20 11:59:54.000 PM	2020-03-24T23:59:54.000+0000,,Domain_A Domain_A,"user_f user_1",.....,Account Management,.....,ACME-002,.....,-4726,A user account was deleted.0,.....,Audit Success,....,Security,....,0xA369,.....,"A user account was deleted. Subject: Security ID: Domain_A\user_f Show all 63 lines host = 86c43ba6654   source = windows_server_logs.csv   sourcetype = csv
3/24/20 11:51:52.000 PM	2020-03-24T23:51:52.000+0000,,Domain_A Domain_A,"user_n user_m",.....,Account Management,.....,ACME-002,.....,-4726,A user account was deleted.0,.....,Audit Success,....,Security,....,0x4076,.....,"A user account was deleted. Subject:

The screenshot shows the Splunk interface with two main windows. The top window is a modal titled "Save As Alert" containing configuration fields for an alert. The bottom window shows the alert's details on the "Alerts" page.

**Save As Alert Dialog Fields:**

- Settings**
  - Title: Alert\_signature\_a user account was deleted."
  - Description: Optional
  - Permissions: Private (selected)
  - Alert type: Scheduled (selected)
  - Run every hour ▾
  - At: 0 minutes past the hour
  - Expires: 24 hour(s) ▾
- Trigger Conditions**
  - Trigger alert when: Number of Results ▾
  - is greater than ▾: 35
  - Trigger: Once For each result
  - Throttle?
- Trigger Actions**
  - + Add Actions ▾

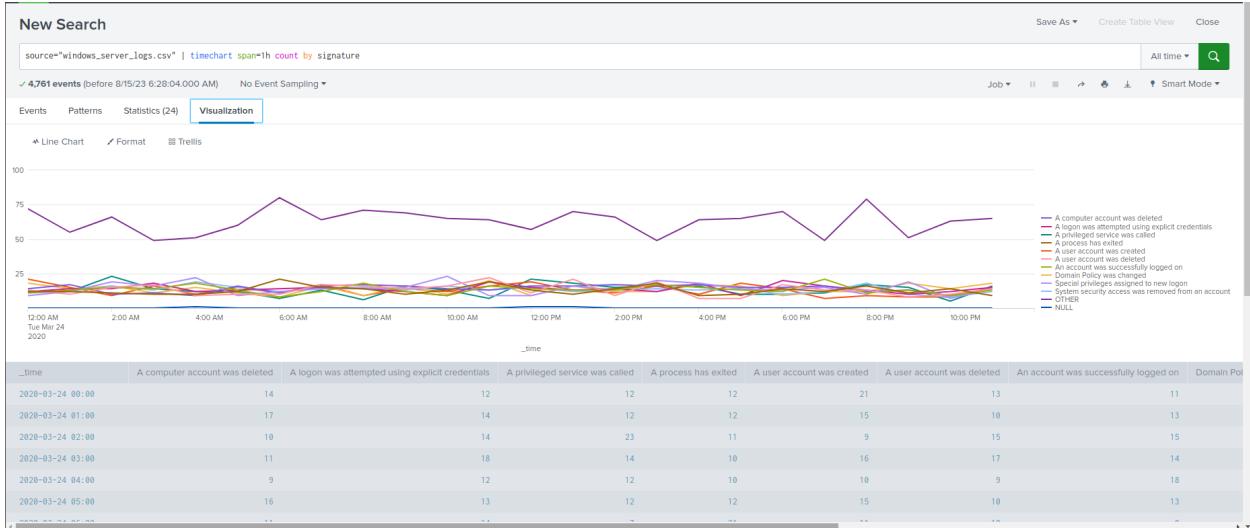
**Alert Configuration Page Details:**

- Alert Name:** Alert\_signature\_a user account was deleted."
- Enabled:** Yes, Disable
- App:** search
- Permissions:** Private. Owned by admin. [Edit](#)
- Modified:** Aug 16, 2023 5:06:01 AM
- Alert Type:** Scheduled. Hourly, at 0 minutes past the hour. [Edit](#)
- Trigger Condition:** Number of Results is > 35. [Edit](#)
- Actions:** 1 Action [Edit](#)
- Action:** Send email

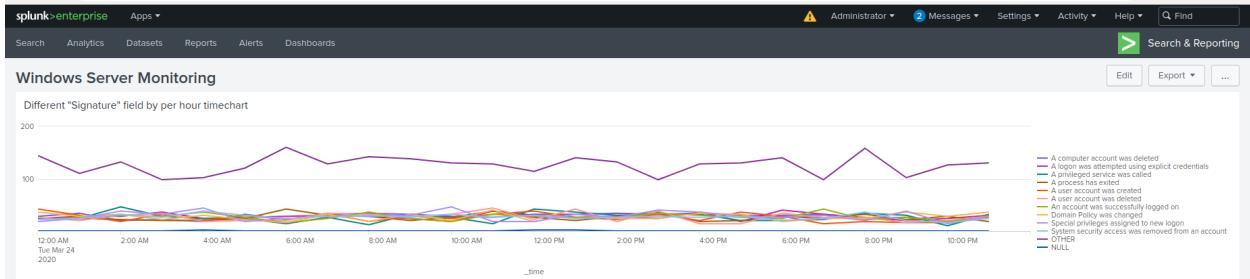
**Note:** There are no fired events for this alert.

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)



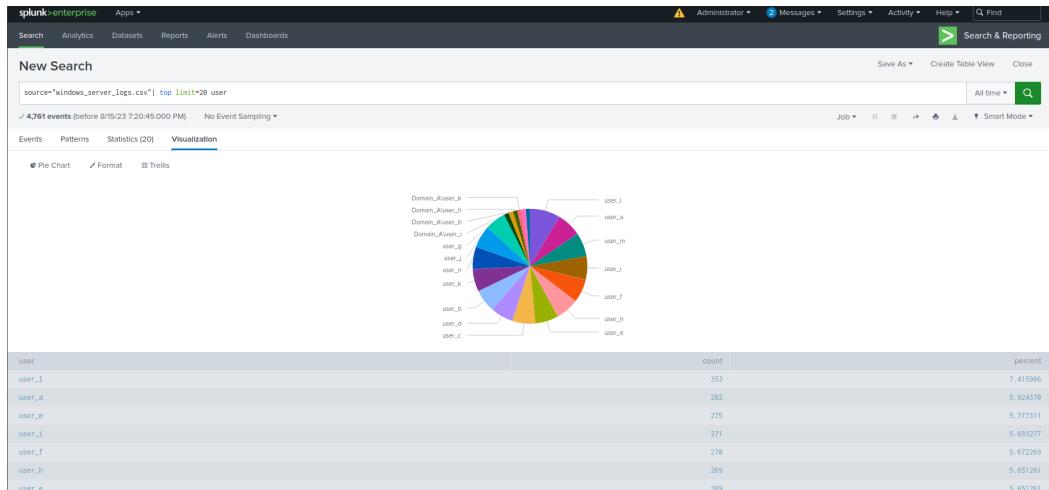
(New Dashboard created with the Different “Signature” field by per hour in the Line chart Visualization)



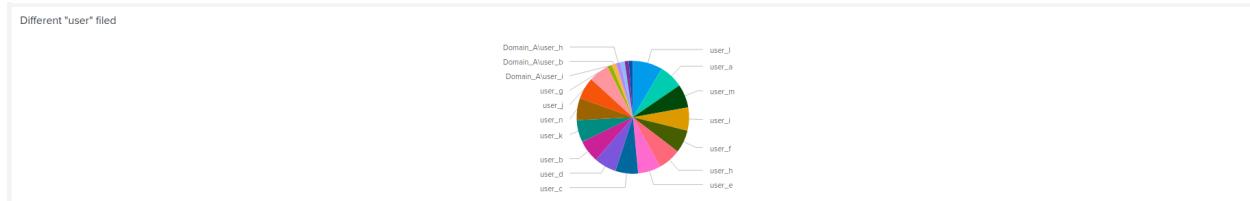
- A line chart that displays the different “user” field values over time.

a. Take a screenshot of the chart.

(Search for the different “user” field)

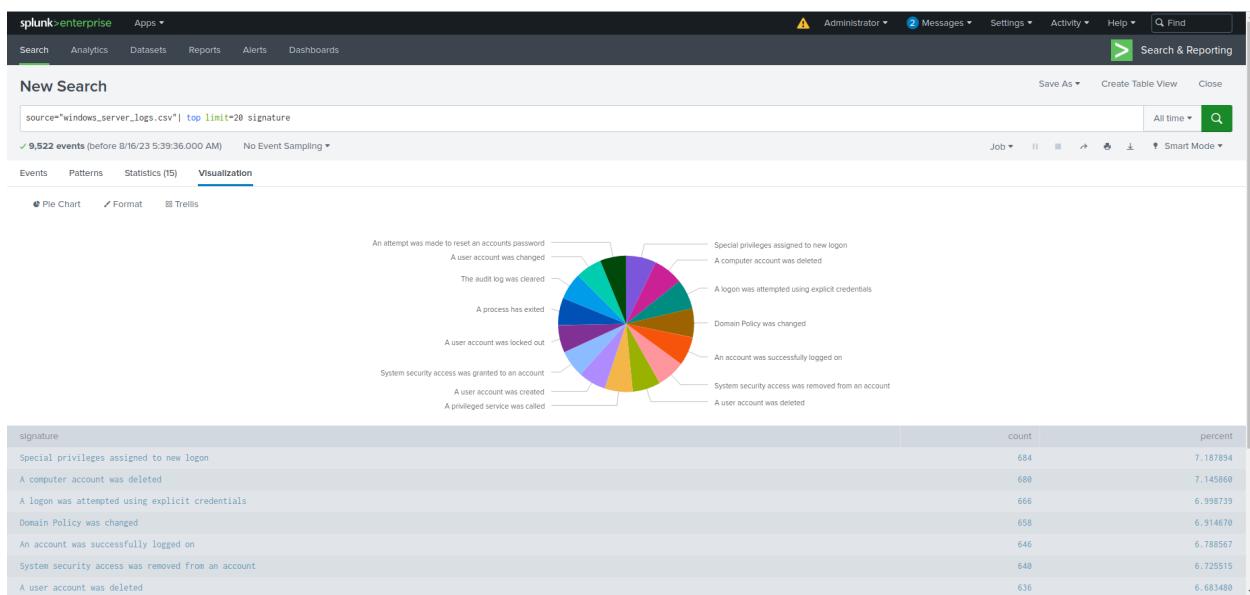


(Panel added to existing Windows Server Monitoring Dashboard with name Different “user”)



- 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”)

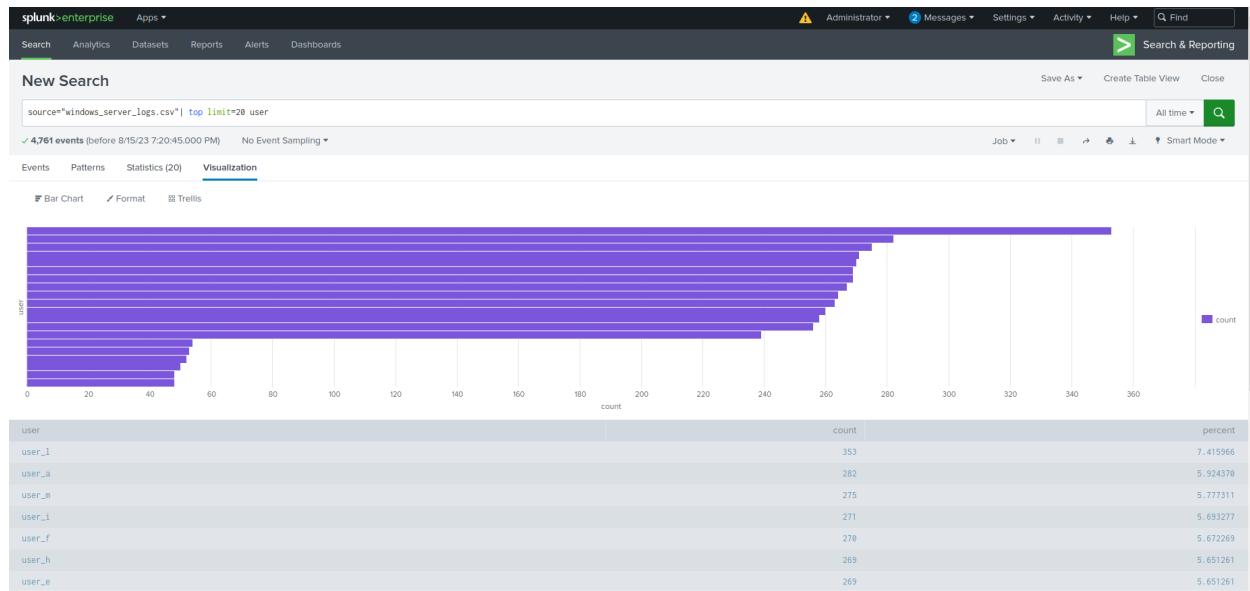


(Panel added to existing Windows Server Monitoring Dashboard)



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

(Search for the different users)



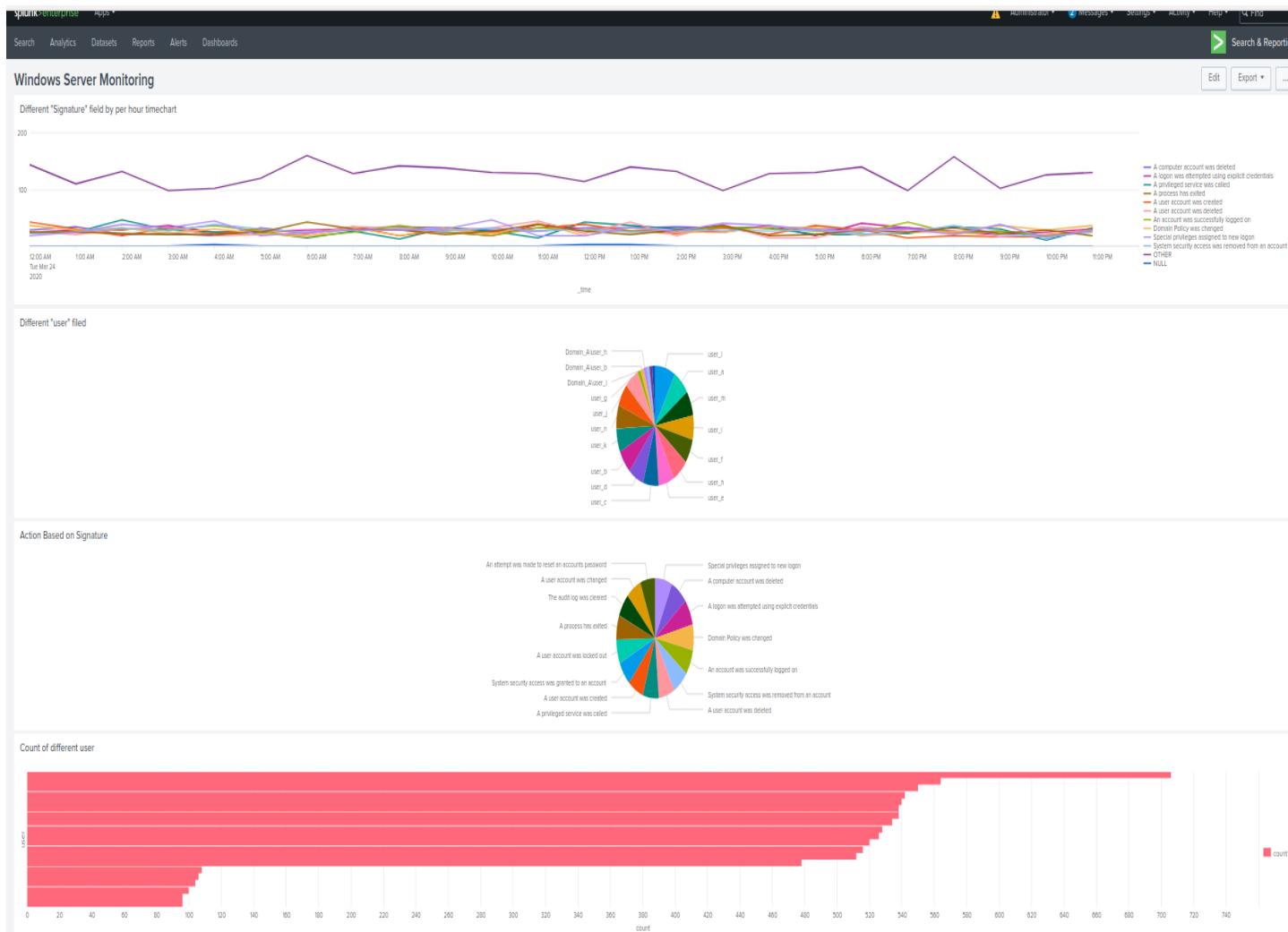
(Panel added to existing Windows Server Monitoring Dashboard)

- 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.”

The screenshot shows the Splunk Enterprise search interface. At the top, there's a navigation bar with links for Apps, Search, Analytics, Datasets, Reports, Alerts, and Dashboards. Below the search bar, it says "10,000 events (before 8/15/23 7:40:31.000 PM) No Event Sampling". The search bar contains the query "source=apache\_logs.txt". The results table shows several log entries from March 2020. The first few entries are:

Time	Event
3/20/20 9:05:59.000 PM	5.10.83.53 - [20/Mar/2020:21:05:59 +0000] "GET /files/grok/TcN;O+A HTTP/1.1" 200 3894 "-" "Mozilla/5.0 (compatible; AhrefsBot/5.0; +http://ahrefs.com/robot/)" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined
3/20/20 9:05:59.000 PM	66.249.73.135 - [20/Mar/2020:21:05:59 +0000] "GET /blog/tags/wine HTTP/1.1" 200 10021 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6.0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A537f Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined
3/20/20 9:05:58.000 PM	63.149.98.88 - [20/Mar/2020:21:05:58 +0000] "GET /images/VISI_headquarters.jpg HTTP/1.1" 200 6146 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined
3/20/20 9:05:57.000 PM	38.99.236.50 - [20/Mar/2020:21:05:57 +0000] "GET /presentations/logstash-puppetconf-2012/images/frontend-response-codes.png HTTP/1.1" 200 52878 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined
3/20/20 9:05:57.000 PM	63.149.98.88 - [20/Mar/2020:21:05:57 +0000] "GET /presentations/logstash-puppetconf-2012/css/reset.css HTTP/1.1" 200 1382 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined
3/20/20 9:05:56.000 PM	188.76.6.56 - [20/Mar/2020:21:05:56 +0000] "GET /robots.txt HTTP/1.1" 200 "-" "Mozilla/5.0 (Windows NT 5.1; rv:6.0.2) Gecko/20100101 Firefox/6.0.2" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined

**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

Time	Event
3/20/20 09:05:59:000 PM	5.10.83.53 - - [20/Mar/2020:21:05:59 +0000] "GET /files/grok/?Cn;O/A HTTP/1.1" 200 3894 "-" "Mozilla/5.0 (compatible; AhrefsBot/5.0; +http://ahrefs.com/robot)" host = "Apache_Logs" ; source = apache_logs.txt ; sourcetype = access_combined
3/20/20 09:05:59:000 PM	66.249.73.135 - - [20/Mar/2020:21:05:59 +0000] "GET /blog/tags/wine HTTP/1.1" 200 10021 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A537e Safari/6536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)" host = "Apache_Logs" ; source = apache_logs.txt ; sourcetype = access_combined
3/20/20 09:05:58:000 PM	63.140.98.80 - - [20/Mar/2020:21:05:58 +0000] "GET /images/VSI_headquarters.jpg HTTP/1.1" 200 6146 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36" host = "Apache_Logs" ; source = apache_logs.txt ; sourcetype = access_combined
3/20/20 09:05:57:000 PM	38.99.236.50 - - [20/Mar/2020:21:05:57 +0000] "GET /presentations/logstash-puppetconf-2012/images/frontend-response-codes.png HTTP/1.1" 200 52878 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36" host = "Apache_Logs" ; source = apache_logs.txt ; sourcetype = access_combined

**method**

4 Values, 100% of events Selected Yes No

**Reports**

Top values Top values by time Rare values

Events with this field

Values	Count	%
GET	9,851	98.51%
POST	106	1.06%
HEAD	42	0.42%
OPTIONS	1	0.01%

9:05:55:000 PM 1a/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36 host = "Apache\_Logs" ; source = apache\_logs.txt ; sourcetype = access\_combined

3/20/20 09:05:44:000 PM 38.99.236.50 - - [20/Mar/2020:21:05:44 +0000] "GET /presentations/logstash-puppetconf-2012/css/main.css HTTP/1.1" 200 26498 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36" host = "Apache\_Logs" ; source = apache\_logs.txt ; sourcetype = access\_combined

- referer\_domain

Time	Event
3/20/20 09:05:59:000 PM	5.10.83.53 - - [20/Mar/2020:21:05:59 +0000] "GET /files/grok/?Cn;O/A HTTP/1.1" 200 3894 "-" "Mozilla/5.0 (compatible; AhrefsBot/5.0; +http://ahrefs.com/robot)" host = "Apache_Logs" ; source = apache_logs.txt ; sourcetype = access_combined
3/20/20 09:05:59:000 PM	66.249.73.135 - - [20/Mar/2020:21:05:59 +0000] "GET /blog/tags/wine HTTP/1.1" 200 10021 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A537e Safari/6536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)" host = "Apache_Logs" ; source = apache_logs.txt ; sourcetype = access_combined
3/20/20 09:05:58:000 PM	63.140.98.80 - - [20/Mar/2020:21:05:58 +0000] "GET /images/VSI_headquarters.jpg HTTP/1.1" 200 6146 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36" host = "Apache_Logs" ; source = apache_logs.txt ; sourcetype = access_combined
3/20/20 09:05:57:000 PM	38.99.236.50 - - [20/Mar/2020:21:05:57 +0000] "GET /presentations/logstash-puppetconf-2012/images/frontend-response-codes.png HTTP/1.1" 200 52878 "http://semicomplete.com/presentations/logstash-puppetconf-2012/" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36" host = "Apache_Logs" ; source = apache_logs.txt ; sourcetype = access_combined

**referer\_domain**

>100 Values, 59.27% of events Selected Yes No

**Reports**

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
http://www.semicomplete.com	3,038	51.25%
http://semicomplete.com	2,001	33.76%
http://www.google.com	123	2.075%
https://www.google.com	105	1.772%
http://stackoverflow.com	34	0.574%
http://www.google.fr	31	0.523%
http://s-chassis.co.nz	29	0.489%
http://logstash.net	28	0.472%
http://www.google.es	25	0.422%
https://www.google.co.uk	23	0.388%

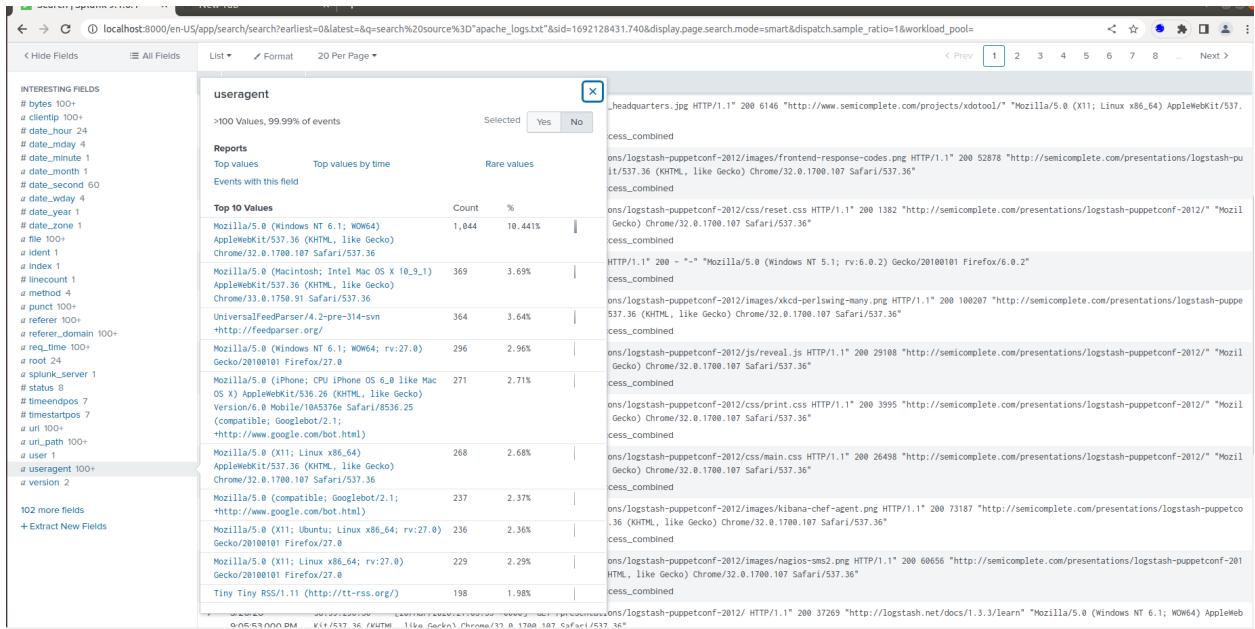
3/20/20 09:05:53:000 PM 38.99.236.50 - - [20/Mar/2020:21:05:53 +0000] "GET /presentations/logstash-puppetconf-2012/images/kibana-chief-agent.png HTTP/1.1" 200 73187 "http://semicomplete.com/presentations/logstash-puppetco... host = "Apache\_Logs" ; source = apache\_logs.txt ; sourcetype = access\_combined

- status

## ○ clientip

clientip				
>100 Values, 100% of events		Selected	Yes	No
<b>Reports</b>				
Top values      Top values by time      Rare values				
Events with this field				
<b>Top 10 Values</b>				
66.249.73.135	Count	%		
482		4.82%		
46.185.14.53				
364		3.64%		
130.237.218.86				
357		3.57%		
75.97.9.59				
273		2.73%		
58.16.19.13				
113		1.13%		
209.85.238.199				
102		1.02%		
68.180.224.225				
99		0.99%		
288.115.111.72				
83		0.83%		
198.46.149.143				
82		0.82%		
100.43.83.137				
79		0.79%		
<b>cess_combined</b>				
ons/logstash-puppetconf-2012/images/frontend-response-codes.png HTTP/1.1" 200 52878 "http://semicomplete.com/presentations/logstash-puppetconf-2012/it/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"				
cess_combined				
ons/logstash-puppetconf-2012/css/reset.css HTTP/1.1" 200 1382 "http://semicomplete.com/presentations/logstash-puppetconf-2012/* (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"				
cess_combined				
HTTP/1.1" 200 - "-" "Mozilla/5.0 (Windows NT 5.1; rv:6.0.2) Gecko/20100101 Firefox/6.0.2"				
cess_combined				
ons/logstash-puppetconf-2012/images/xkcd-perlwing-many.png HTTP/1.1" 200 100207 "http://semicomplete.com/presentations/logstash-puppetconf-2012/it/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"				
cess_combined				
ons/logstash-puppetconf-2012/js/reveal.js HTTP/1.1" 200 25108 "http://semicomplete.com/presentations/logstash-puppetconf-2012/* (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"				
cess_combined				
> 3/20/2020 38.99.236.50 - [20/Mar/2020:21:05:55 +0000] "GET /presentations/logstash-puppetconf-2012/css/print.css HTTP/1.1" 200 3995 "http://semicomplete.com/presentations/logstash-puppetconf-2012/* (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"				
9:05:55:000 PM i/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36" host = "Apache_Logs" : source = apache_logs.txt : sourcetype = access_combined				
> 3/20/2020 38.99.236.50 - [20/Mar/2020:21:05:54 +0000] "GET /presentations/logstash-puppetconf-2012/css/main.css HTTP/1.1" 200 26498 "http://semicomplete.com/presentations/logstash-puppetconf-2012/* (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"				
9:05:54:000 PM i/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36"				

### ○ useragent

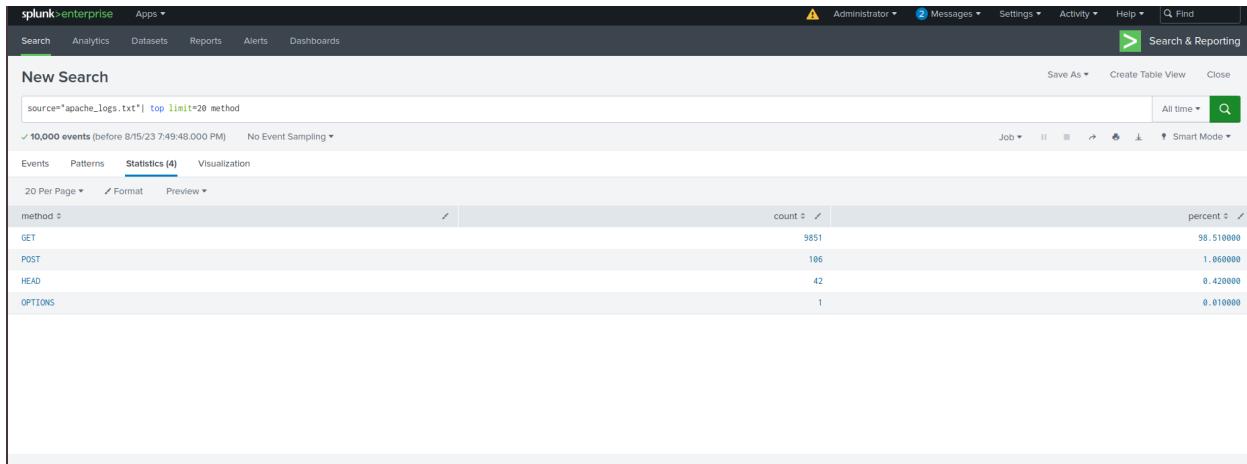


## Part 4: Create Reports, Alerts, and Dashboards for the Apache Logs

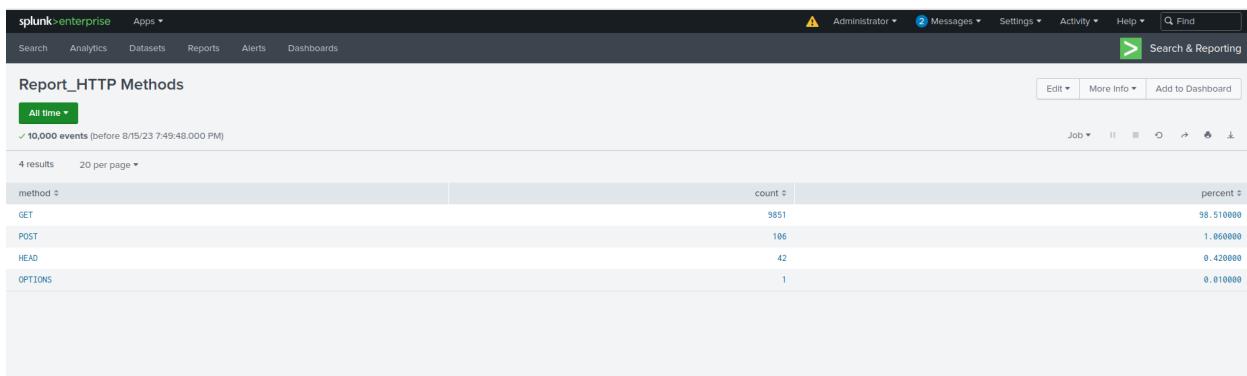
In this part, you will create reports, alerts, and dashboards to monitor for suspicious activity against VSI's Apache web server. To do so, complete the following steps:

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)

Splunk > enterprise Apps ▾

Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search & Reporting

New Search

source="apache\_logs.txt" host=""Apache\_logs"" sourcetype="access\_combined" | top limit=20 referer\_domain

✓ 10,000 events (before 8/16/23 6:06:47:000 AM) No Event Sampling ▾

Events Patterns Statistics (20) Visualization

20 Per Page ▾ Format Preview ▾

referer_domain	count	percent
http://www.semicomplete.com	3038	51.25%
http://semicomplete.com	2001	33.76%
http://www.google.com	123	2.07%
https://www.google.com	105	1.77%
http://stackoverflow.com	34	0.57%
http://www.google.fr	31	0.52%
http://s-chassis.co.nz	29	0.48%
http://logstash.net	28	0.47%
http://www.google.es	25	0.42%
https://www.google.co.uk	23	0.38%
http://www.s-chassis.co.nz	22	0.37%
http://www.google.de	18	0.30%
https://www.google.fr	15	0.25%
http://www.google.co.uk	14	0.23%
https://www.google.de	13	0.21%
https://www.google.co.in	13	0.21%
http://www.eoole.co.in	12	0.20%

## (Report created for the Top 10 Domains)

Splunk > enterprise Apps ▾

Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search & Reporting

Top 10 Domains

source="apache\_logs.txt" host=""Apache\_logs"" sourcetype="access\_combined" | top limit=20 referer\_domain

✓ 10,000 events (before 8/16/23 6:03:48:000 AM) No Event Sampling ▾

Events (10,000) Patterns Statistics (20) Visualization

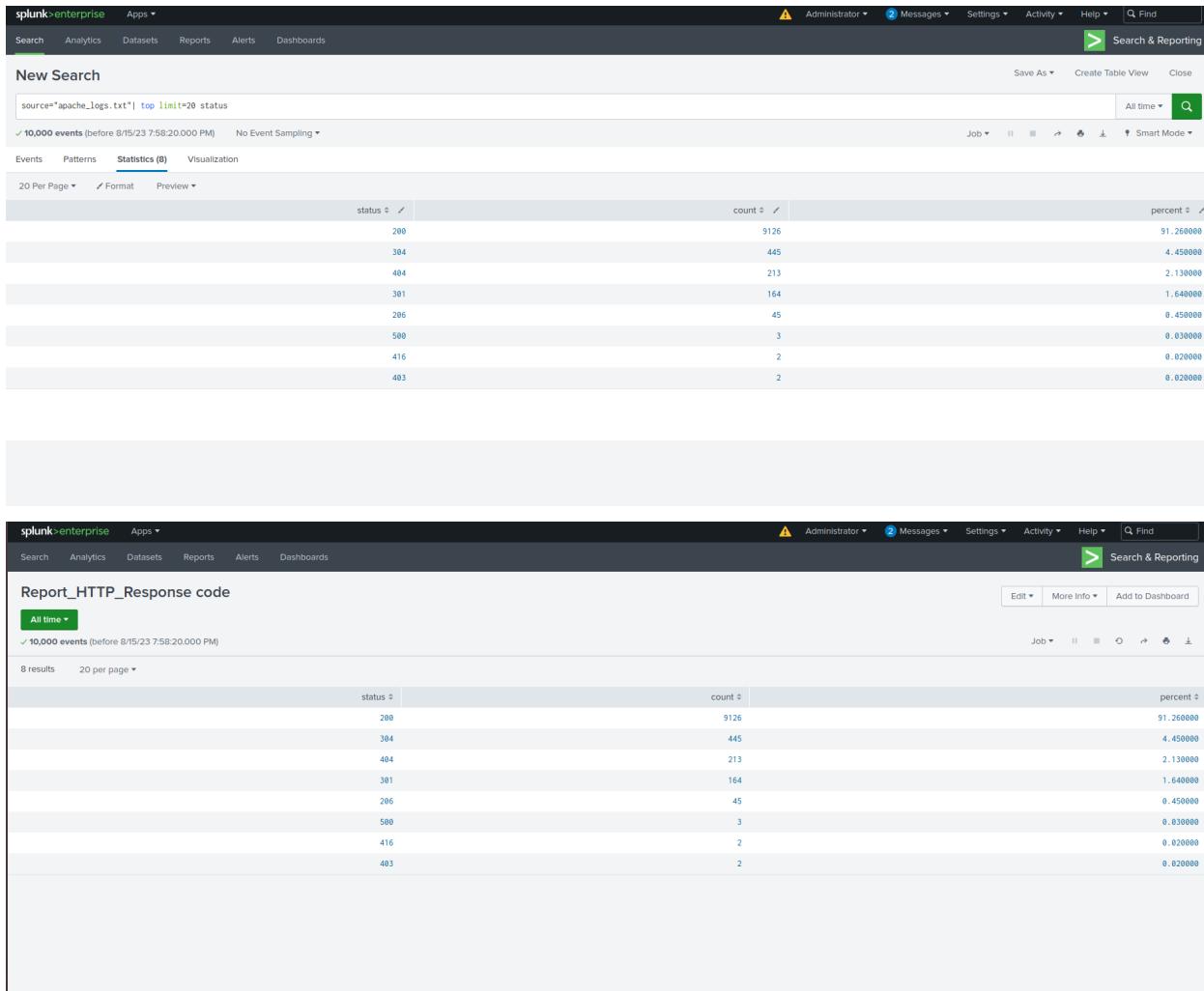
20 Per Page ▾ Format Preview ▾

referer_domain	count	percent
http://www.semicomplete.com	3038	51.25%
http://semicomplete.com	2001	33.76%
http://www.google.com	123	2.07%
https://www.google.com	105	1.77%
http://stackoverflow.com	34	0.57%
http://www.google.fr	31	0.52%
http://s-chassis.co.nz	29	0.48%
http://logstash.net	28	0.47%
http://www.google.es	25	0.42%
https://www.google.co.uk	23	0.38%
http://www.s-chassis.co.nz	22	0.37%
http://www.google.de	18	0.30%
https://www.google.fr	15	0.25%
http://www.google.co.uk	14	0.23%
https://www.google.de	13	0.21%
https://www.google.co.in	13	0.21%
http://www.eoole.co.in	12	0.20%

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:
  - 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](mailto:SOC@VSI-company.com).

Screenshot of Splunk search results for Apache logs from outside the United States:

```
source="apache_logs.txt" | iplocation clientip | where NOT Country="United States" | table clientip, status, City, Country
```

6,640 events (before 8/15/23 8:42:55.000 PM) No Event Sampling ▾

Events (6,640) Patterns Statistics (6,640) Visualization

Format Timeline ▾ Zoom Out + Zoom to Selection X Deselect

1 hour per column

List Format 20 Per Page ▾

Time	Event
3/20/20 9:05:59:000 PM	5.10.83.53 - [20/Mar/2020:21:05:59 +0000] "GET /files/grok/?Cn;0:A HTTP/1.1" 200 3894 "-" "Mozilla/5.0 (compatible; AhrefsBot/5.0; +http://ahrefs.com/robot/)" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined
3/20/20 9:05:56:000 PM	188.76.6.56 - [20/Mar/2020:21:05:56 +0000] "GET /robots.txt HTTP/1.1" 200 "-" "Mozilla/5.0 (Windows NT 5.1; rv:6.0.2) Gecko/20100101 Firefox/6.0.2" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined
3/20/20 9:05:50:000 PM	91.151.182.109 - [20/Mar/2020:21:05:50 +0000] "GET /VSI_Company_Homepage.html HTTP/1.1" 200 3638 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined
3/20/20 9:05:48:000 PM	91.151.182.109 - [20/Mar/2020:21:05:48 +0000] "GET /images/VSI_headquarters.jpg HTTP/1.1" 200 6146 "http://www.semicomplete.com/projects/xdotool/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined
3/20/20 9:05:46:000 PM	92.115.179.247 - [20/Mar/2020:21:05:46 +0000] "GET /blog/geekery/rrttool-behavior-detection.html HTTP/1.1" 200 8500 "http://www.google.md/url?sa=t&rct=j&q=&esrc=s&source=web&d=g6cad+rja&ved=0CQFjAF0c&url=http%3A%2F%2Fwww.semicomplete.com%2Fblog%2Fgeekery%2Frrttool-behavior-detection.html&ei=qHCUY-7PEMqhgFeyIDAw&usg=AFQjCN67nAfw0Fe7BxTySbgZ2FubVhw" "Mozilla/5.0 (X11; Ubuntu; Linux ux 18.04; rv:68.0) Gecko/20100101 Firefox/68.0" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined
3/20/20 9:05:42:000 PM	176.31.39.38 - [20/Mar/2020:21:05:42 +0000] "GET /blog/tags/logs HTTP/1.1" 200 34598 "http://www.semicomplete.com/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:22.0) Gecko/20100101 Firefox/22.0" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined
3/20/20 9:05:39:000 PM	46.195.14.53 - [20/Mar/2020:21:05:39 +0000] "GET /blog/tags/puppet?flav=rs20 HTTP/1.1" 200 14872 "-" "UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined
3/20/20 9:05:36:000 PM	5.10.83.21 - [20/Mar/2020:21:05:36 +0000] "GET /files/blogposts/20070826/test_new_re.rb HTTP/1.1" 200 1293 "-" "Mozilla/5.0 (compatible; AhrefsBot/5.0; +http://ahrefs.com/robot/)" host = "Apache_logs" source = apache_logs.txt sourcetype = access_combined

Save As Alert

When triggered

Send email

To: SOC@VSI-company.com

Priority: Normal

Subject: Splunk Alert: \$name\$

Message: The alert condition for '\$name\$' was triggered.

Include:  Link to Alert  Link to Results  
 Search String  Inline Table  
 Trigger  Attach CSV  
 Trigger Time  Attach PDF  
 Allow Empty Attachment

Type: HTML & Plain Text Plain Text

Save

Alert\_Connection\_from outside UNITED STATES

Enabled: Yes Disable

App: Search

Permissions: Private. Owned by admin. Edit

Modified: Aug 15, 2023 8:52:12 PM

Alert Type: Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: Number of Results is > 5. Edit

Actions: 1 Action Edit

Send email

Alerts

Search & Reporting

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾

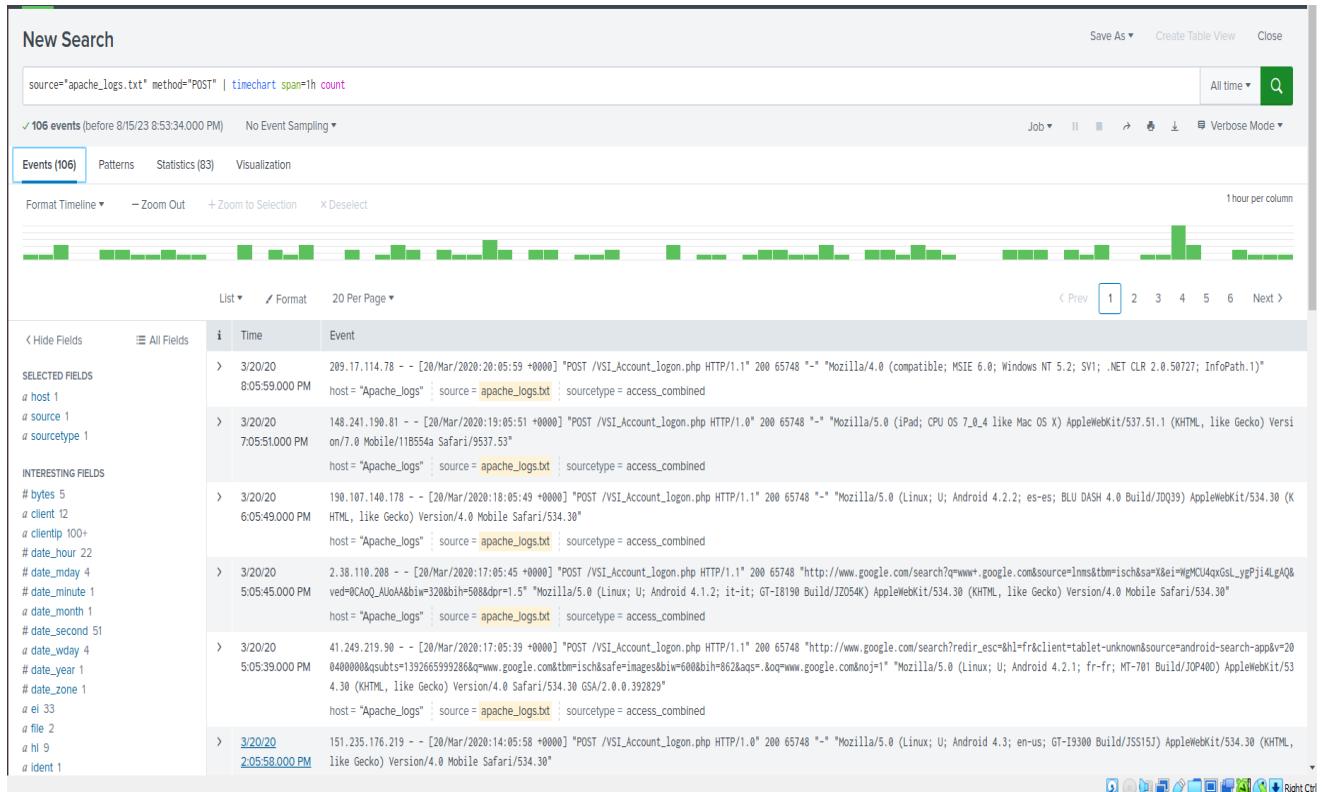
Alerts

Alert\_Connection\_from outside UNITED STATES

There are no fired events for this alert.

- 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](mailto:SOC@VSI-company.com).



**Save As Alert**

**Settings**

- Title: Alert\_Hourly\_Count\_HTTP POST METHOD
- Description: Optional
- Permissions: Private / Shared in App
- Alert type: Scheduled / Real-time
- Run every hour ▾
- At 0 minutes past the hour
- Expires: 24 hour(s) ▾

**Trigger Conditions**

- Trigger alert when Number of Results ▾
- is greater than ▾ 4
- Trigger Once / For each result
- Throttle? □

**Trigger Actions**

- + Add Actions ▾

**Save As Alert**

When triggered ▾

- Send email

To: SOC@VSI-company.com

Priority: Normal

Subject: Splunk Alert: \$name\$

The email subject, recipients and message can include tokens that insert text based on the results of the search. [Learn More](#)

Message: The alert condition for \$name\$ was triggered.

Include:

- Link to Alert
- Link to Results
- Search String
- Inline Table
- Trigger Condition
- Attach CSV
- Trigger Time
- Attach PDF
- Allow Empty Attachment

Type: HTML & Plain Text / Plain Text

**Alert\_Hourly\_Count\_HTTP POST METHOD**

Enabled: Yes Disable

App: search

Permissions: Private. Owned by admin. Edit

Modified: Aug 15, 2023 8:55:35 PM

Alert Type: Scheduled. Hourly, at 0 minutes past the hour. Edit

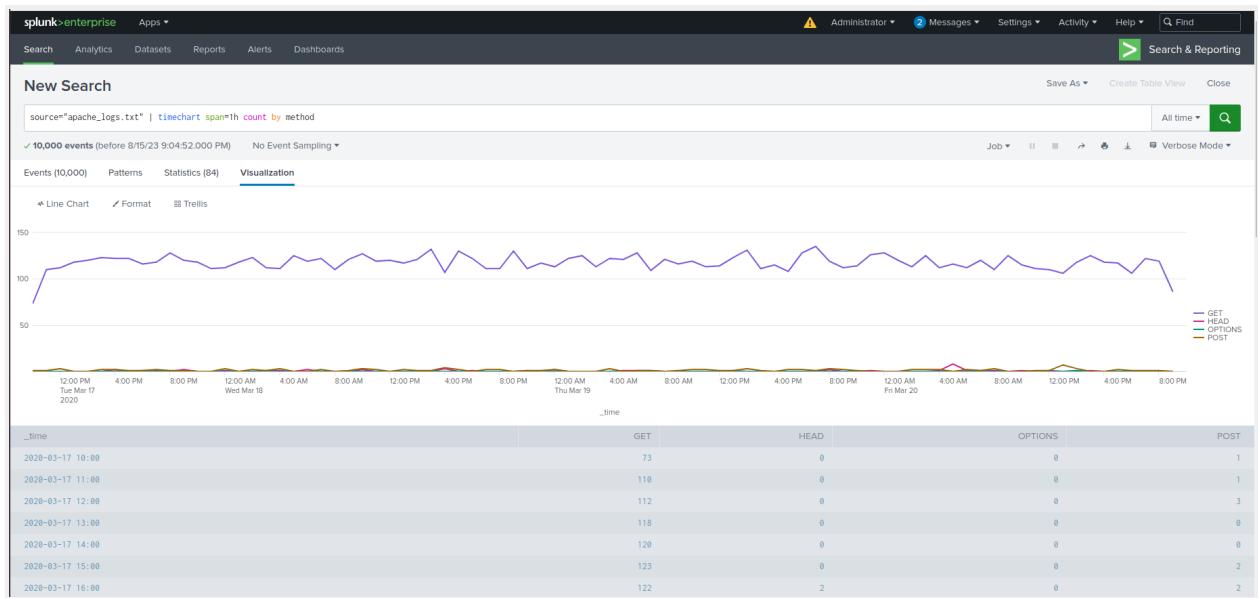
Trigger Condition: Number of Results is > 4. [Edit](#)

Actions: 1 Action [Edit](#)

Send email

There are no fired events for this alert.

- **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.`



### Save Panel to New Dashboard

Dashboard Title: 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

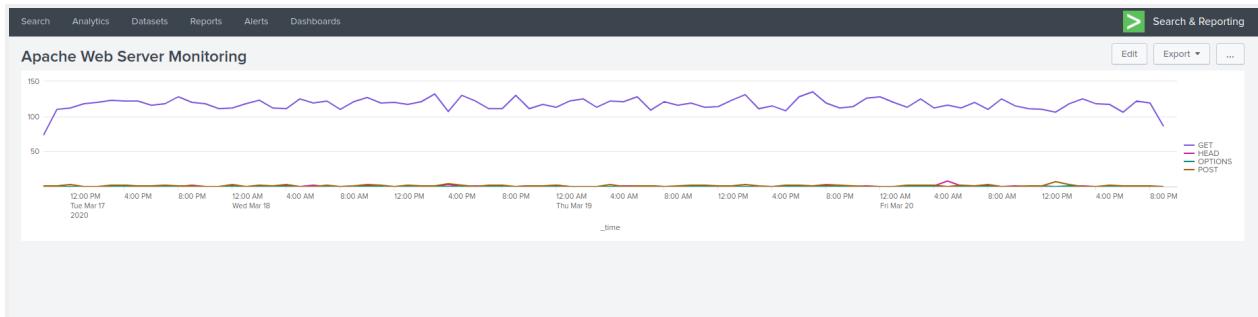
**Dashboard Studio** NEW  
 A new builder to create visually-rich, customizable dashboards

Panel Title: Optional

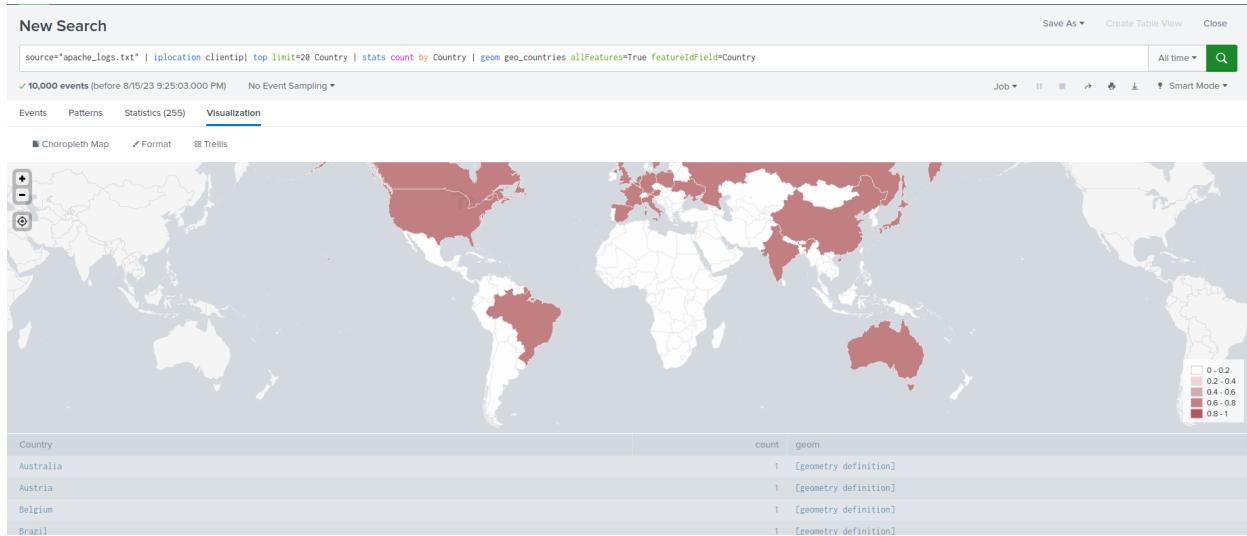
Visualization Type:  Line Chart  Statistics Table

[Advanced Panel Settings](#)

[Cancel](#) [Save to Dashboard](#)



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



### Save Panel to Existing Dashboard

Select an Existing Dashboard Sort: Title (A - Z) ↴

Search By Title

- Apache Web Server Monitoring
- Integrity Check of Installed Files
- Job Details Dashboard
- jQuery Upgrade
- Orphaned Scheduled Searches, Reports, and Alerts

---

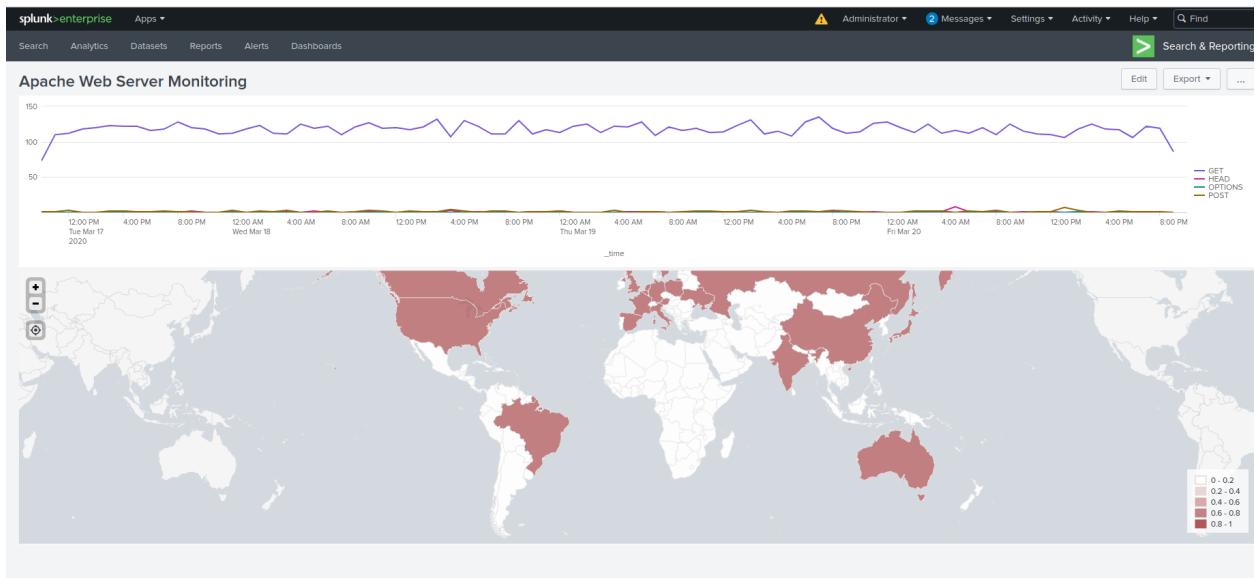
Panel Title Optional

Visualization Type  Choropleth Map  Statistics Table

[Advanced Panel Settings](#)

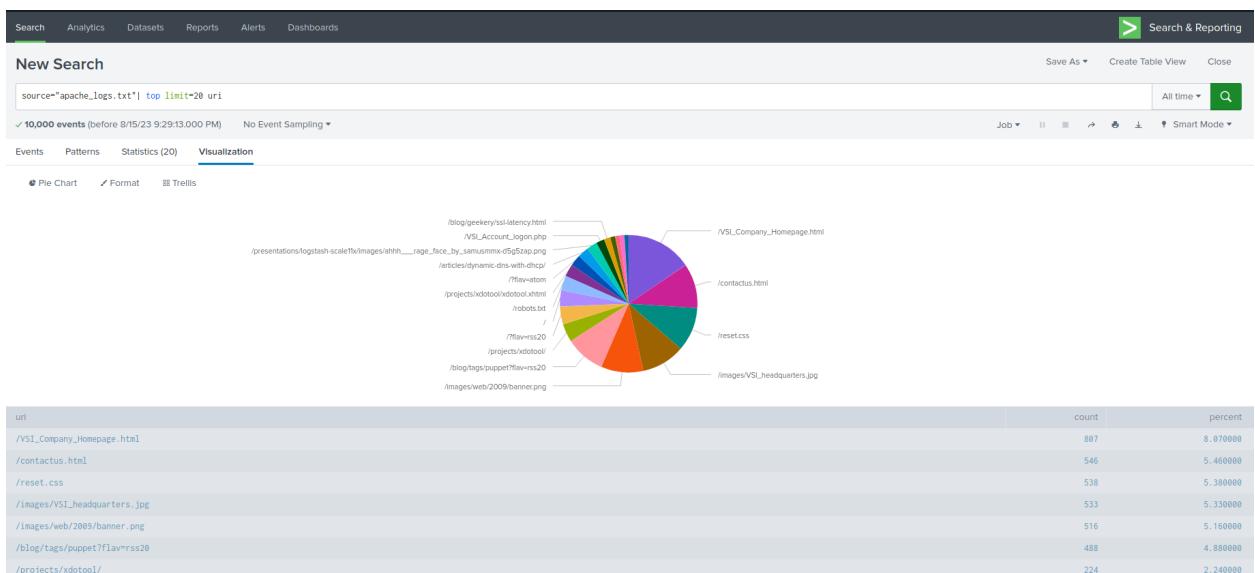
---

Cancel Save to Dashboard



- 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](#).



**Save Panel to Existing Dashboard**

Select an Existing Dashboard      Sort: Title (A - Z) ↓

Search By Title

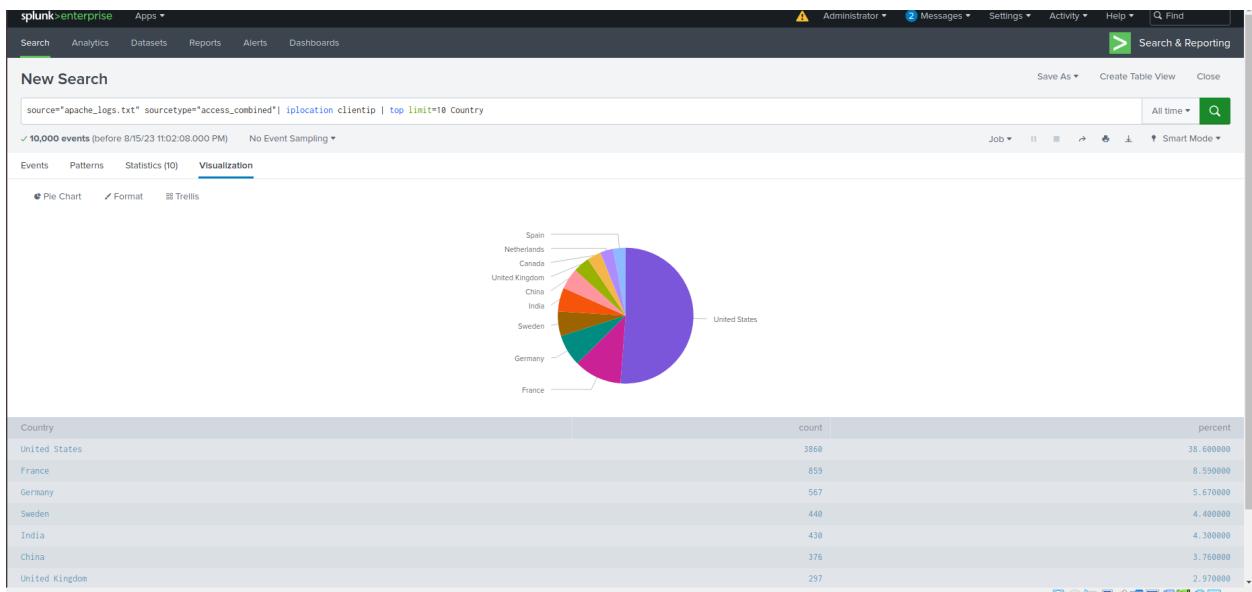
- Apache Web Server Monitoring
- Integrity Check of Installed Files
- Job Details Dashboard
- jQuery Upgrade
- Orphaned Scheduled Searches, Reports, and Alerts

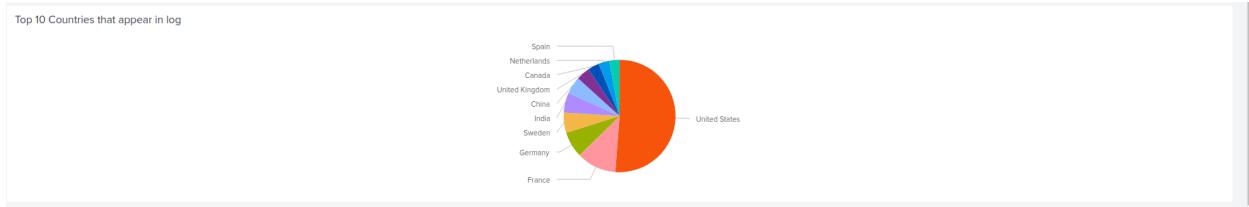
Panel Title      Optional

Visualization Type       Pie Chart       Statistics Table

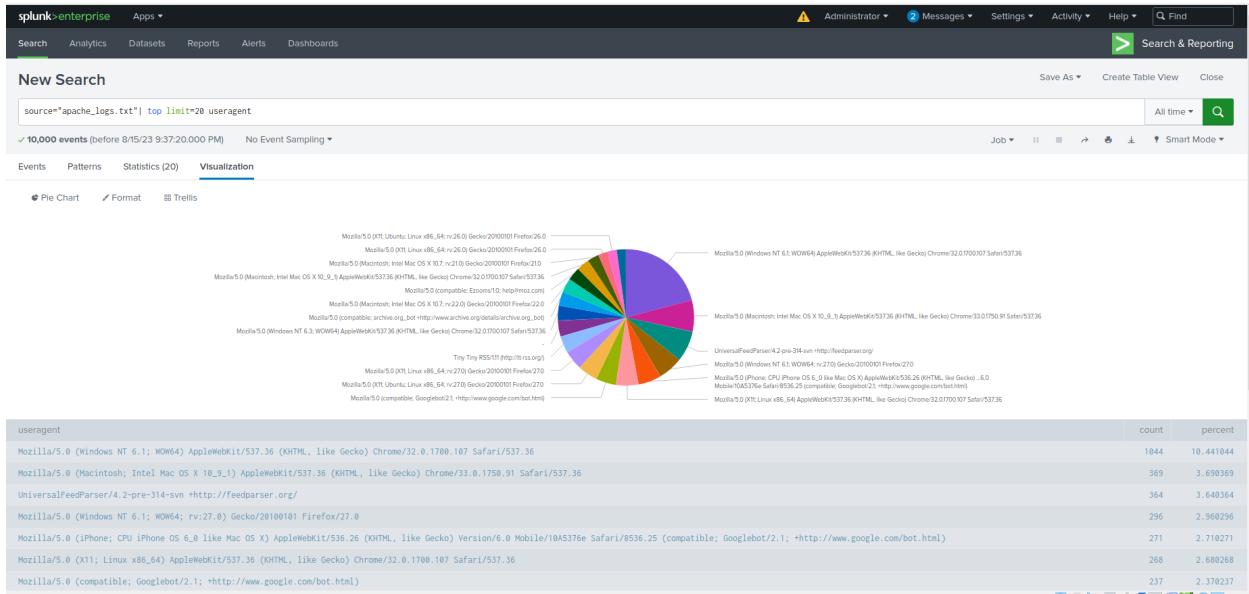
> Advanced Panel Settings

- 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.



Save Panel to Existing Dashboard X

Select an Existing Dashboard Sort: Title (A - Z) ↓

Search By Title  🔍

Apache Web Server Monitoring

Integrity Check of Installed Files

Job Details Dashboard

jQuery Upgrade

Orphaned Scheduled Searches, Reports, and Alerts

---

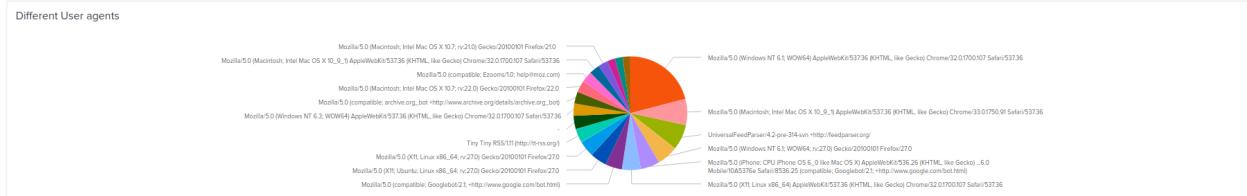
Panel Title

Visualization Type Pie Chart Statistics Table

Advanced Panel Settings

---

Cancel Save to Dashboard



- 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.

