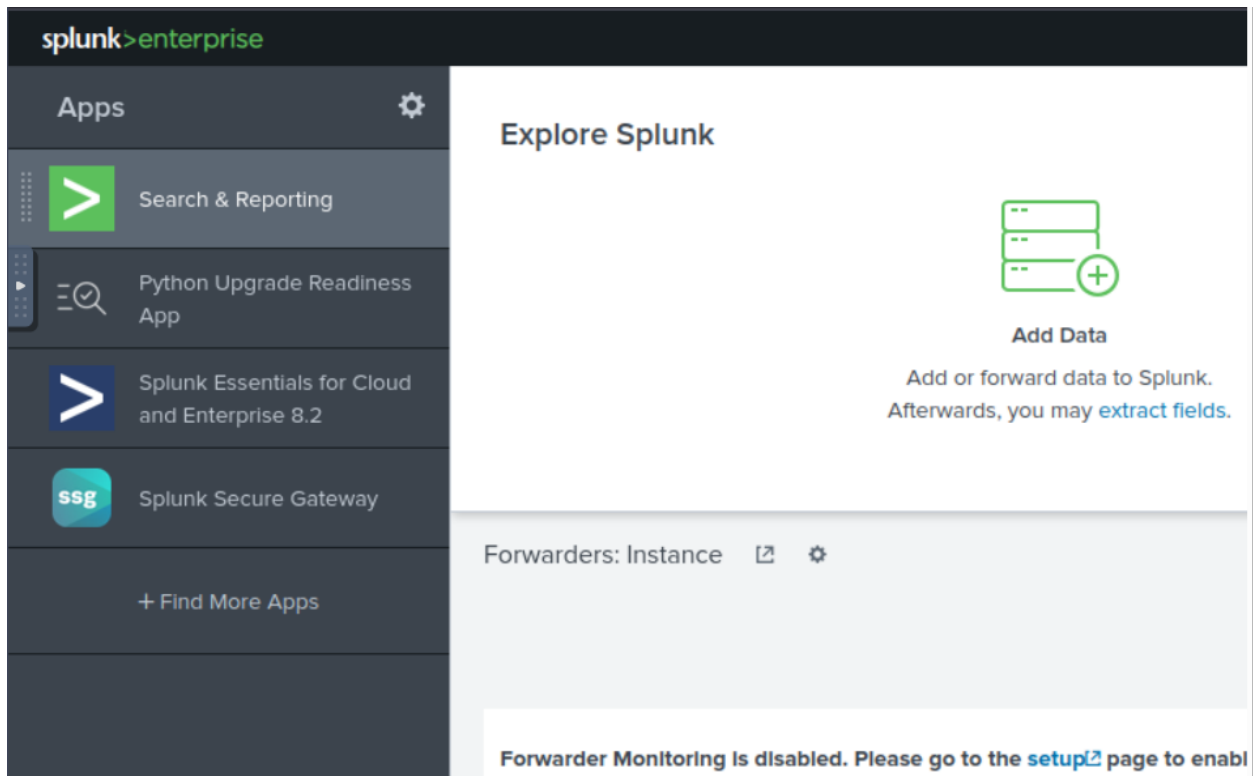


SPLUNK BASIC Report

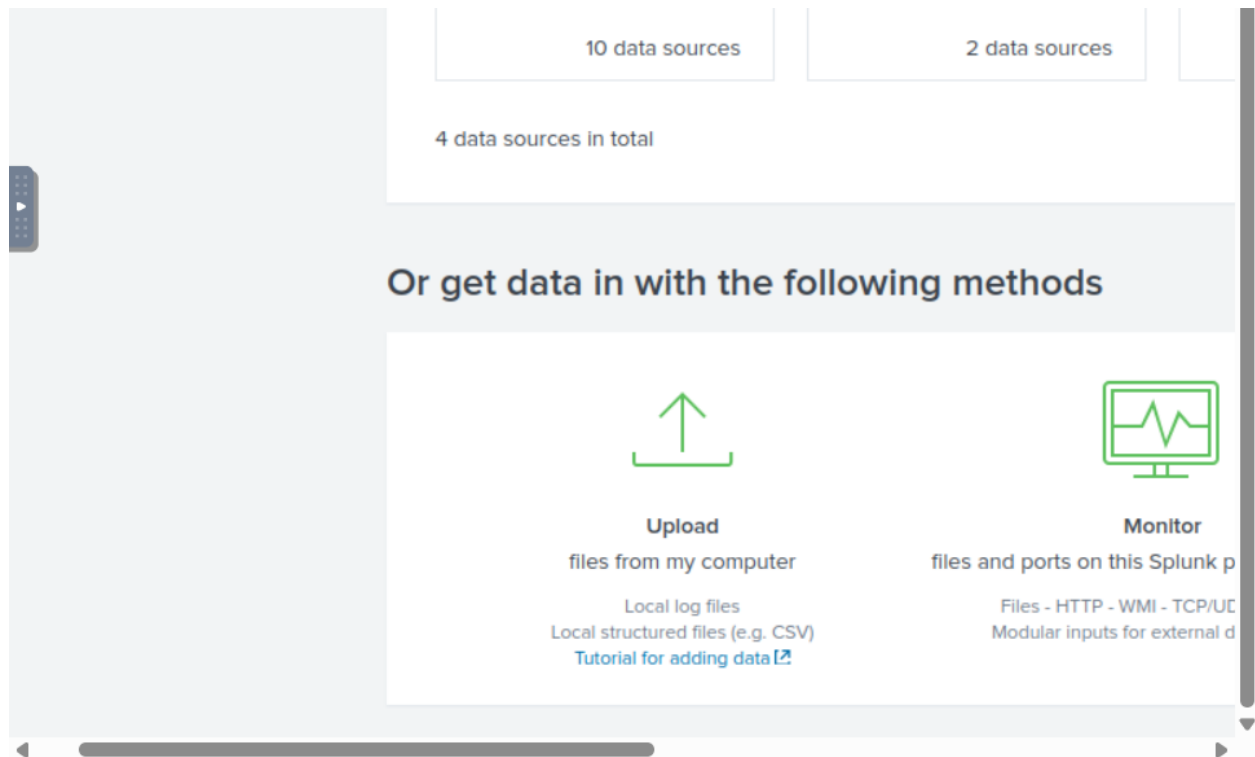
2025/12/08

Objective: Ingesting log data into splunk and performing a log analysis.

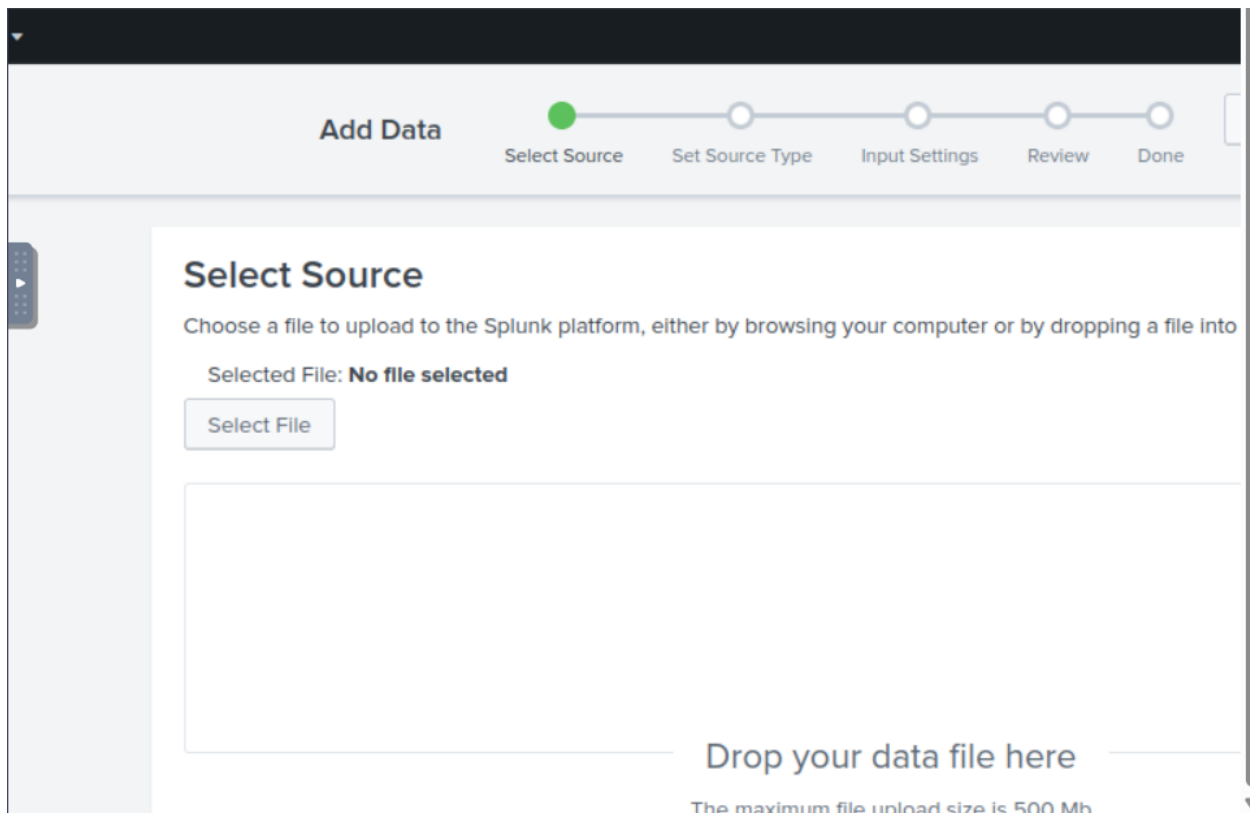
STEP 1: Loading splunk as a web application and ingesting data.



I clicked 'Add Data' in the 'Explore Splunk' section.



I then scrolled down just a bit and clicked on 'Upload', navigated my way to the correct directory then into the correct folders to upload the relevant files from my computer.



I was then faced with the 'Select Source' page and chose the log file as well as the data source.

Add Data

Select Source

Set Source Type

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right format, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an app for your data, create a new one by clicking "Save As".

Source: **VPNlogs.json**

Source type: **_json**

Save As

Table

Format

20 Per Page

> Timestamp

> Advanced

	_time	action	Color
1	1/1/22 7:58:42.000 AM	built	Cyber
2	1/1/22 5:26:59.000 PM	teardown	Cyber
3	1/1/22 7:10:01.000 AM	built	Cyber

Next was the 'Set Source Type' where I had to select the type of logs being ingested but, in this case, all I had to do was verify that it was in the intended format.

splunk>enterprise 3 Messages Settings Activity He

Add Data

Select Source Set Source Type **Input Settings** Review Done < Back

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

FAQ

- > How do indexes work?
- > How do I know when to create or use multiple indexes?

Index **Default** Create a new

- history
- main
- summary
- test_index
- titanic
- vpn_logs**
- win_eventlogs

After that I landed on 'Input Settings' where I created the Index and selected it as the default index where the logs would then be dumped and associated it with the HOSTNAME of my choice.

splunk>enterprise 3 Messages Settings Activity He

Add Data

Select Source Set Source Type Input Settings Review Done

< Back

Review

Input Type Uploaded File

File Name VPNlogs.json

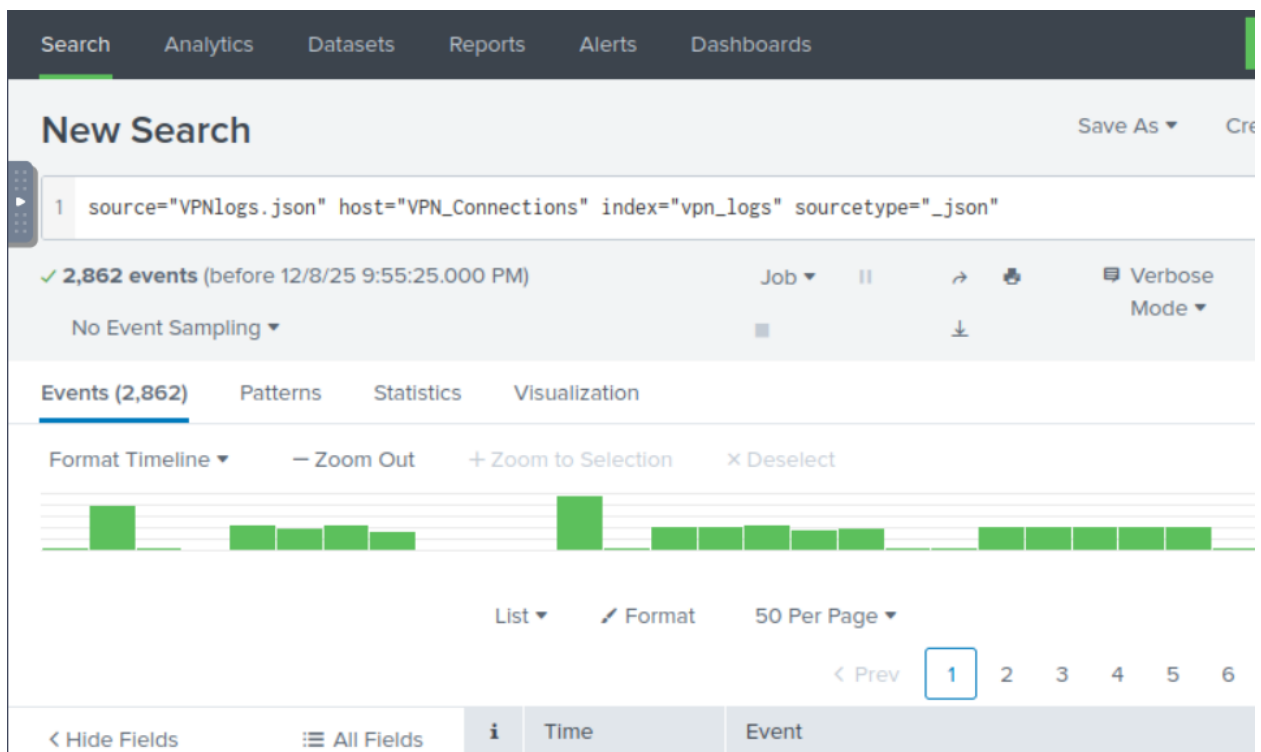
Source Type _json

Host VPN_Connections

Index vpn_logs

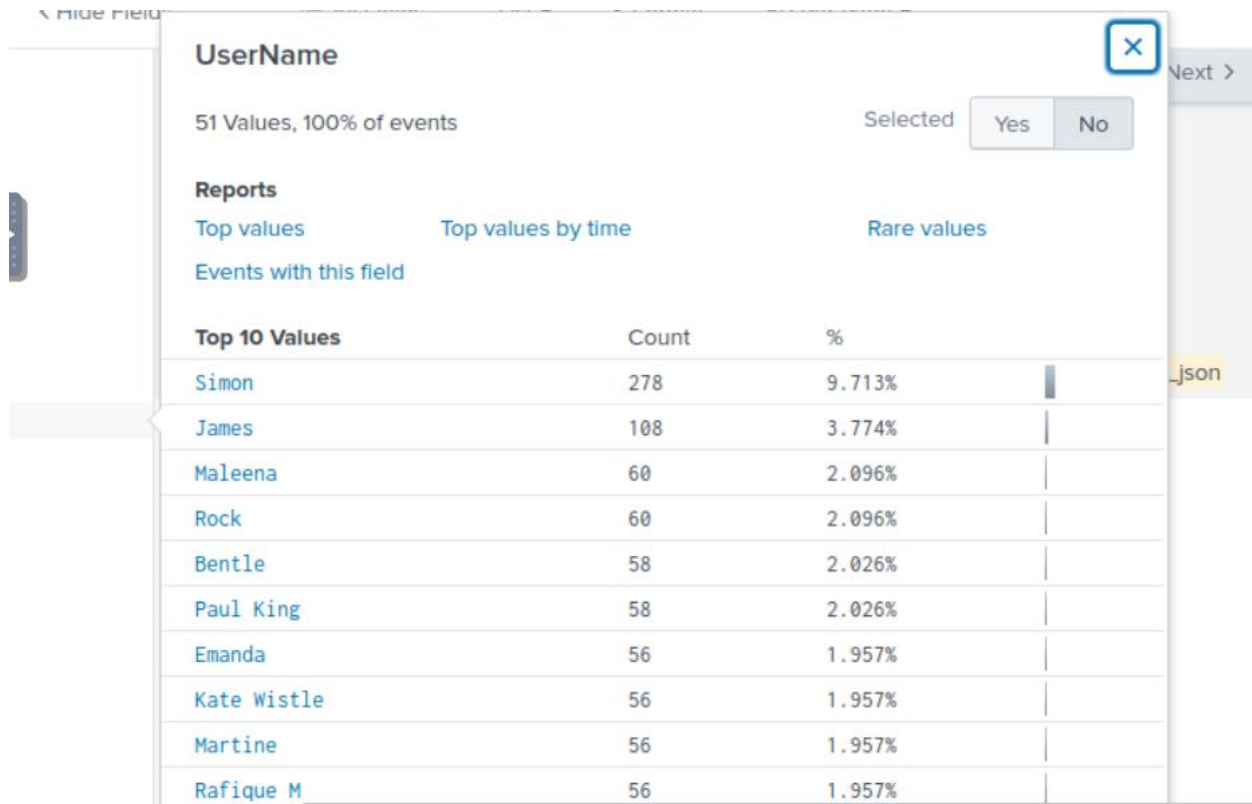
Before landing on the 'Done' page and wrapping up the ingestion phase and loading the data, I was faced with the preceding 'Review' page where I had a chance to double check the choices I had made and was happy so I proceeded onto the next step.

STEP 2: Finding how many events are present in the file.



I skimmed through the page where the data loaded manifests itself and identified the number of events (2862).

STEP 2: Discovering the number of log events by the user Maleena.



UserName

51 Values, 100% of events

Selected

Reports

Top values Top values by time Rare values

Events with this field


Top 10 Values	Count	%
Simon	278	9.713%
James	108	3.774%
Maleena	60	2.096%
Rock	60	2.096%
Bentle	58	2.026%
Paul King	58	2.026%
Emanda	56	1.957%
Kate Wistle	56	1.957%
Martine	56	1.957%
Rafique M	56	1.957%





I looked to the left side of the page and scrolled down to find the target name in the 'UserName' filter and clicked on it. I looked through the section and spotted the target name as well as the Count of events associated with the name – 60.


STEP 3: Locating the name associated with username associated with IP 107.14.182.38.

The screenshot shows a search interface with a query bar at the top containing the text: `host="VPN_Connections" index="vpn_logs" sourcetype="_json" source_ip="107.14.182.38"`. To the right of the query bar are buttons for "Save As", "Create Table View", and "Close". Below the query bar is a status bar showing "10:08:27.000 PM)", "Job", a pause icon, a refresh icon, a download icon, and "Verbose Mode". Below the status bar are tabs for "Statistics" and "Visualization". At the bottom, there are zoom controls: "Zoom Out", "+ Zoom to Selection", and "x Deselect", along with a scale indicator "1 day per column". The main content area displays the message "No results found."


I entered the following query (`source_ip="107.14.182.38"`) and nothing showed up. I took a few steps back and took a breather prior to my second attempt.




" host="VPN_Connections" index="vpn_logs" sourcetype="_json" 107.14.182.38 All time 

5 10:13:42.000 PM) Job    Verbose Mode 

 Statistics Visualization

Zoom Out + Zoom to Selection × Deselect 1 day per column



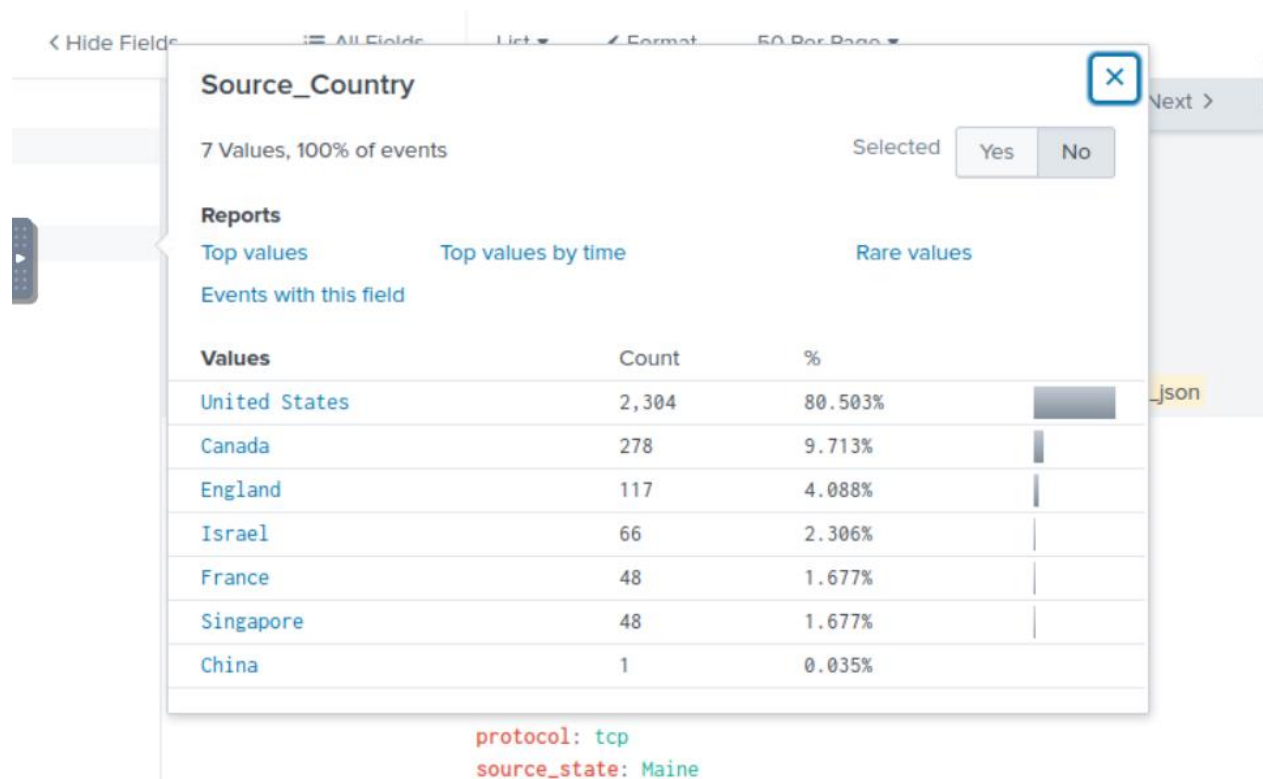
List  Format  50 Per Page 

All Fields	i	Time	Event
>		1/31/22 6:22:08.000 PM	{ [-] Company: CyberT EventTime: 2022-01-31T18:22:08 Source_Country: United States Source_ip: 107.14.182.38 UserName: Smith action: teardown

<https://tryhackme.com>

I then removed the filter and pasted only the desired IP and voila! UserName identified – Smith.

STEP 4: What is the number of events that originated from all countries except France?



There were a total of 2862 events from the countries and I looked at France and saw 48. I took the 48 and differenced it from the total and got the answer – 2814.

STEP 5: How many VPN events were associated with the IP 107.3.206.58

The screenshot displays the Splunk Search interface. At the top, the 'New Search' header is visible. The search bar contains the query: `source="VPNlogs.json" host="VPN_Connections" index="vpn_logs" sourcetype="_json" 107.3.206.58`. Below the search bar, a status bar indicates '14 events (before 12/8/25 10:18:18.000 PM)'. The interface includes tabs for 'Events (14)', 'Patterns', 'Statistics', and 'Visualization'. A 'Format Timeline' button is present, along with zoom and selection controls. At the bottom, there are options to 'Hide Fields', 'All Fields', and a table header showing 'Time' and 'Event' columns.

I pasted the IP address in the filter/search section and got the number of events associated with it - 14.

Summary Conclusion

This exercise demonstrated the complete process of ingesting and analysing log data in Splunk. I successfully uploaded data, verified the source type, configured input settings, and created a custom index for log storage. Once ingested, I carried out several analysis tasks, including identifying total events, filtering events by specific users, locating usernames linked to IP addresses, and calculating event counts based on geographic sources. Through targeted searches and filters, I identified user activity patterns, IP-associated behaviours, and event counts across different criteria. Overall, this exercise strengthened my understanding of Splunk's workflow, search capabilities, and practical log analysis techniques essential for cybersecurity monitoring.