

Splunk: Basics

Cyber Defense > Security Operations & Monitoring > Splunk: Basics

Splunk: Basics
Learn the basics of Splunk.
Easy 30 min

Start AttackBox Help Save Room 856 Options

Room progress (20%)

Target Machine Information

Title	Target IP Address	Expires
Splunk-Basics	10.10.55.158	1h 52min 42s

? Add 1 hour Terminate

Introduction

This repository showcases my work using Splunk to analyze and derive insights from event data. This project involves creating specific queries to filter and count events, helping to identify patterns and anomalies in the data. It demonstrates my ability to manipulate and extract valuable information from large datasets using Splunk.

Objectives

The primary objectives of this project were to:

1. Count the number of events originating from all countries except France.
2. Determine the number of VPN events observed by a specific IP address.

Task 1: Introduction

Task 1 Introduction

Splunk is one of the leading SIEM solutions in the market that provides the ability to collect, analyze and correlate the network and machine logs in real-time. In this room, we will explore the basics of Splunk and its functionalities and how it provides better visibility of network activities and help in speeding up the detection.

Learning Objective and Pre-requisites

If you are new to SIEM, please complete the [Introduction to SIEM](#). This room covers the following learning objectives:

- Splunk overview
- Splunk components and how they work
- Different ways to ingest logs
- Normalization of logs

Answer the questions below

Continue with the next task.

No answer needed Correct Answer

Task 2: Connect with the Lab

Task 2 Connect with the Lab

Room Machine ▶ Start Machine

Before moving forward, deploy the machine. When you deploy the machine, it will be assigned an IP. Access this room in a web browser on the AttackBox, or via the VPN at `http://10.10.55.158`. The machine will take up to 3-5 minutes to start.

Answer the questions below

Connect with the lab.

✓ Correct Answer

The screenshot shows the Splunk 8.2.6 web interface in a browser. The address bar shows `10.10.55.158/en-US/app/launcher/home`. The interface includes a sidebar with 'Apps' and 'Search & Reporting' sections. The main content area is titled 'Explore Splunk' and features three cards: 'Add Data', 'Splunk Apps', and 'Splunk Docs'. Below these cards, there is a section for 'Forwarders: Instance' with a 'Close' button. At the bottom, a message states: 'Forwarder Monitoring is disabled. Please go to the [setup](#) page to enable it.'

Task 3: Splunk Components

Task 3 Splunk Components

Splunk has three main components, namely Forwarder, Indexer, and Search Head. These components are explained below:

Indexer

Search Head

Forwarder

Answer the questions below

Which component is used to collect and send data over the Splunk instance?

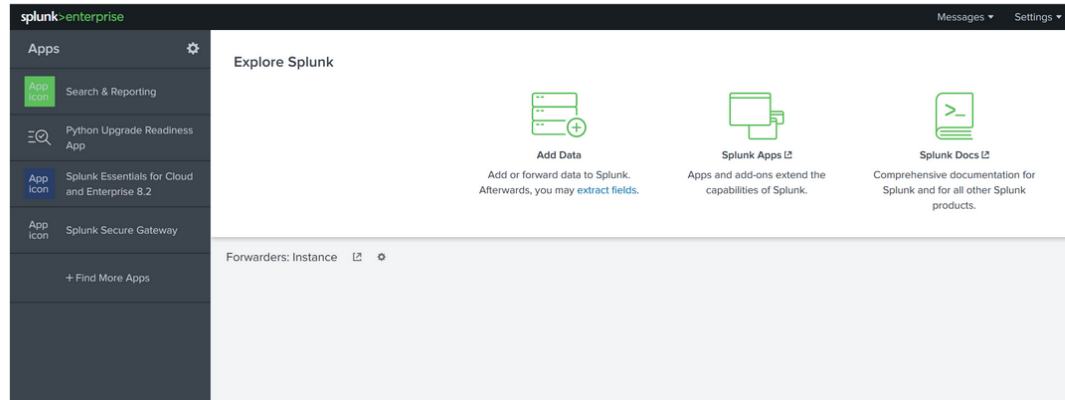
✓ Correct Answer

Task 4: Navigating Splunk

Task 4 Navigating Splunk

Splunk Bar

When you access Splunk, you will see the default home screen identical to the screenshot below.



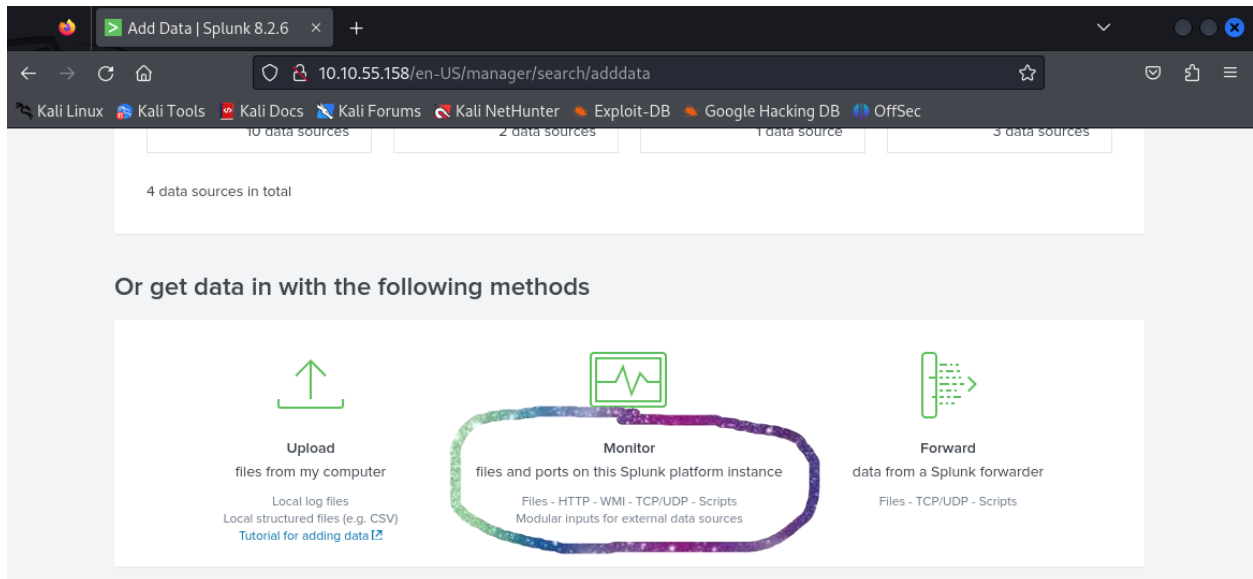
Answer the questions below

In the Add Data tab, which option is used to collect data from files and ports?

Monitor

✓ Correct Answer

💡 Hint



Task 5: Adding Data

Task 5 Adding Data



Splunk can ingest any data. As per the Splunk documentation, when data is added to Splunk, the data is processed and transformed into a series of individual events.

[Download Task Files](#)

The data sources can be event logs, website logs, firewall logs, etc.

Data sources are grouped into categories. Below is a chart listing from the Splunk documentation detailing each data source category.

Data source	Description
Files and directories	Most data that you might be interested in comes directly from files and directories.
Network events	The Splunk software can index remote data from any network port and SNMP events from remote devices.
IT Operations	Data from IT Ops, such as Nagios, NetApp, and Cisco.
Cloud services	Data from Cloud services, such as AWS and Kinesis.
Database services	Data from databases such as Oracle, MySQL, and Microsoft SQL Server.
Security services	Data from security services such as McAfee, Microsoft Active Directory, and Symantec Endpoint Protection.
Virtualization services	Data from virtualization services such as VMWare and XenApp.
Application servers	Data from application servers such as JMX & JMS, WebLogic, and WebSphere.
Windows sources	The Windows version of Splunk software accepts a wide range of Windows-specific inputs, including Windows Event Log, Windows Registry, WMI, Active Directory, and Performance monitoring.
Other sources	Other input sources are supported, such as FIFO queues and scripted inputs for getting data from APIs, and other remote data interfaces.

In this room, we're going to focus on **VPN logs**. When we click on the **Add Data** link (from the Splunk home screen), we're presented with the following screen.

What data do you want to send to the Splunk platform?

Follow guides for onboarding popular data sources



Cloud computing

Get your cloud computing data in to the Splunk platform.

10 data sources



Networking

Get your networking data in to the Splunk platform.

2 data sources



Operating System

Get your operating system data in to the Splunk platform.

1 data source



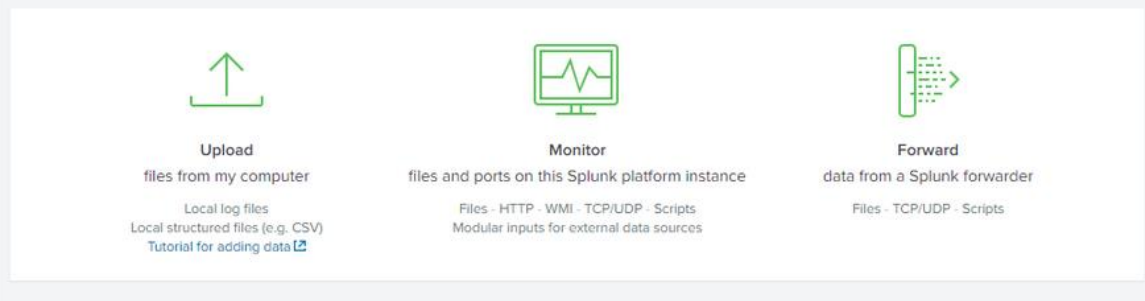
Security

Get your security data in to the Splunk platform.

3 data sources

4 data sources in total

Or get data in with the following methods



We will use the Upload Option to upload the data from our local machine. Download the attached log file and upload it on [Splunk](#).

As shown above, it has a total of 5 steps to successfully upload the data.

1. **Select Source** -> Where we select the Log source.
2. **Select Source Type** -> Select what type of logs are being ingested.
3. **Input Settings** -> Select the index where these logs will be dumped and hostName to be associated with the logs.
4. **Review** -> Review all the gif
5. **Done** -> Final step, where the data is uploaded successfully and ready to be analyzed.

Step 1. **Select Source**

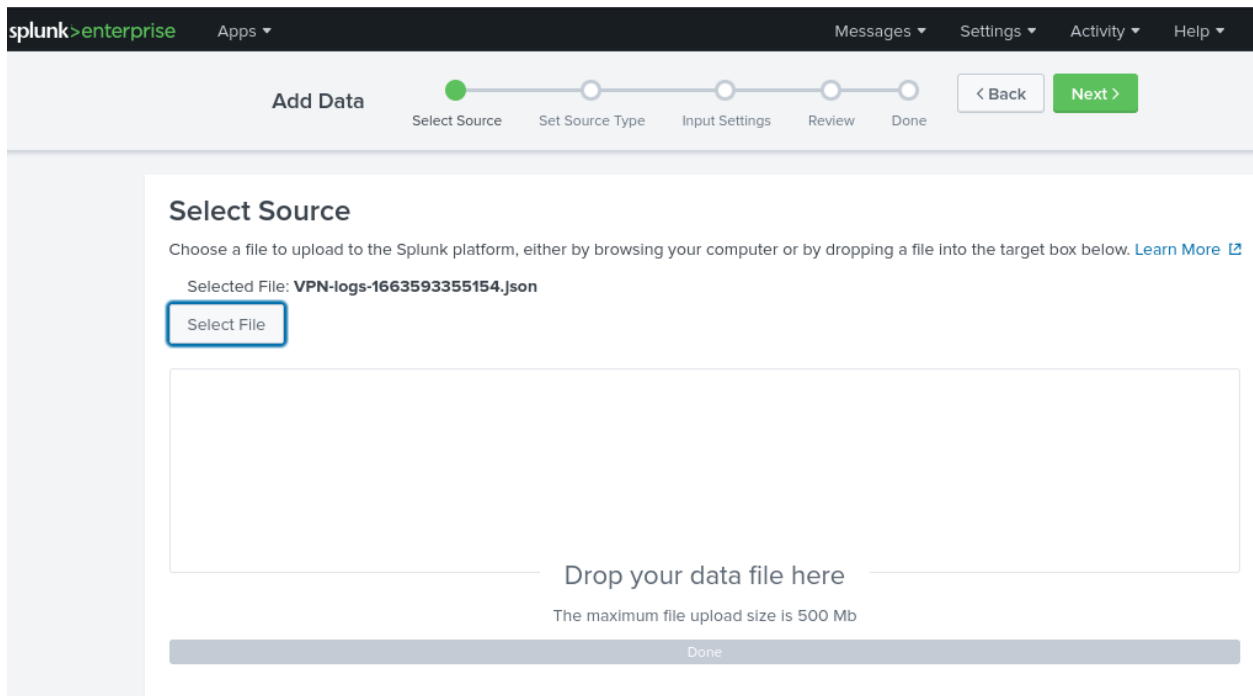
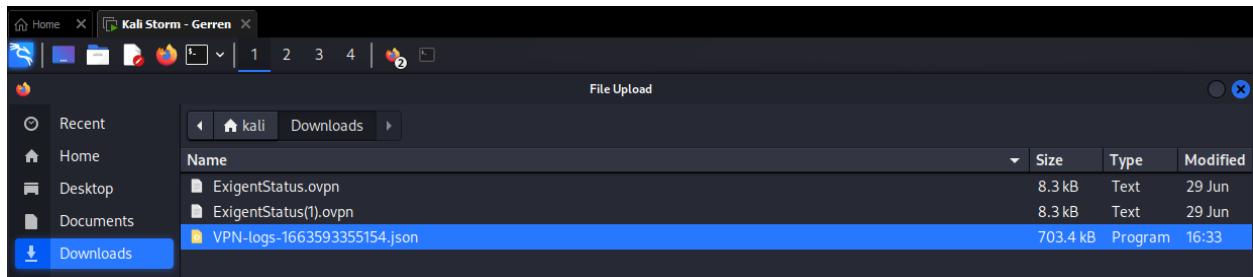
The screenshot shows the Splunk web interface for the 'Select Source' step. The browser address bar shows the URL: `10.10.55.158/en-US/manager/search/adddatamethods/selectsource?input_mode=0`. The navigation bar includes links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main header shows 'splunk>enterprise' and 'Apps'. A progress bar at the top indicates the current step is 'Select Source', with other steps being 'Set Source Type', 'Input Settings', 'Review', and 'Done'. Navigation buttons for '< Back' and 'Next >' are present.

The 'Select Source' section contains the following text and elements:

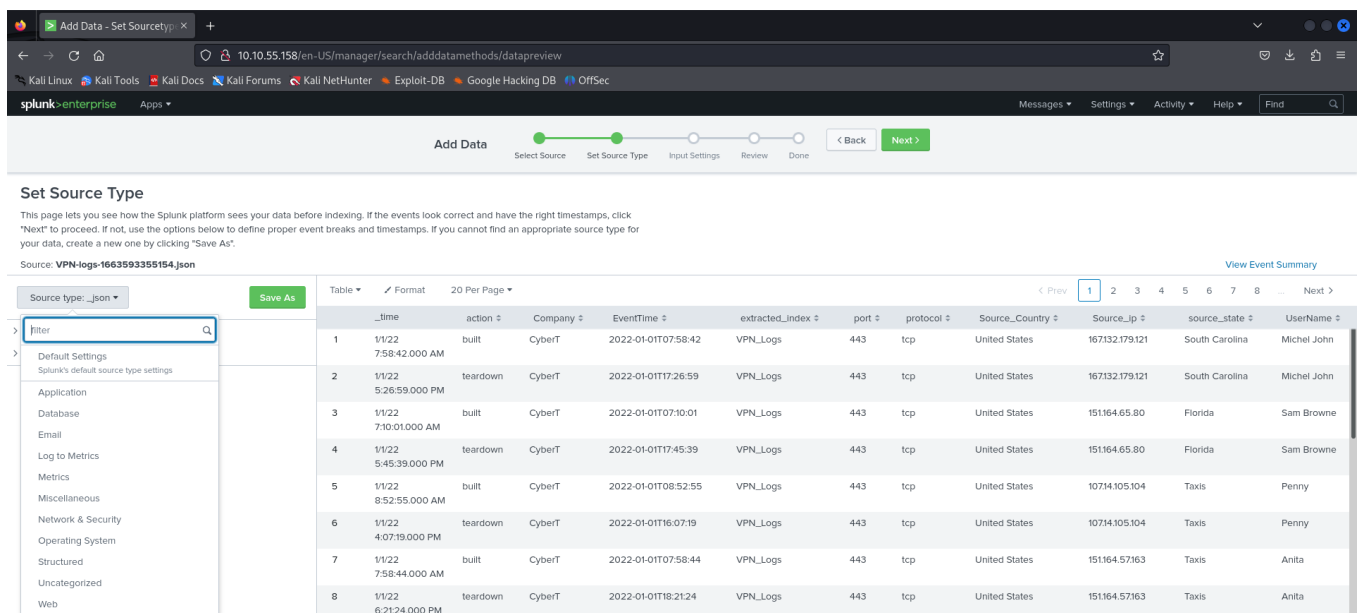
- Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. [Learn More](#)
- Selected File: **No file selected**
- A 'Select File' button.
- A large rectangular drop zone with the text 'Drop your data file here' and 'The maximum file upload size is 500 Mb'.

Below the main content area is an 'FAQ' section with three questions:

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



Step 2. Set Source Type



Step 3. Input Settings

splunk>enterprise

Apps

Messages

Settings

Activity

Help

Find

Add Data

Select Source

Set Source Type

Input Settings

Review

Done

< Back

Review >

Input Settings

Optionally set additional input parameters for this data input as follows:

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

☒ Constant value
☐ Regular expression on path
☐ Segment in path

Host field value

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](#)

Index Default [Create a new index](#)

- ☒ Constant value
- ☐ Regular expression on path
- ☐ Segment in path

Host field value

Index

[Create a new index](#)

New Index



General Settings

Index Name

Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Step 4. Review

splunk>enterprise

Apps ▾

Messages ▾

Settings ▾

Activity ▾

Help ▾

Add Data

Select Source

Set Source Type

Input Settings

Review

Done

< Back

Submit >

Review

Input Type Uploaded File
File Name VPN-logs-1663593355154.json
Source Type _json
Host VPN_Connections
Index vpn_logs

Step 5. File has been uploaded successfully

splunk>enterprise

Apps ▾

Messages ▾

Settings ▾

Activity ▾

Help ▾

Add Data

✓

Select Source

Set Source Type

Input Settings

Review

Done

< Back

Next >



File has been uploaded successfully.

Configure your inputs by going to Settings > [Data Inputs](#)

Start Searching

Search your data now or see [examples and tutorials](#). [🔗](#)

Extract Fields

Create search-time field extractions. [Learn more about fields](#). [🔗](#)

Add More Data

Add more data inputs now or see [examples and tutorials](#). [🔗](#)

Download Apps

Apps help you do more with your data. [Learn more](#). [🔗](#)

Build Dashboards

Visualize your searches. [Learn more](#). [🔗](#)

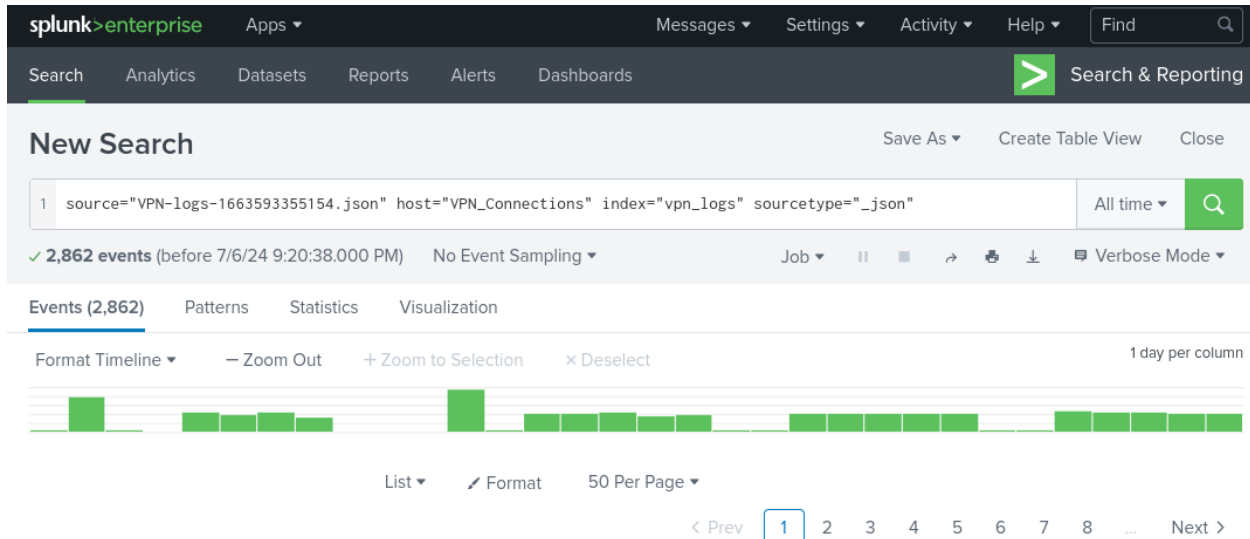
Review Questions

1.

Upload the data attached to this task and create an index "VPN_Logs". How many events are present in the log file?

2862

✓ Correct Answer



Splunk Search Query Breakdown:

1. **source="VPN-logs-168539355154.json"**
 - This part of the query specifies the source file for the events. In this case, it is a JSON file named VPN-logs-168539355154.json.
2. **host="VPN_Connections":**
 - This filter restricts the search to events from a specific host named VPN_Connections. The host can represent the machine or system that generated the log data.
3. **Index="vpn_logs":**
 - This specifies the index where the data is stored. In Splunk, an index is a repository for data, and vpn_logs are the names of the index containing VPN connection logs.
4. **sourcetype="_json":**
 - This indicates the type of data being searched, which in this case is JSON format. Sourcetype helps Splunk understand how to parse the incoming data.

2.

How many log events by the user **Maleena** are captured?

60

✓ Correct Answer

Select Fields

✕

Select All Within Filter

Deselect All

All fields ▾

Filter

Q

+ Extract New Fields

Field

of Values

Event Coverage

Type

>

☐

Source_ip

>100

100%

String

▼

☐

UserName

51

100%

String

Reports

Top values

Top values by time

Rare values

Events with this field

Simon

278

9.713%

James

108

3.774%

Maleena

60

2.096%

3.

What is the name associated with IP 107.14.182.38?

Smith

✓ Correct Answer

>	1/31/22 6:22:08.000 PM	<pre>{ [-] Company: CyberT EventTime: 2022-01-31T18:22:08 Source_Country: United States Source_ip: 107.14.182.38 Username: Smith action: teardown index: VPN_Logs port: 443 protocol: tcp source_state: Tennessee }</pre>
		Show as raw text host = VPN_Connections source = VPN-logs-1663593355154.json sourcetype = _json

4.

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

2814

✓ Correct Answer

Source_Country!=France | stats count as event_count

The screenshot shows the Splunk web interface. At the top, there's a navigation bar with 'splunk>enterprise' and various menu items like 'Apps', 'Messages', 'Settings', 'Activity', 'Help', and a 'Find' search bar. Below this is a secondary navigation bar with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main content area is titled 'New Search' and contains a search bar with the query: `source="VPN-logs-1663593355154.json" host="VPN_Connections" index="vpn_logs" sourcetype="_json" Source_Country!=France | stats count as event_count`. The search results show '2,814 events' and a table with one column, 'event_count', containing the value '2814'.

5.

How many VPN Events were observed by the IP 107.3.206.58?

14

✓ Correct Answer

Source_ip="107.3.206.58"

The screenshot shows the Splunk web interface. At the top, there's a navigation bar with 'splunk>enterprise' and various menu items like 'Apps', 'Messages', 'Settings', 'Activity', 'Help', and a 'Find' search bar. Below this is a secondary navigation bar with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main content area is titled 'New Search' and contains a search bar with the query: `source="VPN-logs-1663593355154.json" host="VPN_Connections" index="vpn_logs" sourcetype="_json" Source_ip="107.3.206.58"`. The search results show '14 events' and a table with one column, 'event_count', containing the value '14'.

Reflection

Working on this Splunk project has enhanced my skills in data manipulation and event analysis. Understanding how to filter and count events based on various criteria is essential for cybersecurity and IT operations. This project highlights my proficiency in using Splunk to gain valuable insights from data and improve overall system security.