What is Splunk?

- One of the leading SIEM (System Information Event Management System) that allows use to collect, analyze and correlate network/machine logs in real time.

Splunk Forward

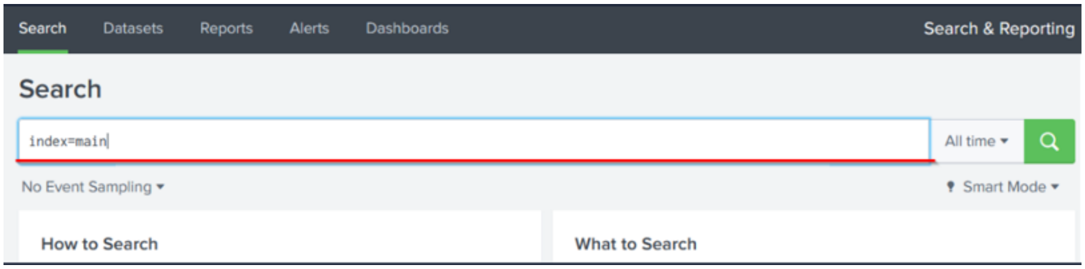
- A lightweight machine that is installed on the endpoint that's collects data and sends it to the Splunk Instance.
    - Web server gathering web traffic
    - Windows Event Logs, PowerShell and Sysmon data.
    - Generating Host Centric Logs for Linux.
    - Generating databases connection request, responses, and errors.

Splunk Indexer

- Parses and normalizes the data into field-value pairs, categorizes it and stores the result as events.

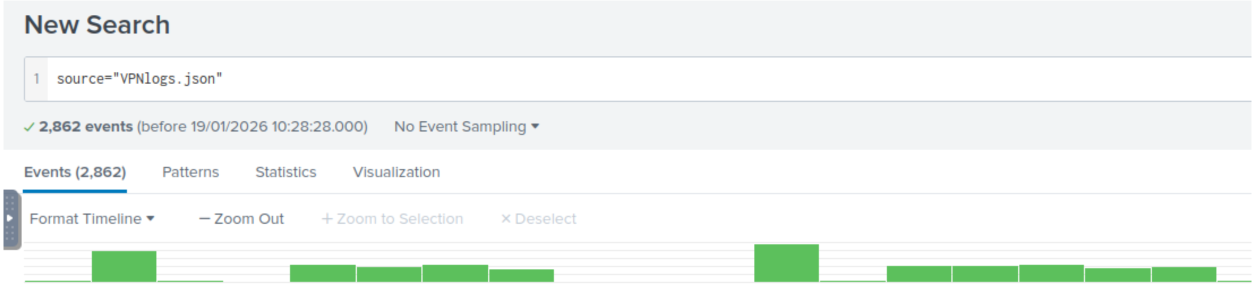
Search Head

- Within the search & reporting app where user can search logs and additional information within the logs.
- When utilizing the Search Head, the user of the SIEM must be mindful that Splunk is case sensitive



```
index=main
```

1. **How many events are presented in the log file?**



New Search

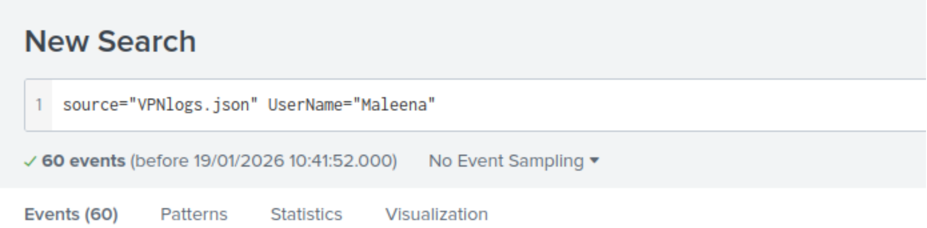
```
source="VPNlogs.json"
```

✓ 2,862 events (before 19/01/2026 10:28:28.000)

Answer: 2,862

- By uploading the .Json file into the Splunk indexer and accessing the log file by typing source=”VPNlogs.json” or source=”VPNlogs.json” | stats count.
- Once the search query is completed, the results will be displayed.

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



New Search

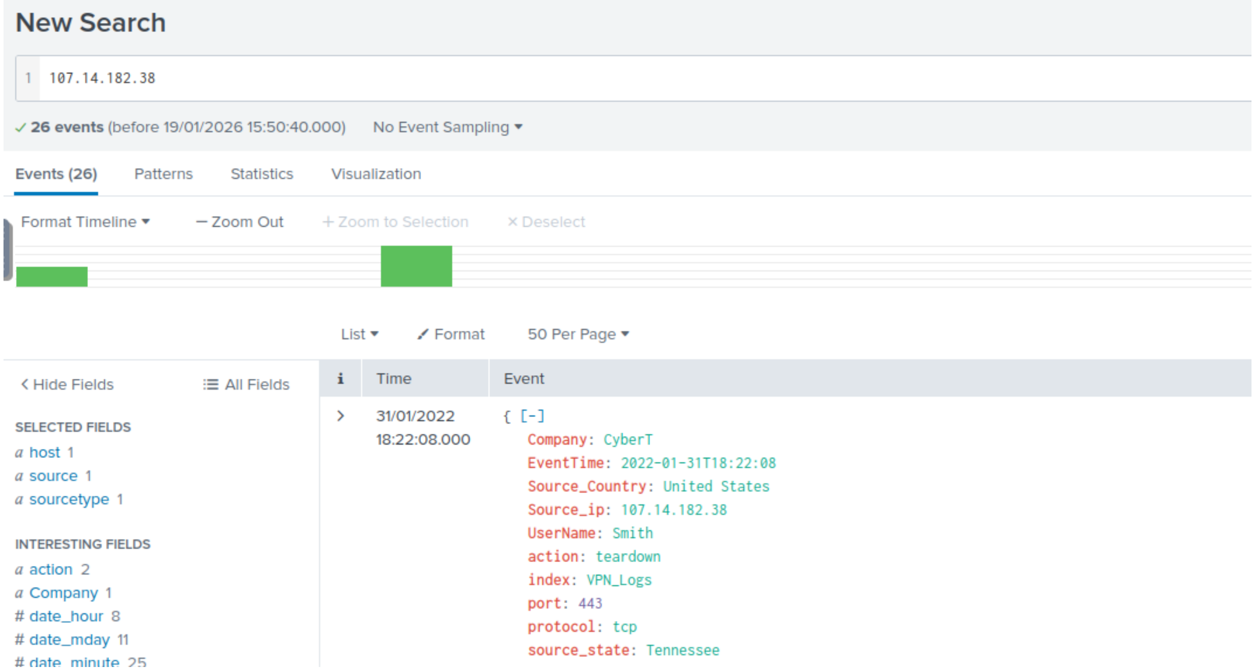
```
source="VPNlogs.json" UserName="Maleena"
```

✓ 60 events (before 19/01/2026 10:41:52.000)

Answer: 60

- In the question, we are looking for a specific user that has generated events in the network or servers.
- You would simply make a search using source=”VPNlogs.json” UserName=”Maleena”
- This Manual filter identifies the specific user and the number of events that have accord in their machine.

3. **What is the username associated with the IP Address 107.14.182.38?**



```
1  107.14.182.38
```

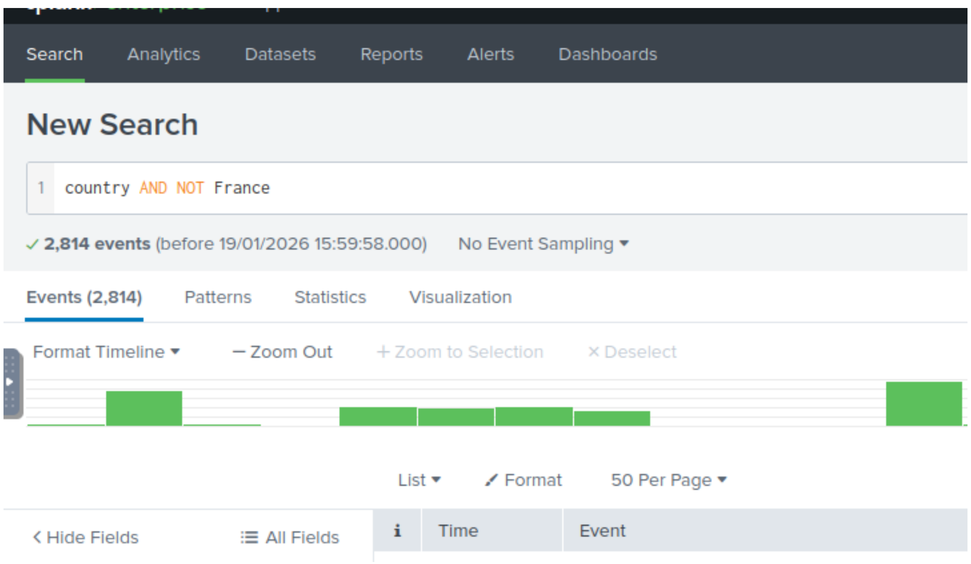
✓ 26 events (before 19/01/2026 15:50:40.000) No Event Sampling ▾

```
31/01/2022 18:22:08.000   { [-]
   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
```

Answer: Smith

- Since the files are fed into Splunk, some searches – such as Ip address – can be searched by inputting the content itself in the search bar.
- Since we are looking for a specific username, the ip address will display the user in the results, as shown above.

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



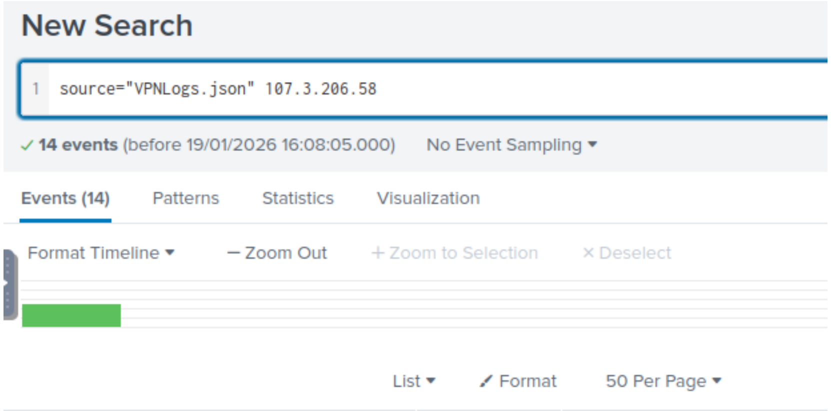
```
1  country AND NOT France
```

✓ 2,814 events (before 19/01/2026 15:59:58.000) No Event Sampling ▾

Answer: 2,814

- For this search, you want to identify the number of events of all countries except for France.
- In the search bar you would input source=”VPNLogs.json” country AND NOT France
- You can also input country AND NOT France
- This will display result of all events occurred from other countries except for France.

5. **How many VPN events were associated with the IP 107.3.206.58?**



New Search

```
source="VPNLogs.json" 107.3.206.58
```

✓ **14 events** (before 19/01/2026 16:08:05.000) No Event Sampling ▾

Answer: 14

- Similar to question 3 - identifying the username that had the ip address 107.14.182.38, we can input the ip address into the search bar and it will populate the number of events that had occurred.
- To search for the number of events, you would input source=”VPNLogs.json” 107.3.206.58