Splunk

Splunk is one of the **leading SIEM solutions** in the market. It allows users to collect, analyze, and correlate network and machine **logs in real time**

Splunk has **three** main components:

1. **Forwarder**
2. **Indexer**
3. **Search Head**

A **Splunk instance** is the main Splunk server that receives, indexes, and analyzes data sent by forwarders.

Splunk Forwarder

Splunk Forwarder is a **lightweight agent** installed on the endpoint intended to be monitored, and its **main task is to collect the data and send it to the Splunk instance** . It does not affect the endpoint's performance as it **takes a few resources** to process

Some of the key data sources are:

- **Web server** generating web traffic.
- **Windows machine** generating Windows Event Logs, PowerShell, and Sysmon data.
- **Linux host** generating host-centric logs.
- **Database generating DB connection** requests, responses, and errors.

The forwarder collects the **data from the log sources** and sends it to the Splunk Indexer.

Splunk Indexer

Splunk Indexer plays the main role in **processing the data** it receives from forwarders.It **parses and normalizes the data into field-value pairs**, categorizes it, and stores the results as **events, making the processed data easy to search and analyze.**

Now, the data, which is normalized and stored by the indexer, can be **searched by the Search Head,**

Search Head

Splunk Search Head is the place within the **Search & Reporting App** where users can search the indexed logs, as shown below. **SPL (Search Processing Language)** is **Splunk's query language** used to search and analyze indexed data.

When a search is run, the **indexer** retrieves matching events and returns them as **field-value pairs**. It means each piece of data is shown as a **field** (like "Username") with its corresponding **value** (like "JohnDoe").

The Search Head also allows you to transform results into presentable tables and visualizations such as pie, bar, and column charts, as shown below:

Splunk Bar: Top panel in Splunk for quick access.

- **Messages:** View system notifications
- **Settings:** Configure Splunk instance
- **Activity:** Track search jobs and processes
- **Help:** Access tutorials and docs
- **Find:** Search across apps
  It also lets users **switch between installed apps** quickly.

Yes, the **Apps Panel** shows all the **apps installed on the Splunk instance/server**. These apps extend Splunk's functionality, like adding dashboards, reports, or specialized data inputs.

default app for every **Splunk installation is Search & Reporting.**

Explore Splunk

The next section is **Explore Splunk** . This panel contains quick links to add data to the Splunk instance, add new Splunk apps, and access the Splunk documentation.

Splunk Dashboard

The last section is the **Home Dashboard**

By default, no dashboards are displayed. You can **choose from a range** of dashboards readily available within your Splunk instance.By default, no dashboards are displayed. You can choose from a range of dashboards readily available within your Splunk instance.

Splunk can ingest almost any type of data, not just logs.
It can take in **structured**, **unstructured**, and **semi-structured** data — like:

1. System and application logs
2. Network traffic data
3. JSON, CSV, XML files
4. Metrics, alerts, or sensor data
5. Even text files, API outputs, or database records

when data is added to Splunk, the data is processed and transformed into a series of individual events. The data sources can be event logs, website logs, firewall logs, etc. The **data sources are grouped into categories.**