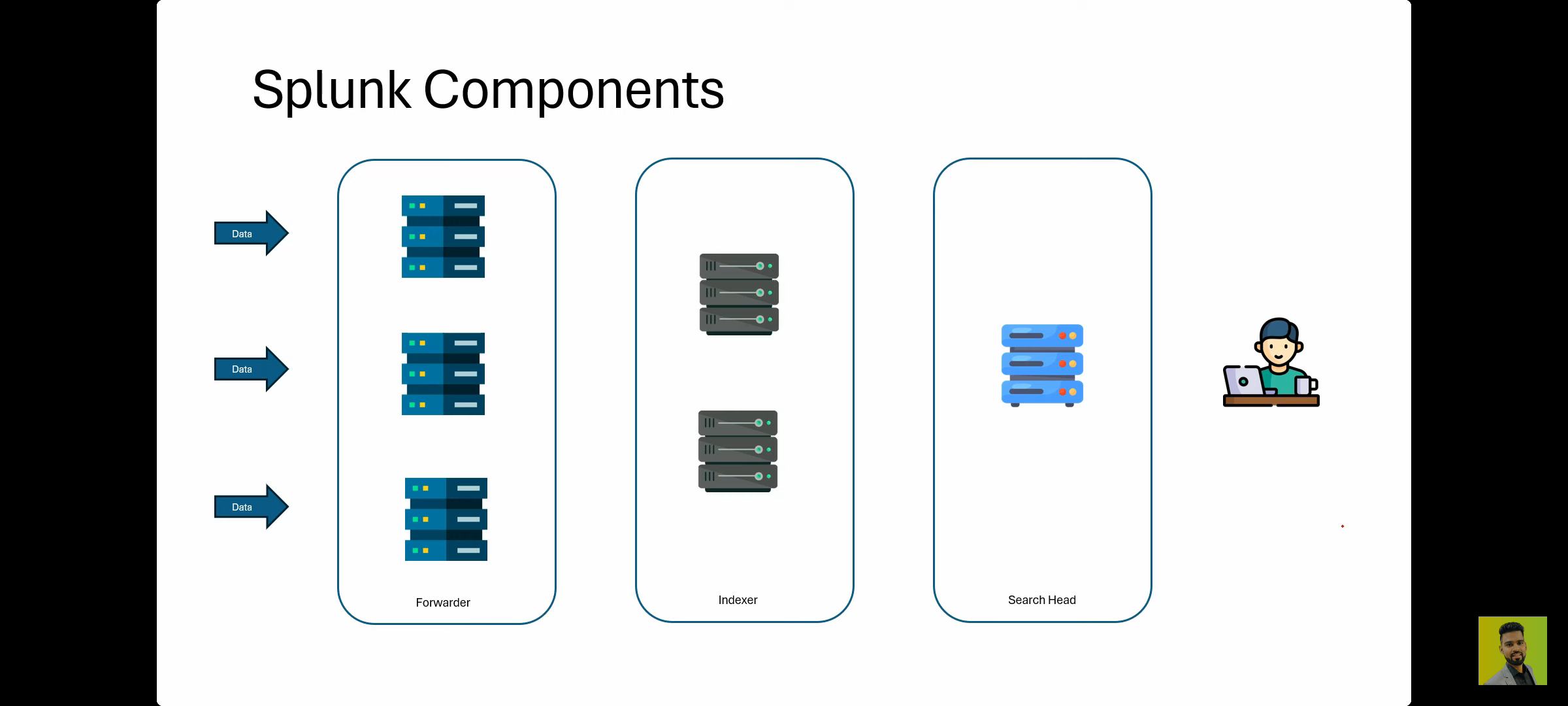


Collescts data and indexes it from al the different sources cloud, OS, databases

Mm

1. The process of transforming data is called Indexing.



1. Above pic

## Forwarder

* A forwarder is a lightweight agent that collects data from various sources (like logs, metrics, etc.) and sends it to a central location for analysis.
* Think of it like a messenger who gathers information from different places and sends it to headquarters for processing.

## Index

* An index is like a massive database that stores all the data sent by the forwarders.
* It's where Splunk stores and organizes the data, making it searchable and analyzable.
* Think of it like a massive library where all the information is stored and categorized.

## Search Head

* A search head is the user interface where you search, analyze, and visualize the data stored in the index.
* It's like the research desk where you ask questions, get answers, and create reports based on the data in the library (index).