INTRODUCING SPLUNK

KARTHICK SELVAM

INTRODUCING SPLUNK

- **Splunk**, whose name was inspired by the process of exploring caves, or splunking, helps analysts, operators, programmers, and many others explore data from their organizations by obtaining, analyzing, and reporting on it.
- This multinational company, cofounded by Michael Baum, Rob Das, and Erik Swan, has a core product called **Splunk Enterprise.**
- This manages searches, inserts, deletes, and filters, and analyzes big data that is generated by machines, as well as other types of data.
- They also have a free version that has most of the capabilities of Splunk Enterprise and is an excellent learning tool.

WHAT IS SPLUNK?

- Log Collection OR Log Management.
- Infrastructure Monitoring Tool.
- Application Performance Monitoring Tool.
- Big Data.
- SIEM (Security Information and Event Management).
- Operation Intelligence.
- Google for your Data.

DIFFERENT PRODUCTS OF SPLUNK

- Splunk Enterprise(Any Size Organization)
  - Splunk Enterprise is the easiest way to aggregate, analyze and get answers from your machine data.
- Splunk Cloud(Delivered in the Cloud)
  - Deploy Splunk securely, reliably and scalably as a service. No infrastructure required.
- Splunk Light(Small IT Environments)
  - The comprehensive solution for small IT environments looking to automate log search and analysis.

DIFFERENT PRODUCTS OF SPLUNK

- Splunk IT Service Intelligence (ITSI)
  - Simplify operations, prioritize problem resolution and align IT with the business using a monitoring and analytics solution tailored for today's environments
- Splunk Insights for AWS Cloud Monitoring
  - Don't lose sight or control of your data. Enjoy end-to-end security, operational and cost-management insights for your AWS workloads
- Splunk App for Infrastructure
  - Unify and correlate logs and metrics on one solution. Get free comprehensive infrastructure monitoring, alerting and investigation with your Splunk Enterprise license.

DIFFERENT PRODUCTS OF SPLUNK

- Splunk Enterprise Security
  - Gain end-to-end visibility into your security posture with actionable intelligence that helps you prioritize and act fast Make Better Security Decisions
- Splunk User Behavior Analytics
  - Protect against insider threats with machine learning-powered user and entity behavior analytics. Find Anomalous Behavior
- Phantom
  - Marshall the full power of your existing security investment using the Phantom Security Operations Platform. Supercharge Your Security
- Splunk Insights for Ransomware
  - Don't pay. Be prepared to combat ransomware with an additional layer of security to help combat persistent and new strains of malware. Get Ready

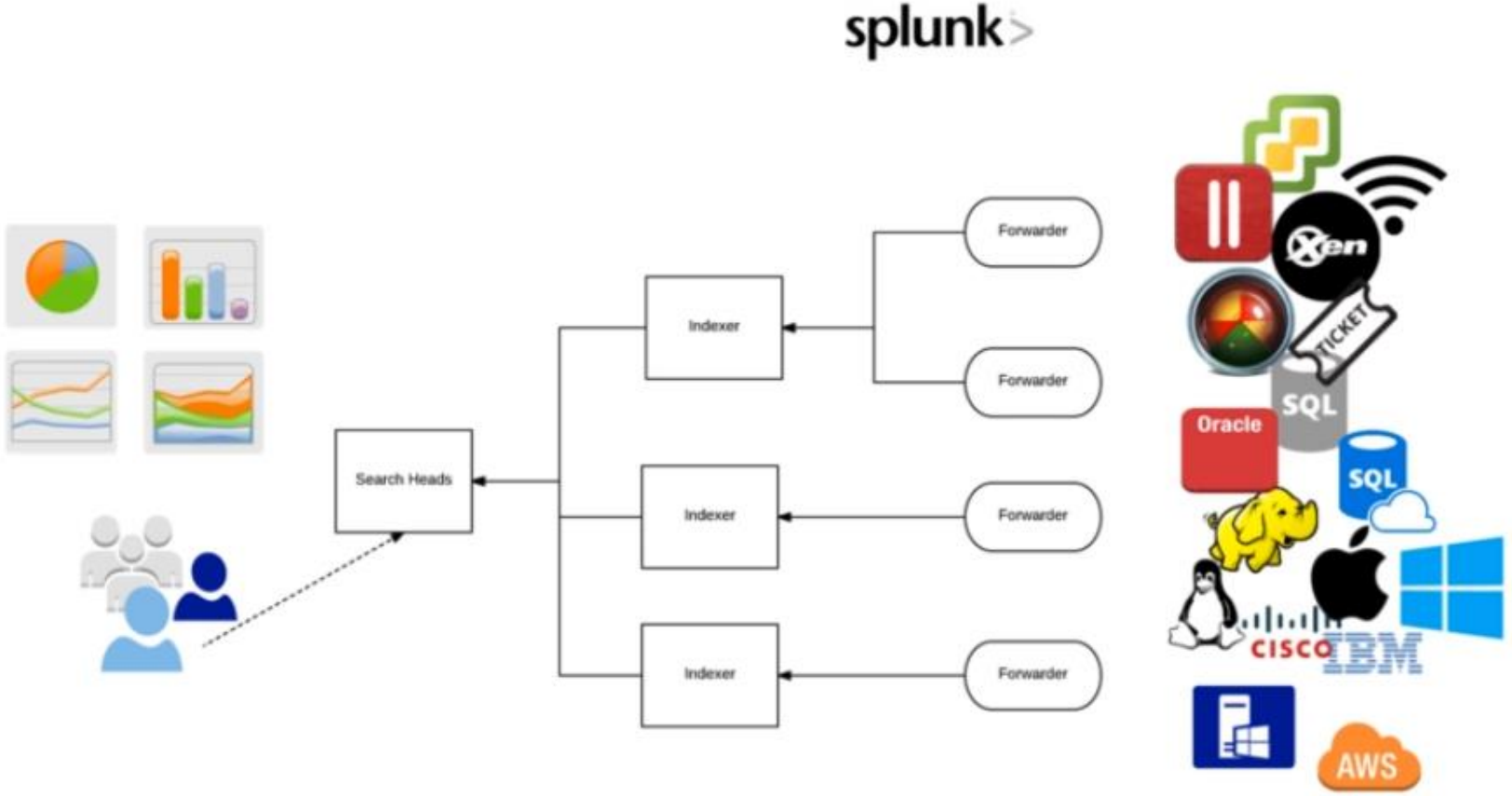
TO LEARN SPLUNK, IT IS IMPORTANT FOR YOU TO FIRST UNDERSTAND THE FOLLOWING CONCEPTS

- How to install Splunk for different operating systems and use it for the first time
- How Splunk works with big data
- Data sources for Splunk
- Events, event types, and fields in Splunk
- How to add data to Splunk

COMPONENTS OF SPLUNK ENTERPRISE

- Search Head.
- Indexer.
- Universal Forwarder.
- Heavy Forwarder.
- License Manager.
- Deployment Server.
- cluster Master.

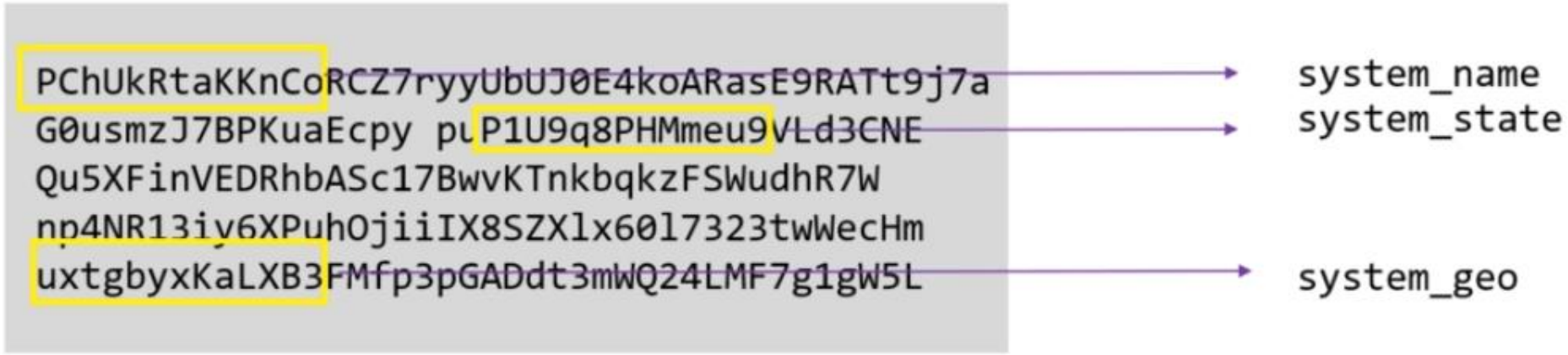
What is Splunk? >



What is Splunk? >

```
PChUkRtaKKnCoRCZ7ryyUbUJ0E4koARasE9RATt9j7a
G0usmzJ7BPKuaEcpy puP1U9q8PHMmeu9VLd3CNE
Qu5XFinVEDRhbASc17BwvKTnkbqkzFSWudhR7W
np4NR13iy6XPuhOjiiIX8SZXlx60l7323twWecHm
uxtgbyxKaLXB3FMfp3pGADdt3mWQ24LMF7g1gW5L
```

What is Splunk? >



What is Splunk? >

Platform	Data	Primary sources	Real-time?	User Friendliness?	Enterprise Licensing Costs
Splunk	Unstructured & Structured	IT Systems	Near	3/5	$$$$
BI Tools	Structured	Databases	Usually No	4/5	$$$

Splunk Deployment Models >

Basic Components of a Splunk deployment

- Search head
  - Handles search requests and consolidating results back to the user
- Indexer
  - Takes raw data from forwarders, turns it into events, and places the results into an index, which is stored in a bucket.
- Forwarder
  - Forwards raw data to other parts of the deployment.

Splunk Deployment Models >

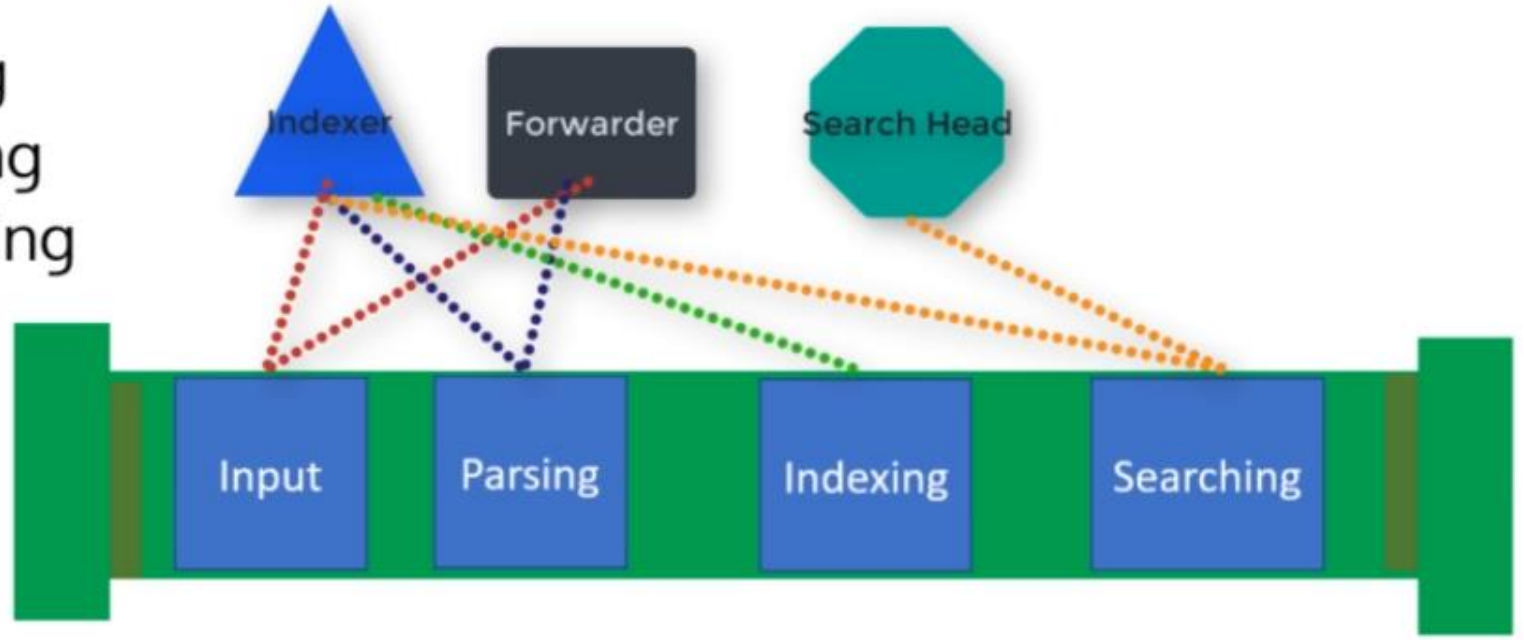
- Variety of configurations
- Data pipeline has four components
  - **I**nput
  - **P**arsing
  - **I**ndexing
  - **S**earching

Splunk Deployment Models >

- Variety of configurations
- Data pipeline has four components
  - **I**nput
  - **P**arsing
  - **I**ndexing
  - **S**earching

Splunk Deployment Models >

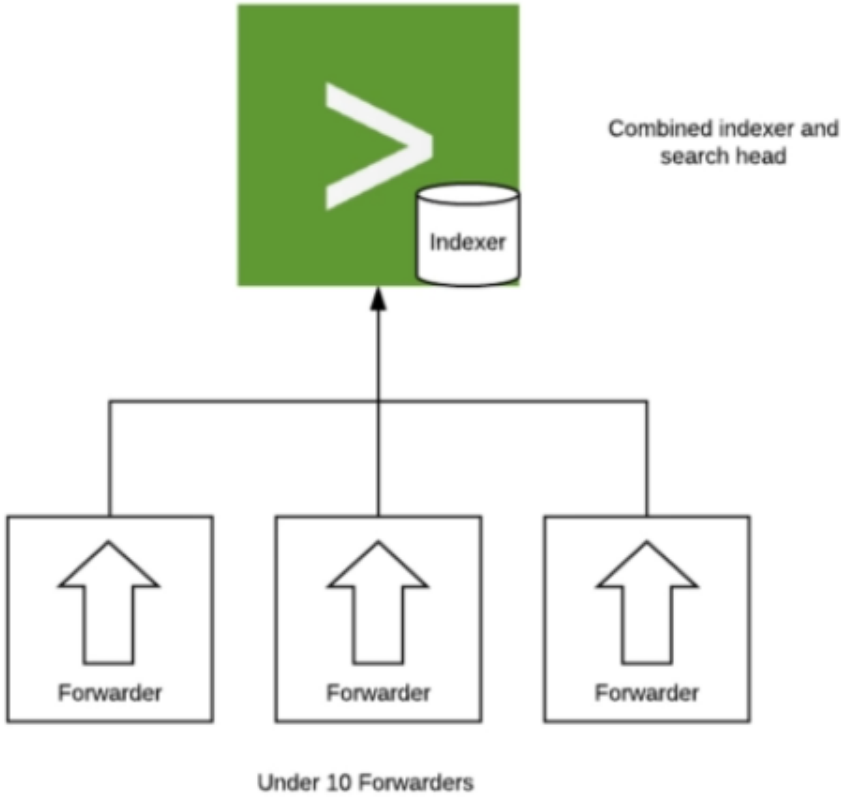
- Variety of configurations
- Data pipeline has four components
  - **I**nput
  - **P**arsing
  - **I**ndexing
  - **S**earching



Splunk Deployment Models >

Departmental Deployment

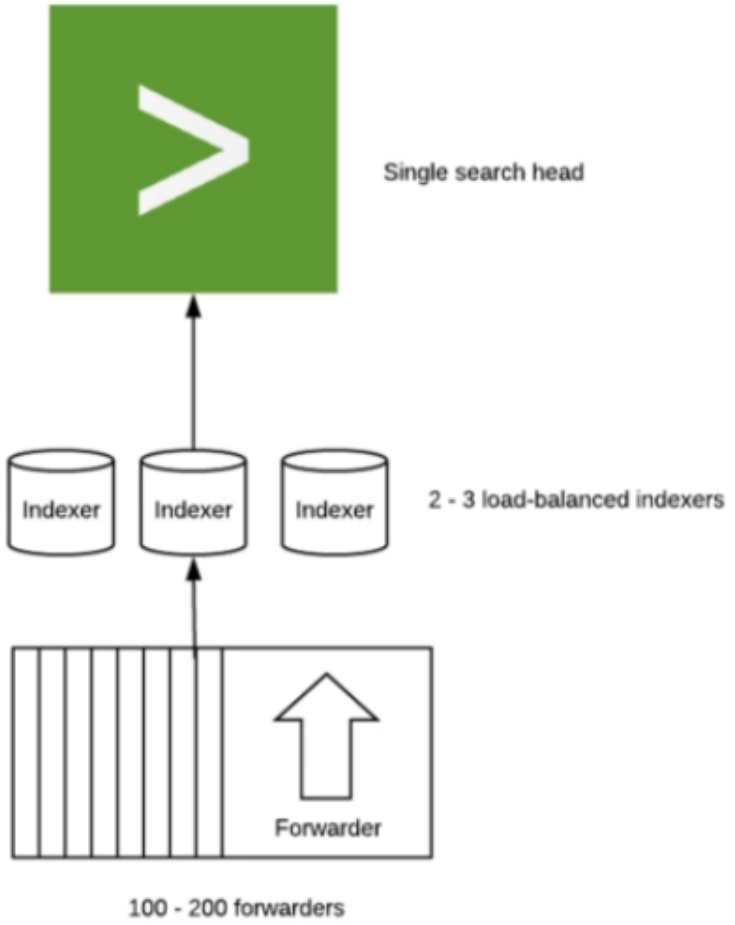
- A single search head/indexer
- Up to 10 forwarders
- Appropriate for up to 10 users



Splunk Deployment Models >

Small Enterprise Deployment

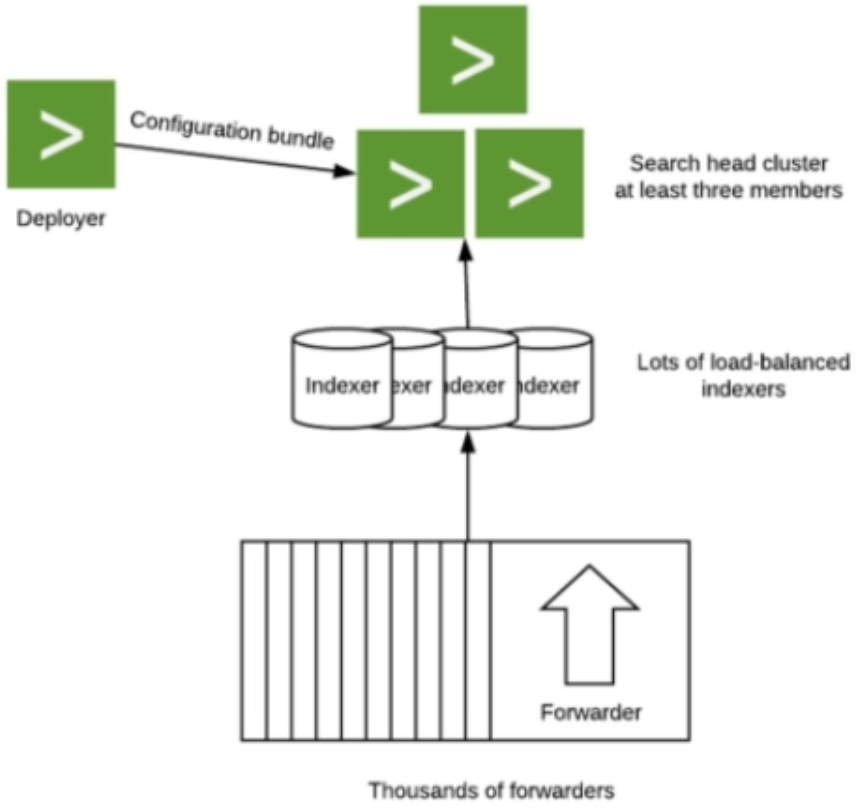
- A single search head
- Two to three indexers
- 100 to 200 forwarders



Splunk Deployment Models >

Large Enterprise Deployment

- Search head cluster
- Lots of indexers
- Thousands of forwarders
- A deployer



Splunk Deployment Models >

Deployment Server Architecture