

Splunk Overview

Author: Nho Luong
Skill: DevOps Engineer Lead




Nho Luong
has successfully passed all requirements for
Microsoft Certified: Azure Solutions Architect Expert

Credential ID: 3CF3D14D253FE551
Certification number: 46F8FB-7D3F5B
Earned on: June 14, 2024
Expires on: June 15, 2025

Online Verifiable



Satya Narayana Nadella





nho luong
AWS Certified Solutions Architect - Professional

VALIDATION NUMBER: 119ee670510e4bb99fe2956152effb7e
VALIDATE AT: <https://aws.amazon.com/verification>

Issue Date: June 21, 2024
Expiration Date: June 21, 2027





HOME

PROFILE

EXAM REGISTRATION

EXAM HISTORY

CERTIFICATIONS

Certification status

Agreement

BENEFITS

DIGITAL BADGES

SUPPORT AND FAQs

Certification status

Active

PROFESSIONAL

AWS Certified Solutions Architect - Professional

SAP

ACTIVE DATE
2024-06-21

EXPIRATION DATE
2027-06-21

VIEW MORE

Active

SPECIALTY

AWS Certified Security - Specialty

SCS

ACTIVE DATE
2024-06-19

EXPIRATION DATE
2027-06-19

VIEW MORE

Active

PROFESSIONAL

AWS Certified DevOps Engineer - Professional

DOP

ACTIVE DATE
2024-06-17

EXPIRATION DATE
2027-06-17

VIEW MORE

Active

ASSOCIATE

AWS Certified Solutions Architect - Associate

SAA

ACTIVE DATE
2024-06-15

EXPIRATION DATE
2027-06-21

VIEW MORE

Active

FOUNDATIONAL

AWS Certified Cloud Practitioner

CLF

ACTIVE DATE
2024-05-27

EXPIRATION DATE
2027-06-21

NHO LUONG

AWS04440050

Activity

Training

Plans

Challenges

Credentials

Q&A


Achievements

Collections

Transcript

4 items

Sorted by expiration date




CERTIFICATION

Microsoft Certified: DevOps Engineer Expert

Expires on June 15, 2025 at 6:59 AM (UTC +07:00) • Earned on June 14, 2024

View certification details




CERTIFICATION

Microsoft Certified: Azure Solutions Architect Expert

Expires on June 15, 2025 at 6:59 AM (UTC +07:00) • Earned on June 14, 2024

View certification details




CERTIFICATION

Microsoft Certified: Azure Administrator Associate

Expires on June 15, 2025 at 6:59 AM (UTC +07:00) • Earned on June 14, 2024

View certification details



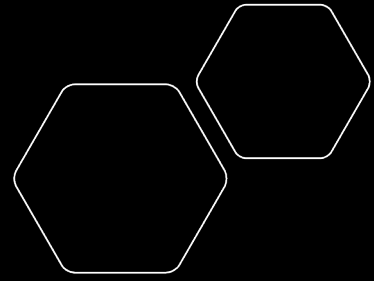
CERTIFICATION

Microsoft Certified: Azure Fundamentals

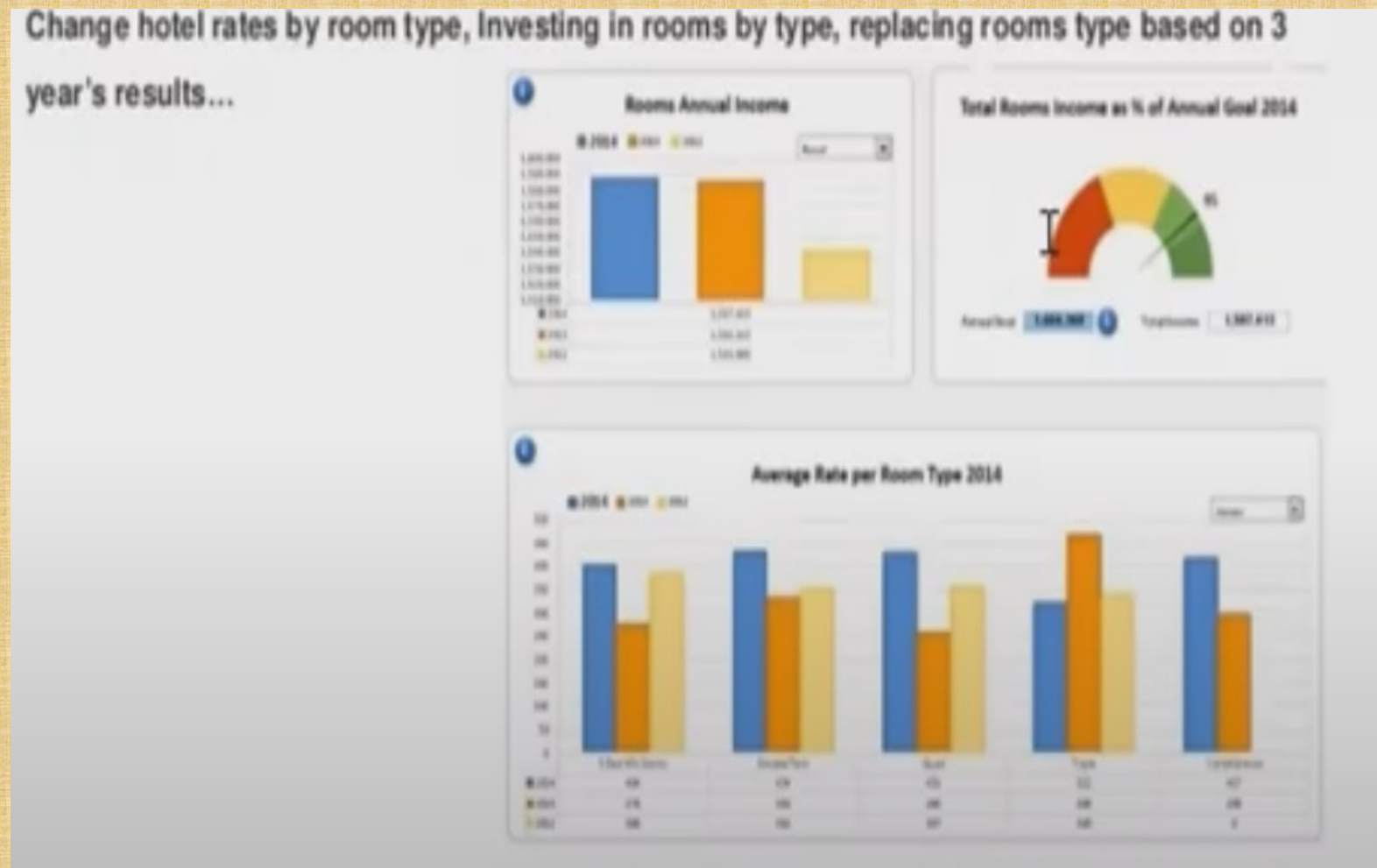
Earned on May 24, 2024

View certification details

- Difference between Business Intelligence and Operational Intelligence



Business Intelligence

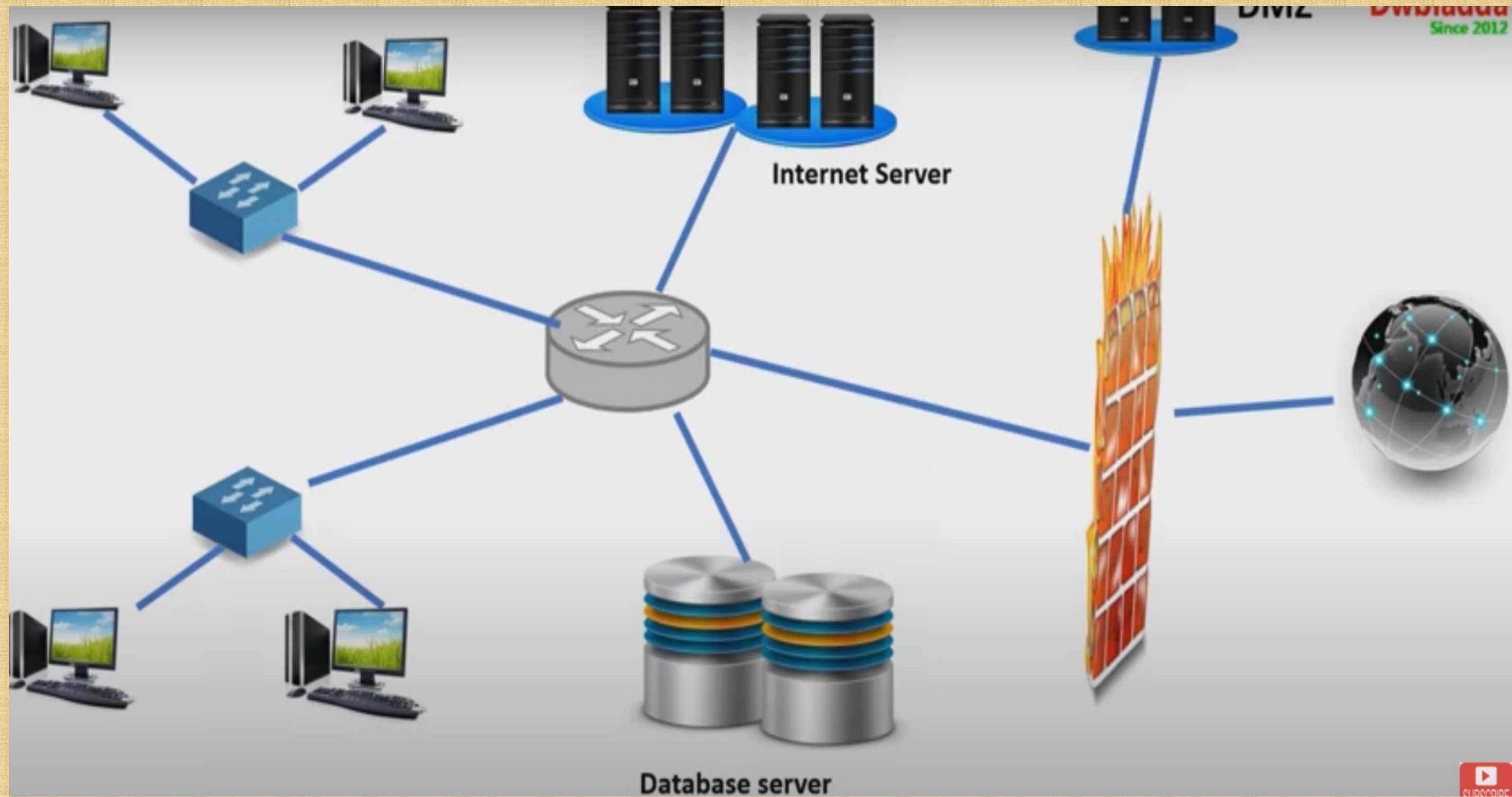


Operational Intelligence

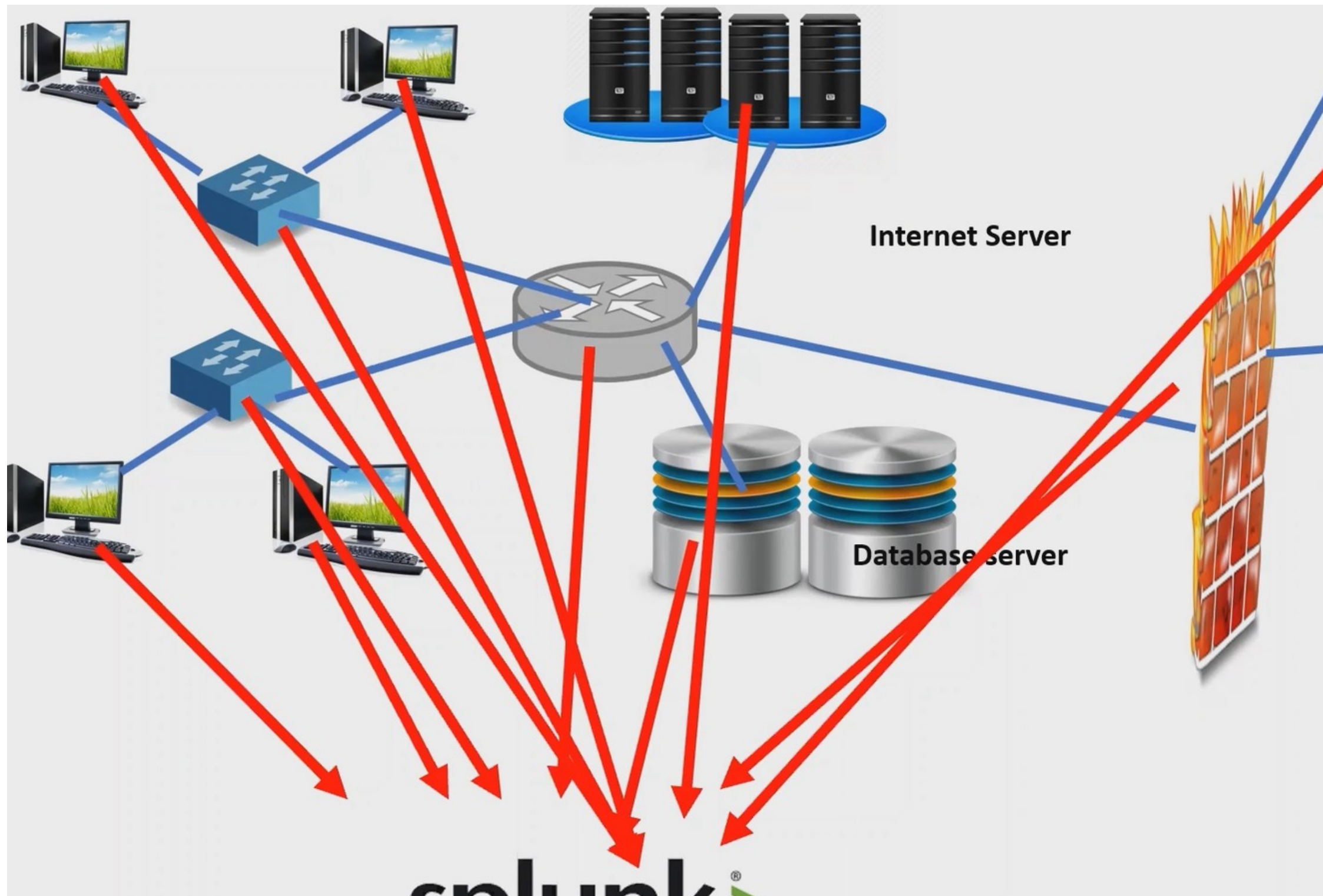
Alert: Your computer is running with High Memory Utilization : 80%

Alert: Your computer is running with High Memory Utilization : 90%

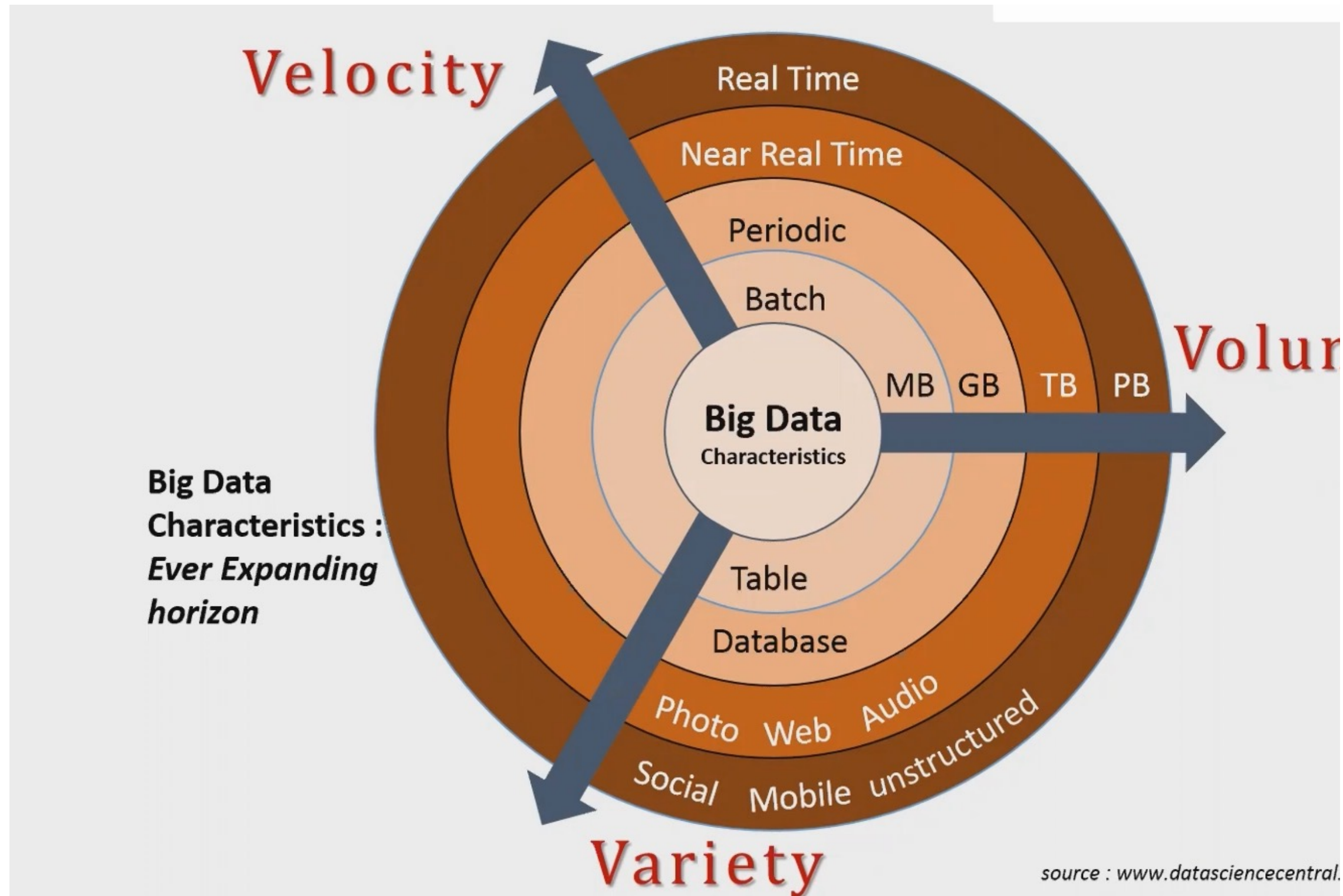
Alert: Your computer is running with High Memory Utilization : 95%



Splunk role



Big Data





Splunk Component

- Splunk is comprised of three main processing components:



Indexer



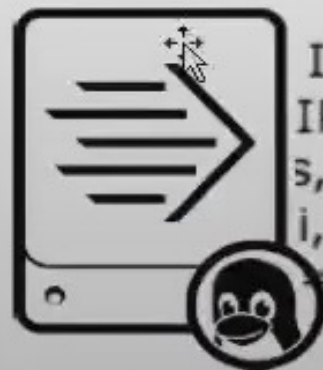
Search Head



Forwarder

Splunk Components – Forwarders

- Splunk Enterprise instances that consume and send data to the index
- Require minimal resources and have little impact on performance
- Typically reside on the machines where the data originates
- Primary way data is supplied for indexing



Web Server
with Forwarder Instance

IP = 10.3.10.6, Session disconnected. Session type = TPsecOver
IP = 10.1.10.216, Session connected. Session type = SSL, Dura
s, IP = 10.1.10.133, Session connected. Session type = IKE, Dur
i, IP = 10.3.10.18, Session disconnected. Session type = IKE, D
= 10.1.10.211, Session connected. Session type = SSL, Duration



Indexer

Splunk Components - Indexer

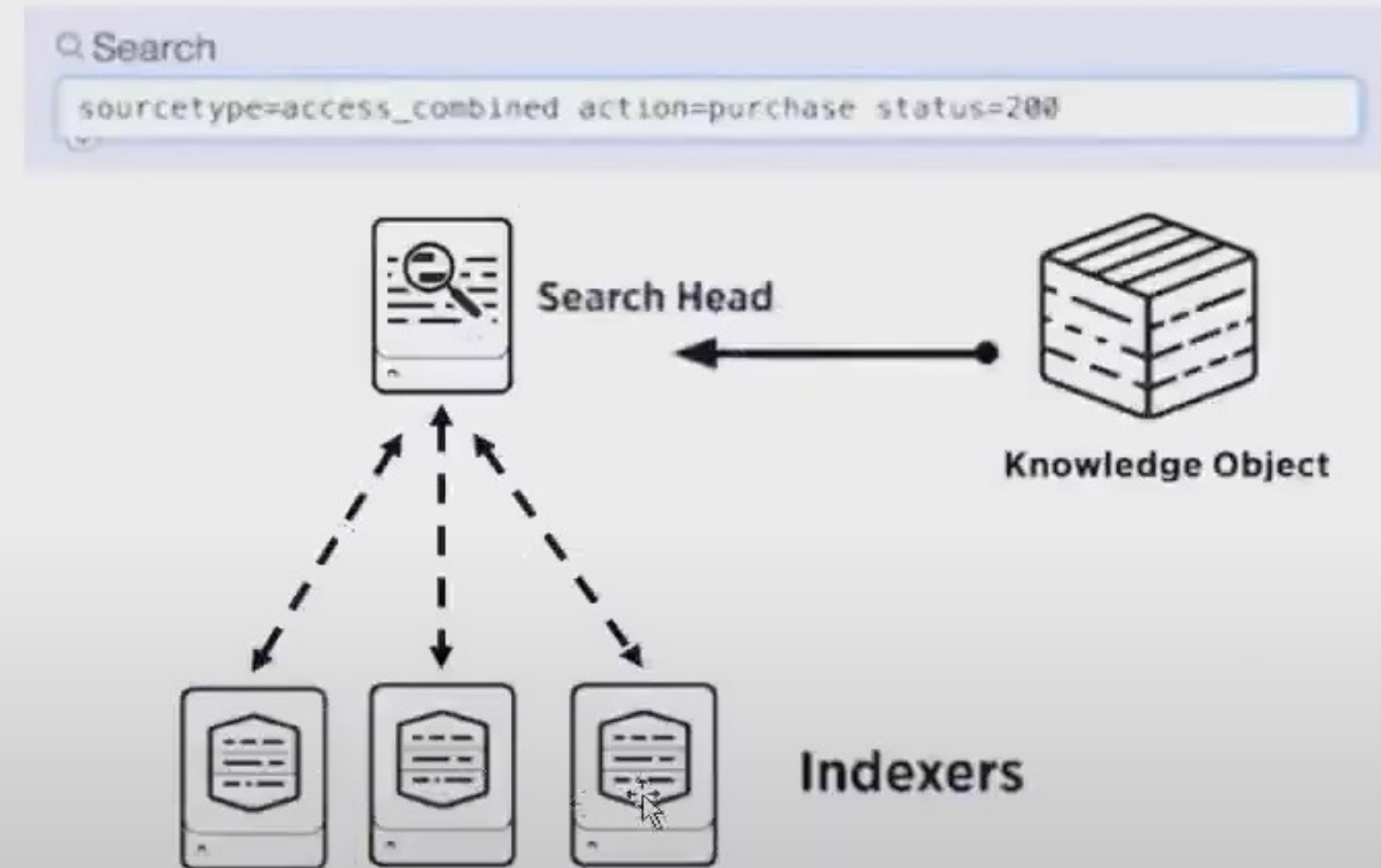
- Processes machine data, storing the results in Indexes as events, enabling fast search and analysis



- As the Indexer indexes data, it creates a number of files organized in sets of directories by age
 - Contains raw data (compressed) and Indexes (points to the raw data)

Splunk Components – Search Heads

- Allows users to use the Search language to search the indexed data
- Distributes user search requests to the Indexers
- Consolidates the results and extract field value pairs from the events to the user
- Knowledge Objects on the Search Heads can be created to extract additional fields and transform the data without changing the underlying Index data



- Splunk Enterprise

Splunk components installed and administered on-premises



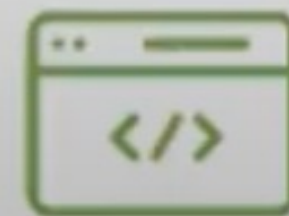
- Splunk Cloud

- Splunk Enterprise as a scalable service
- No infrastructure required



- Splunk Light

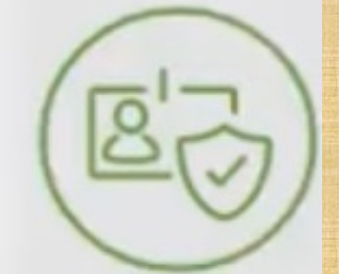
Solution for small IT environments



What are Splunk Enhanced Solutions?

- **Splunk IT Service Intelligence (ITSI)**
 - Next generation monitoring and analytics solution for IT Ops
 - Uses machine learning and event analytics to simplify operations and prioritize problem resolution
- **Splunk Enterprise Security (ES)**
 - Comprehensive Security Information and Event Management (SIEM) solution
 - Quickly detect and respond to internal and external attacks
- **Splunk User Behavior Analytics (UBA)**

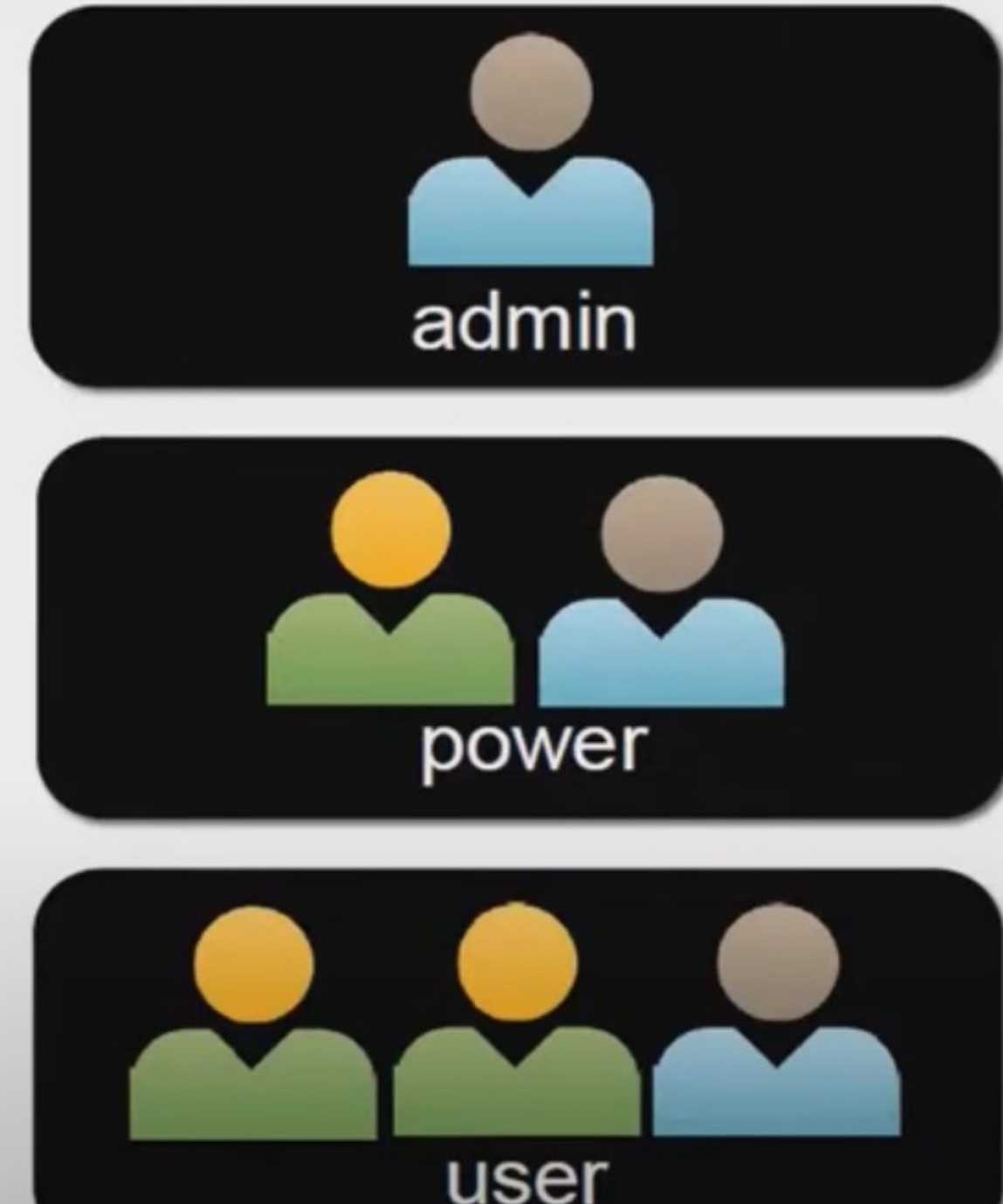
Finds known, unknown, and hidden threats by analyzing user behavior and flagging unusual activity



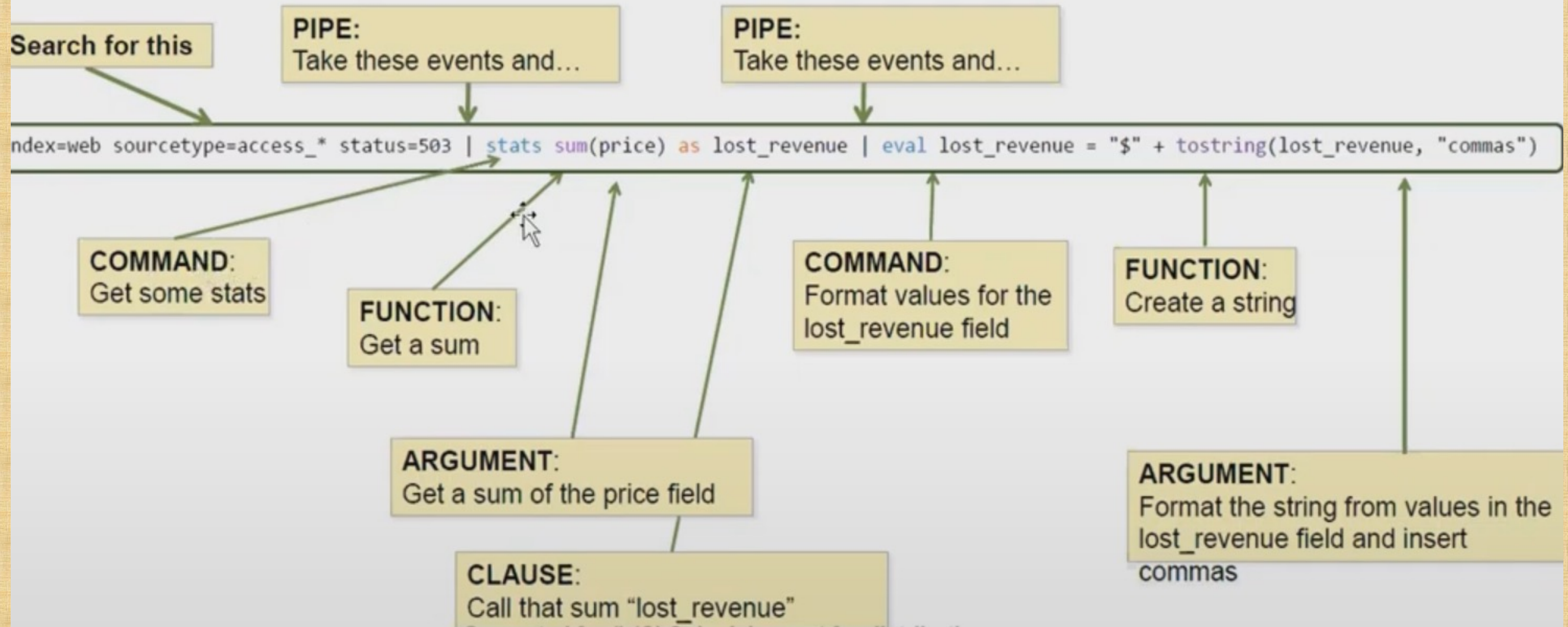
Users and Roles

DevOps
Since 20

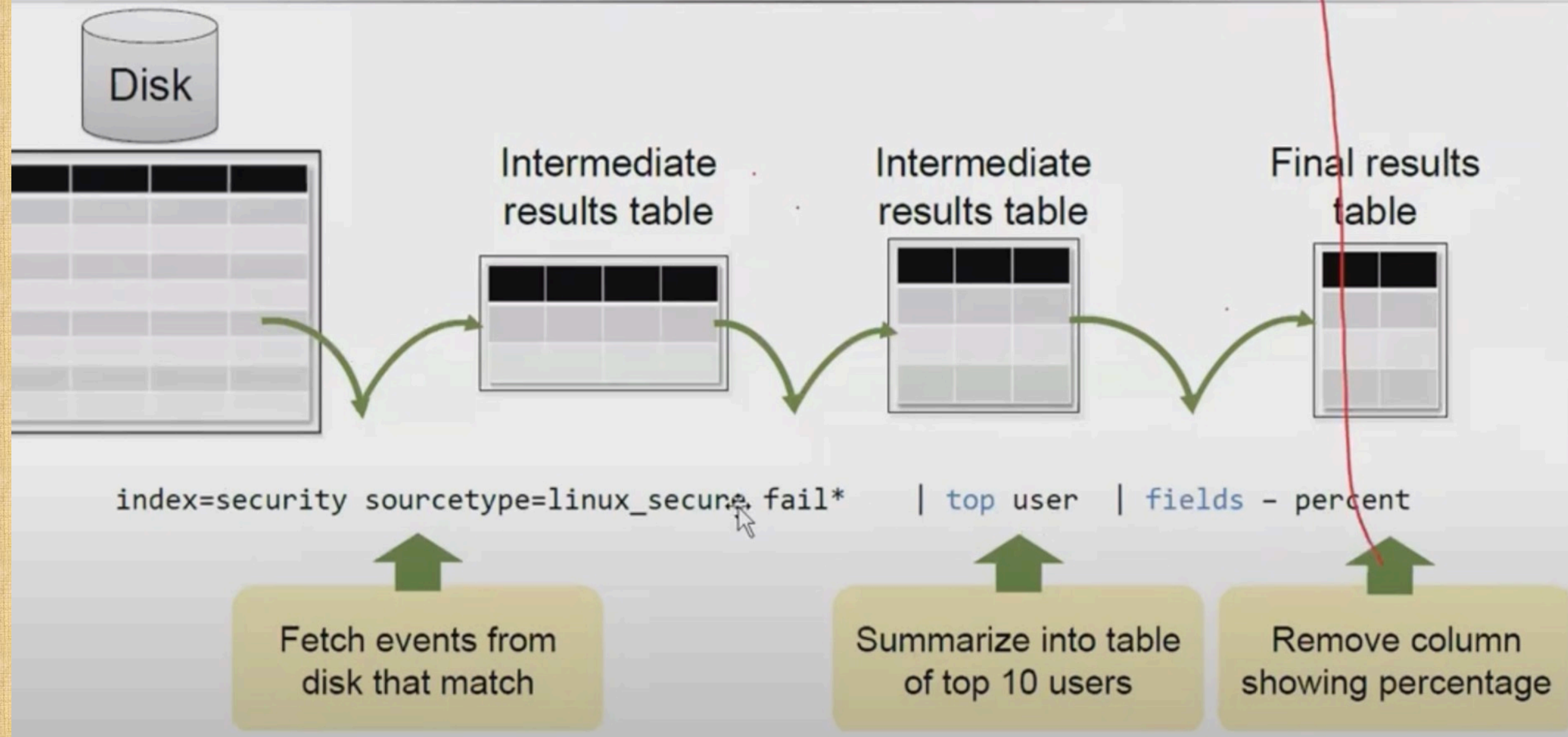
- Splunk users are assigned roles, which determine their capabilities and data access
- Out of the box, there are 3 main roles:
 - Admin
 - Power
 - User
- Splunk admins can create additional roles



This diagram represents a search, broken into its syntax components:



The Search Pipeline



stats Command

- stats enables you to calculate statistics on data that matches your search criteria
- Common functions include:
 - count – returns the number of events that match the search criteria
 - distinct_count, dc – returns a count of unique values for a given field
 - sum – returns a sum of numeric values
 - avg – returns an average of numeric values
 - list – lists all values of a given field
 - values – lists unique values of a given field



Thank You