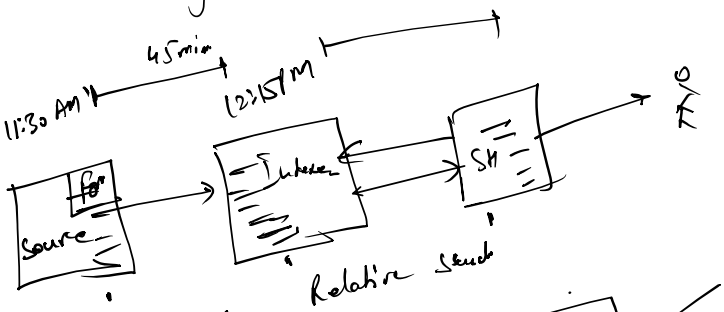
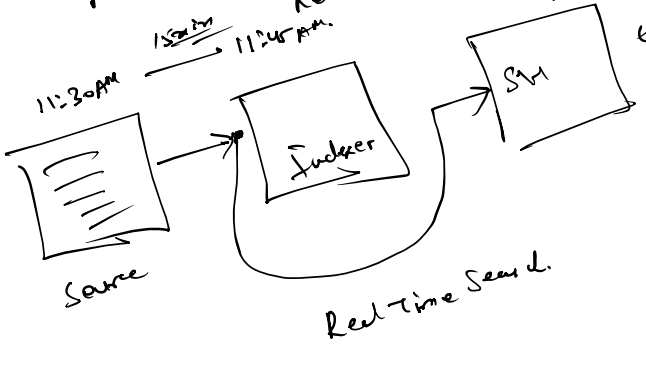
Day - 2

16 September 2025 10:08

Visualization → Geo Visualization (Map)
→ Single Value
→ XY map (Bar, column, pie chart)

(1) chart:- | chart count by current_ticket_state |
count → y-axis
current_ticket_state → x-axis



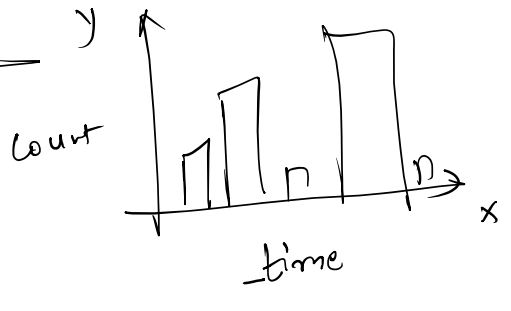


1. Huge load on Indexer.
2. Not use / Avoid in Real time search.
1 min, 2 min

1. Time when event is generated.
2. Time when data is indexed.

[_time = event generated - index_time = index time] → Delay

(2) Time chart:-



|timechart count by severity,
Span = 1d → every one day,
= 1 mon → every one month
↓
interval

time

interval.

hour = H

Day - d
month = mon.
year = y
minute = M
second = S

③ Single Value Visualization —

| stats count.

④ GeoMap :- Coordinates to pin on the Geographical Map.

Latitude — Longitude.

⑤ Custom App :- We can install the custom App from the Appstore

App → Splunk supported → Created by Splunk.
→ Cisco supported → Created by cisco.
→ Developer supported → 3rd party / individual contributor.
→ No support.

Top & Rare Commands —

Top Value over here.

| top Sourcetype → Top 10 sourcetype by default.

| top limit = 3 Sourcetype → to define the no. of values.

| top limit=3 sourcetype

limit=3 → Top 3 values

| top limit=0 sourcetype

→ All the values

Rare:- least values.

| rare sourcetype.

| least value=

Addtotals:- Row wise addition.

Addcoltotals:- Column wise addition.

Dedup:- Remove duplicate values

Sort:- Sorting purpose.

| sort field1

↳ By default → Ascending order

| sort - field1

↳ Descending order

Search:- where you want to filter a particular value of the field.

Where:- when you want to compare two diff field.

| current_ticket.state = "closed"

a	b
5	10
3	15
35	5
7	4

| where a>b

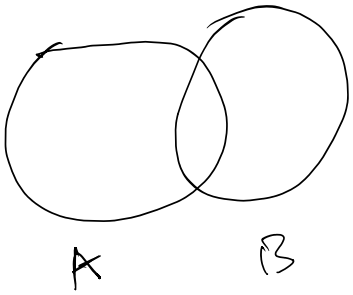
o/p

a	b
35	5
7	4

Rex:-

|rex field="____" "regular expression"

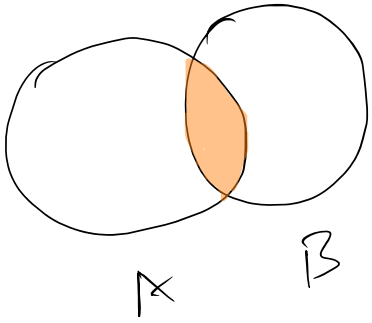
join:- join two different dataset.



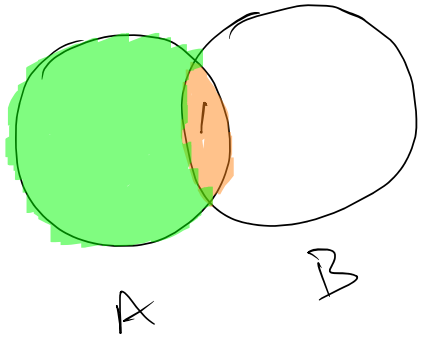
Unique field, it will combine both dataset.

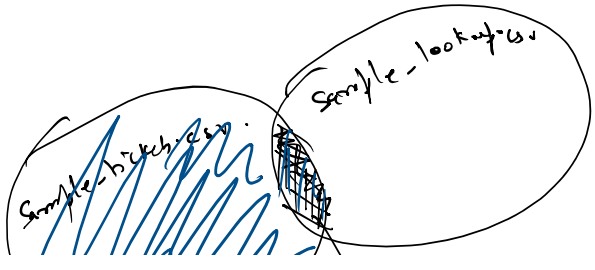
1) Inner join.
2) left/ outer join.

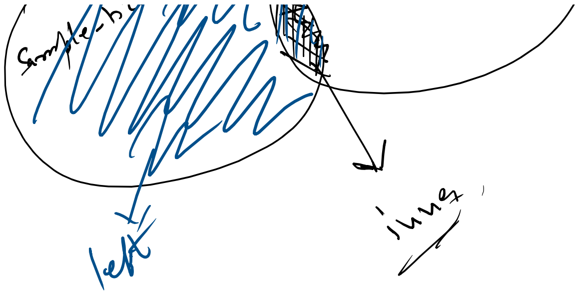
1) Inner join



2) left join:-







fields: include or exclude the specific field.

fields - f1 → exclude.

fields + f1 → include.

Head → first 5 value → head 5

tail → last 5 values ⇒ tail 5

reverse → flip the o/p.

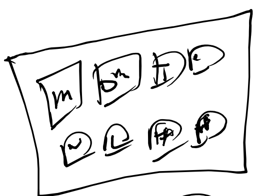
% → $\frac{x}{y} \times 100\%$ → % value,

fields -+, -

table percentage

Tomorrow

1. Knowledge object.



1. Tags & eventtype
2. Lookup
3. field extraction.
4. calculated field.
6. Workflow Action.
7. Macros.
8. Data model & Pivot

(3) field ex
(4) Calculated field-
(5) field Assign