Day - 2

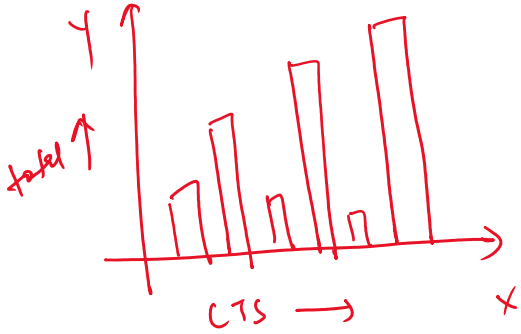
03 December 2024 10:02

1. Command :-

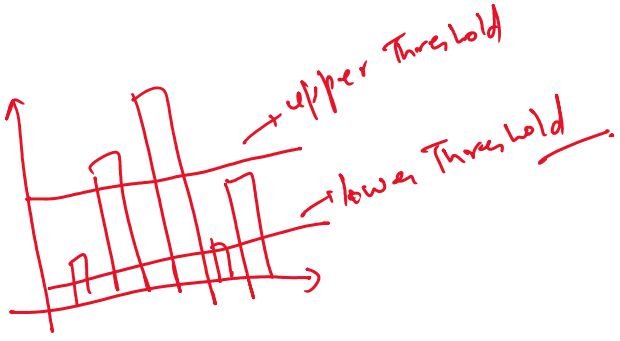
.#£

1. chart.
2. timechart
3. Date & Time func".
4. Visualization.
5. Custom Visualization.
6. Append | Appendpipe | Appendcol
7. join.
8. Rex
9. Addtotal | Addcoltotal.
10. Top | Rare.
11. field.
12. where | search.

1. Chart → | Chart Y over X



10^x = 10, 100, 1000, 10000, ---



2. Time chart :- | timechart count by CTS

1. By default x-axis is reserved for _time field.

09-09-09 09:09:09

APAC → %d-%m-%y
EMEA → %y-%m-%d
US → %m-%d-%y

Datetime → epoc Datetime

Datetime → App/user generated field.

epoc Datetime → system Understandable Format

Datetime function → strptime → Parse Datetime field.

Datetime function → strftime → Format Datetime field.

D1 D2

(D2 - D1) + D1_epoc

D2_epoc - D1_epoc) → correct

(D2_epoc - D1_epoc)

GeoMap → Define the points on the GeoMap.

Coordinates → Latitude, longitude.

Index (VK_idx) → Sourcetype (csv) → Source1 (Sample_tickets.csv)

Sourcetype (csv) → Source2 (Vendors.csv)

→ Checkpoint b/f installing the App from Splunk Appstore:-

1. Compatibility – Splunk Enterprise, Splunk cloud, Version of Splunk
2. Creater of App → Developer (3rd Party)

2. Creater of App → Developer (3rd party)
→ Splunk Inc. (from splunk itself)

Rex:- Ingest data in splunk. Unable field extracted.
Manually write regular expression. to extract field.
|rex field=_raw "regular expression"

Top & Rare:-

Top:- |top fieldname
Top values (default top 10 values)
limit = 3 → Top 3 value
limit = 5 → Top 5 values.
limit = 0 → Top value for all (Descending order)

fieldname	count	Percent

→ These 3 field will be coming as output.

Rare:- Syntax exactly the same as top
Rare will give the least value (Ascending order)
column o/p → field-name, count, percent

field:- It will include or exclude the field from the o/p.
|field - fi

field:- It will include or exclude ...]

| fields - f1

Addcoltotal | Addtotal:-

Addtotal:- Do the addition Row wise.

Addcoltotal:- Do the Addition of Numeric value columnwise.

Search & where:- Both commands are used for filtering Purpose.

| search a>3 → filter the value in the same field.

a	b
5	7
4	8
3	9
2	1
7	2

→ o/p

a	b
5	7
4	8
7	2

| where a > b → Compare the value of two diff. fields.

a	b
7	2

Append | Appendcol | Appendpipe:-

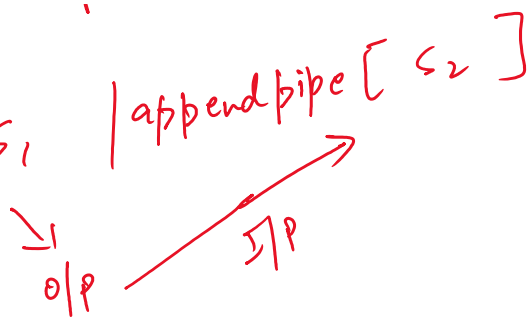
Append:-

s1 | append [search s2] → Combine the o/p of two searches.

a	b	c	d

... dpipe [s2]

Appendpipe :-

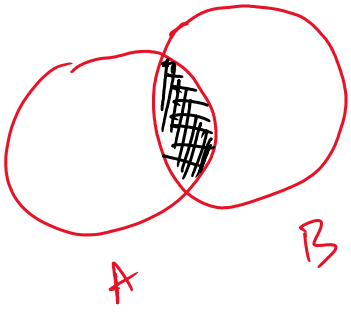


join :- Combine the data from two/more index.

① Inner join.

② Left join.

① Inner join :-



② Left join :-