Day - 2

16 July 2024 10:07

Assignment - 2

FC

O/P

CTS

Completed — Closed — 10] → 30
Resolved — 20

Incomplete — Inprogress — 5] → 25
Open — 10
Customer-hold — 40

Count by ID

Total

30 + 99 → 129 → 38.3%

99 → 55.33%

Percent

(1) chart
(2) Timechart
(3) Event Count
(4) Where
(5) search
(6) Rex.
(7) Addtotal
(8) Addcoltotal

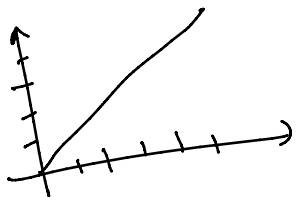
(1) Charts:-

chart Count by current_ticket_state.

Count → y-axis

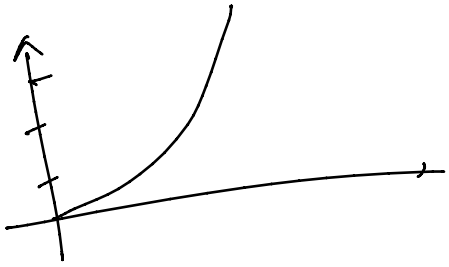
current_ticket_state. → X-Axis

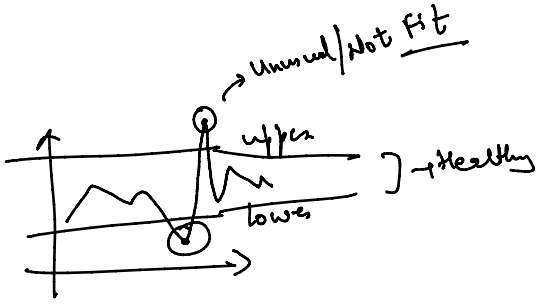
Linear

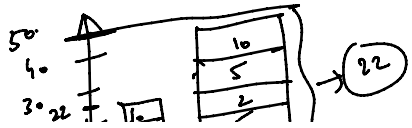


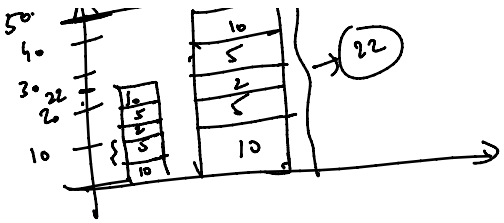
10, 20, 30, 40

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







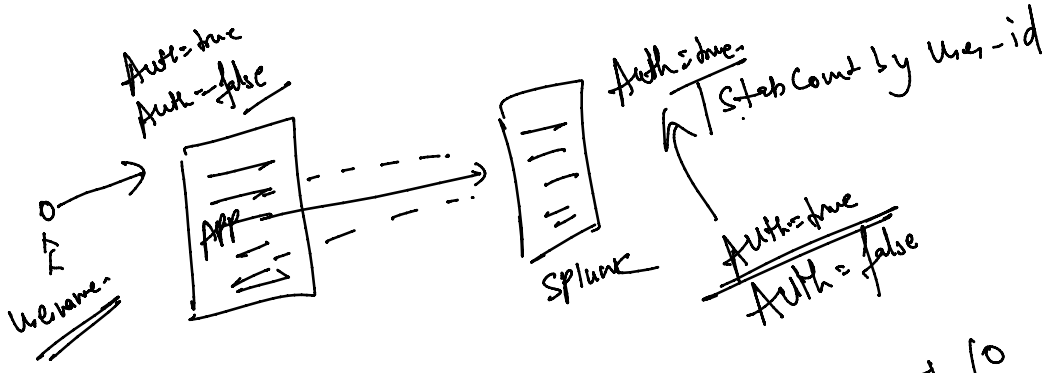


0 → 10
C → 5
ON → 2
I → 5
22

② Single Value Visualization:-

① Numeric, that style Numeric output.

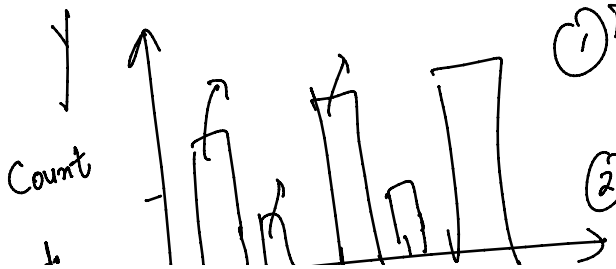
| stats count
↳ count
99



user1 → 10
user2 → 3

③ Timechart:-

|timechart count by Asset_id



① Default x-axis = _time
↳ In built time

② Span
↳ Time interval

Timechart count by time

↓

No where defining the time field in the command

Count

(2) Span

↳ Time interval

X

_time

↓

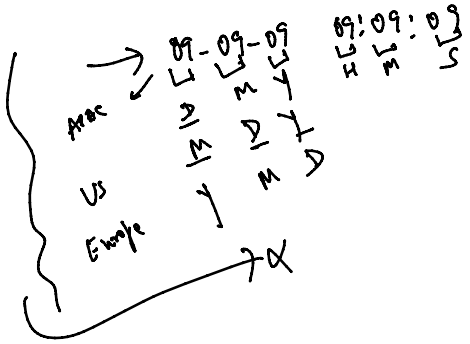
Pre defined | In-built field

↳ time field

time-submitted

Overwrite | Any other time field.

time-submitted



(4) Map:- Coordinate (Latitude, longitude)

(5) Sankey Diagram:-

Precheck:-

App → 1.5.5 / 1.6.0

(1) Memory of server

(2) Dependency | libraries need to run the App.

(3) Compatibility - Splunk Enterprise.

↳ 9.0.x

V. 8.0.2

(4) Compliance → Policy Organization → Author

Search:- filtering the field on the basis of certain value.

a
10
15
20
30
40
50
60

search a>40

a
50
60

Where:- Comparing the value of two different field.

a	Threshold
10	15
5	15
15	15
20	25
30	15
25	15

Where a > Threshold.

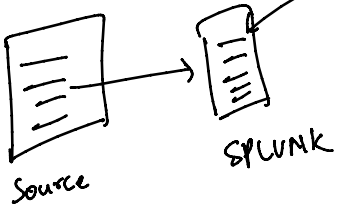
a	Threshold
20	15
30	15
25	15

a	b
5	6
10	12
15	18
20	24
35	21

a>b	
35	24

fields - b

Rex Command:- Regular expression.



Data Masking:- 1234-5678-9101-1123
xxxx-xxxx-xxxx-1123

Data Masking:-

1234-5678-xxxx-1234
xxxx-xxxx-xxxx-1234

Masking.

Data Masking → Replacement → "s|<regex>|<replacement>|<flags>"
Data Masking → Substitution → "y|<string1>|<string2>"

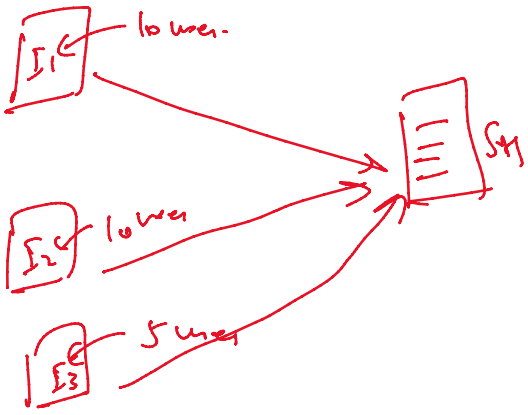
Assignment-3

① Address:- abc colony, Bangalore, 560001
xxx xxxxx, Bangalore, 56xxxx

Addcoltotals:- Addition of data column wise

Addtotals:- Addition of data row wise.

Evencount:-



Knowledge objects:-

1. Tag.
2. Eventtype.
7. Calculated field
6. Macros.
7. Lookup
8. Data Model & Pivot
9. Alerts.
11. Workflow Action.
12. Transaction.

(3) Calculated field

(4) Field Alias

(5) Field extraction.

(9) Alerts.

(10) Reports.

(1) Tags:- Categories the data.