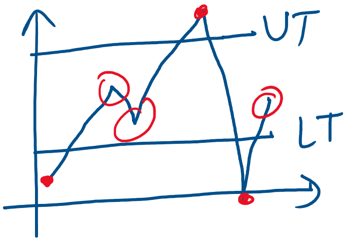
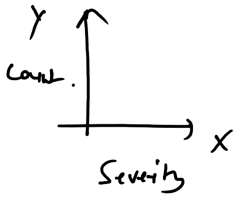
Day - 2

19 March 2025 18:38

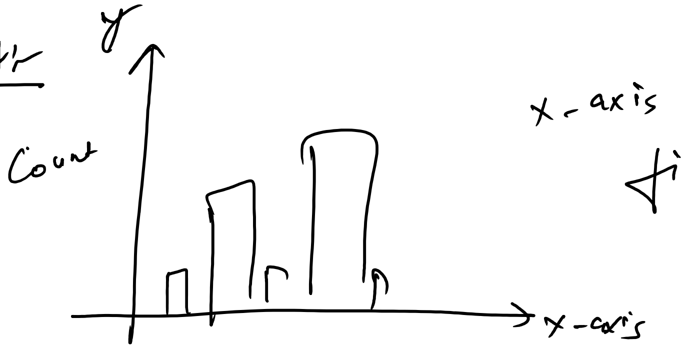
1. chart
2. Timechart.
3. geostats.
4. Single Value Visualization.
5. ~~re~~ rex
   ↳ Field Extraction.
6.



ab...cd



Timechart:-



x-axis is reserved for the _time (time) field.

_time.

Span-interval.

m = minute y = year
h = hour d = day
mon = month

Single Value Visualization:- Single Numeric output.

Geostats:- Geographical Maps.

Latitude → Coordinate
Longitude → ''

Latitude → "
Longitude → "

Rex:- Regular expression
↓
extract the field from the events.

Tail:- Pick the last Value from the column.
|tail 2 → Bottom 2 value from the list.

Head:- Pick the first Value from the column.
|head 2 → first 2 Values from the list.

Field Extraction:-
→ Rex → Regular Expression → Regular
→ Delimiter → Split the event on the basis of Certain Keyword / Symbols.

① Tags.
② eventtype.
③ Field Alias.
④ Alert
⑤ Report.
⑥ Lookup.

① Tag:- Categories your field value.

Severity = $\boxed{3}$ → Normal

Severity = 3 → Normal.

1-abhi

2 fields:-

① tag → Normal.

② tag::fieldname.. → tag::severity= Normal.

② Eventtype:- It helps to categories event on the basis of Certain Condition.

CTS = Resolved   CTS = closed

→ Completed.

→ eventtype.

Normal

tag.

severity = 3

field Name

field Value

Field Value pair

Search → search of the data · in a same field.

where → Compare the data b/w twofields.

A	B
5	15
10	20
15	5
2	1
7	35

Search A >10

Where A >B

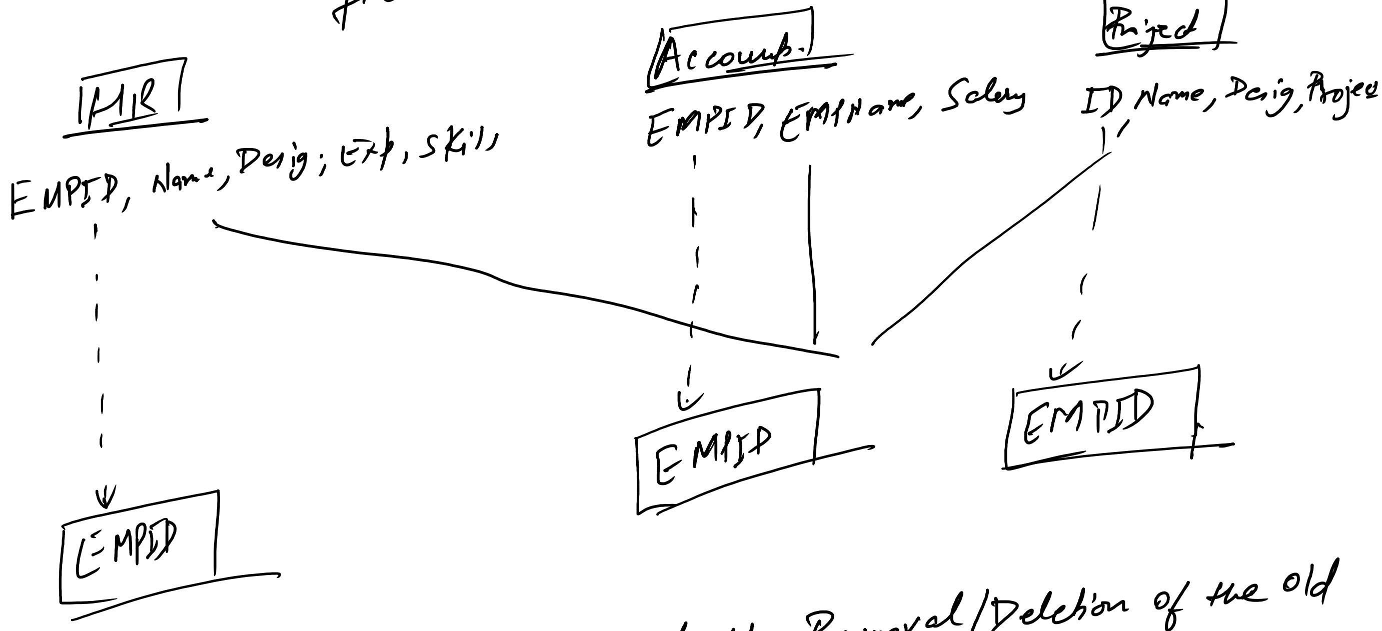
③ Field Alias:-

Field   Alias

↓

Pseudo Name.

field. Pseudo Name.



1. Create the Newfield. No Removal/Deletion of the old field.

Field Alias

Severity → Priority

Severity = 3 → Normal

Field/Value pair → tag.

New field Aswell as Old field too.

Severity → Priority ☑

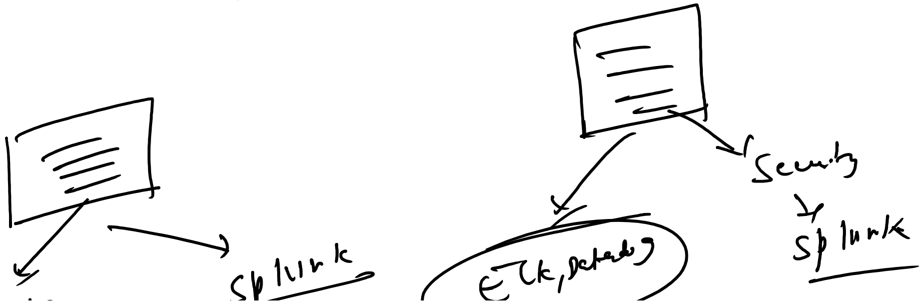
Severity → Priority

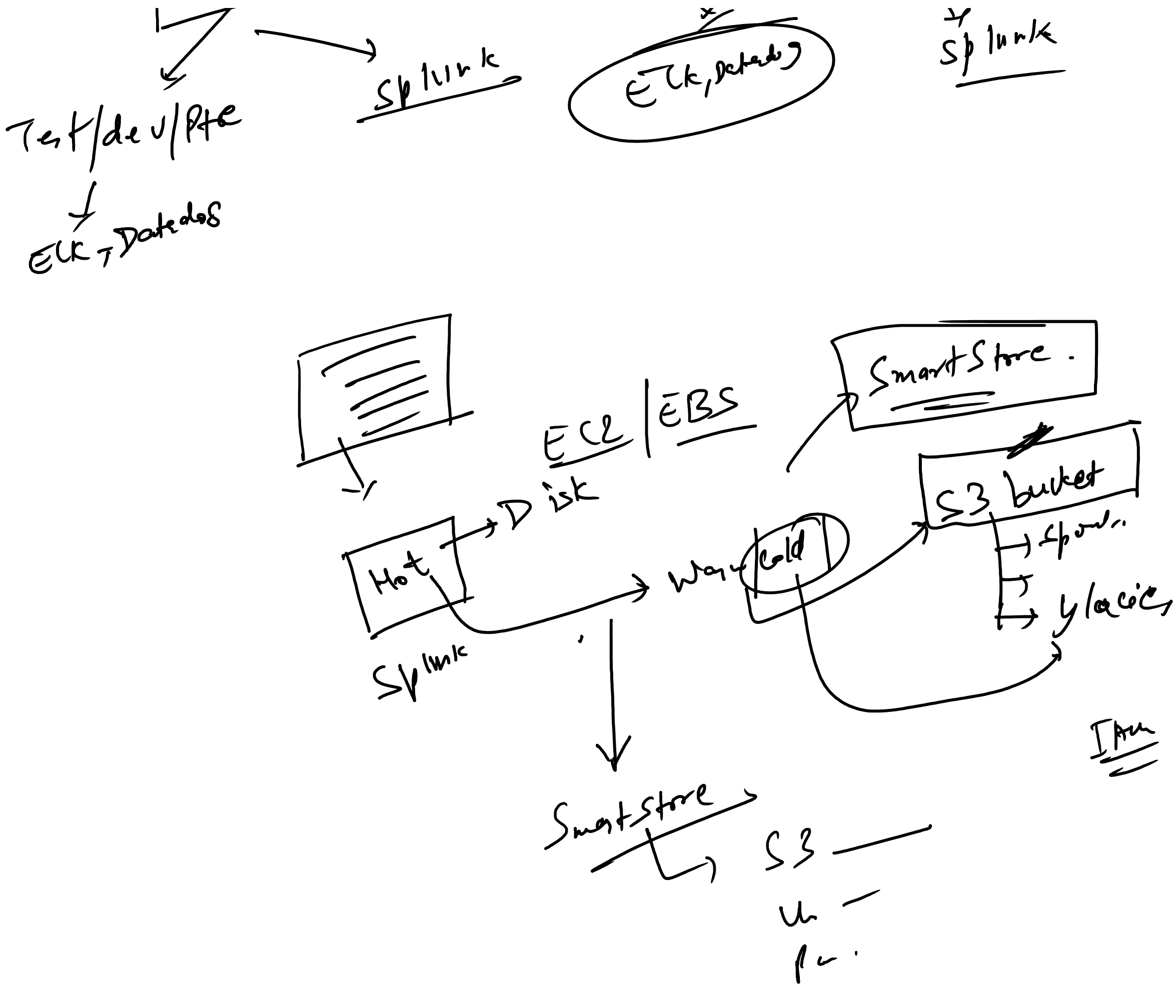
Host → host :: —

Source → source :: —

→ Sourcetype → csv

↳ sample_tickets.csv





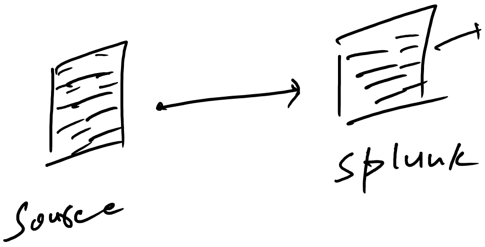
③ Alert:- Condition is met, trigger Action.

[Definition] → internal. → SPL → Schedule.

[Trigger Condition] → When? Alert to trigger.

[Trigger Action] → What? When the Alert will trigger

Email | Webhook
mobile | Alert Action.



Alert that will trigger if no logs is being recieved.

every 15 min.

1. Activity.

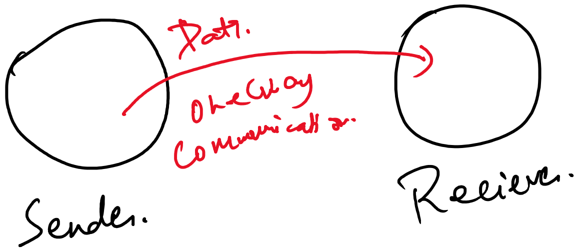
source   every

&

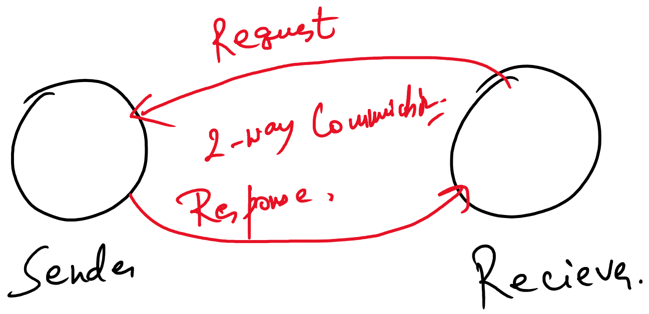
upgrade Activity.

No logs will be their in Splunk.

Webhook



API



Reports

[Definition] → SPL
→ Schedule
→ interval.

[Trigger Action] → Email, script, etc.