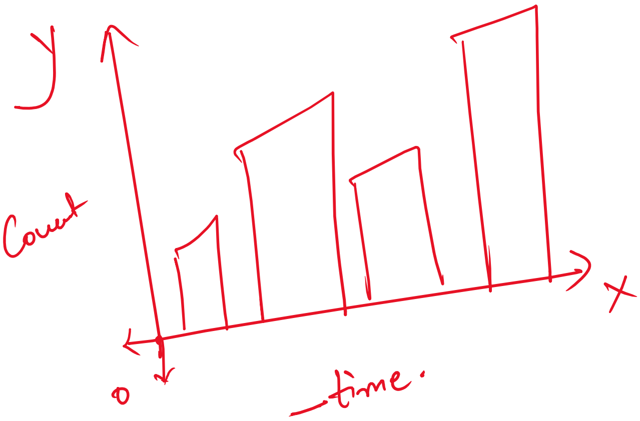
Day - 2

21 January 2026 19:38

Timechart:-

|timechart count by severity.



GeoMap:-

Geographical Map.

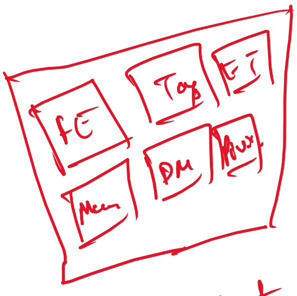
Coordinate - longitude, Latitude
e

Single Value Visualization:-

Single value.

| stats count.

Knowledge object:-



Basket.

Tag:- Categories the value of the field.

→ Normal.

Tag :- Categories the .

2 New fields :- Severity=3 → Normal.

① tag :- normal.

② tag::severity =normal

Eventype :- Categories the event on the basis of certain criteria.

Field Extraction :-

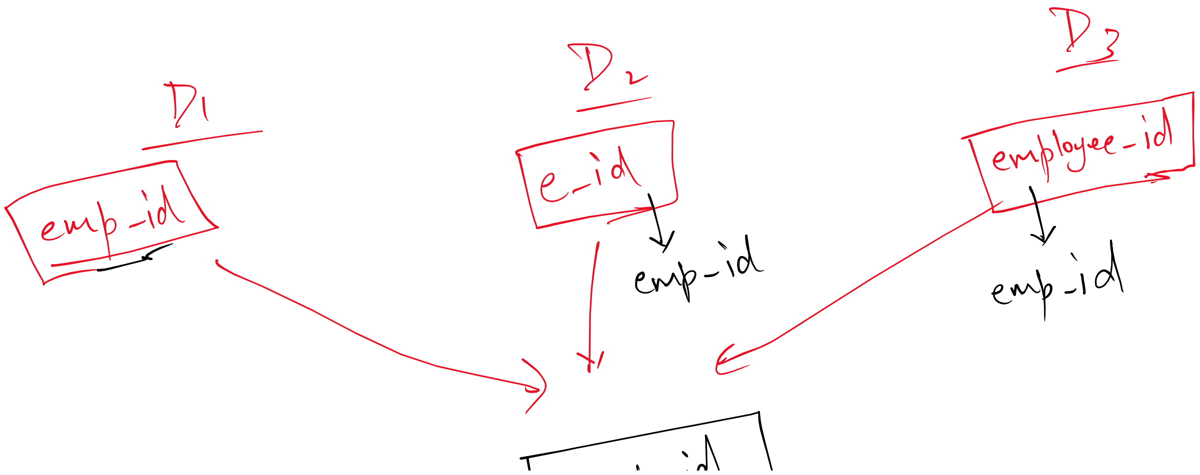
→ Regex :- pattern of the field.

→ Delimiter :- split the event on the basis of symbol & form the field.

Field Alias :-

Field →

Alias :- Other Name.



emp_id

① New field, but it will not delete the old field.

Calulated Field:-

eval VK_Kb = bytes / 1024

Variable

Calulated field:- template → calculation → formula.

Macros:-

Function.

```
function a (b, c)
        {
        d=b+c;
        return d;
        }
```

→ function a(5,4)

a(7,8)

Arg.

return;
}

Macros
- No Arg.
- Single Arg.
- Multi Arg.

Lookup:-

① CSV
② Kvstore.
③ Geospatial.
④ External.
⑤ Database

① CSV:-

① extension- .csv.
② Small & static files.
③ upload in splunk, we are not indexing it.

① upload.
② Lookup Definition.
③ Automatic Lookup.
④ OutputLookup
⑤ Lookup editor Application

④ outputlookup:-

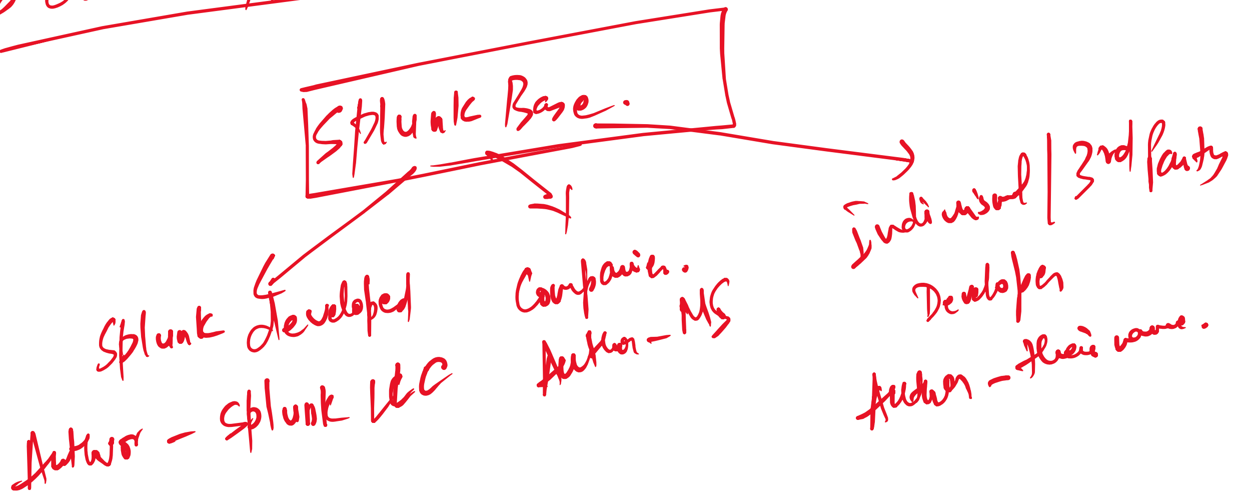
|outputlookup lookup.csv append=t|f

f → Overwrite the value.

t → Add that row

Add that row

⑤ Lookup Editor Application:-



Report & Alert:-

↓

[Definition]

[Action]

Alert

[Definition]

[Condition]

[Action]

Tomorrow:-

Tomorrow:-

(1) Data Model & Pivot

(2) Dashboard.