Data Model:

Why?

1. Data is huge.
2. Searching is delayed.
3. Indexer occupied for longer period of time.

How?

1. Hierarchical concept
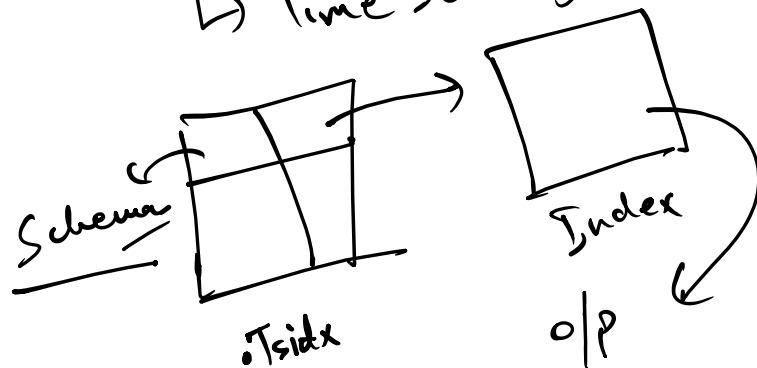   Root
     ↳ child+C'
        ↳ Subchild+C"

2. Tsidx file
     ↳ Time Summary Index.

Schema ← [.Tsidx] → [Index]

.Tsidx   o/p

3. Defining the fields in advance itself.

Cons:-

1. It will consume lot of Computational resources.

Pivot → Creating the visualization.
              1 chart count —) datamodel

givot

index = _____ | chart count _____

datamodel
↓
Pivot → click to go
  ↳ Only when dm
    is their.

Dashboard :- → classic Dashboard → XML
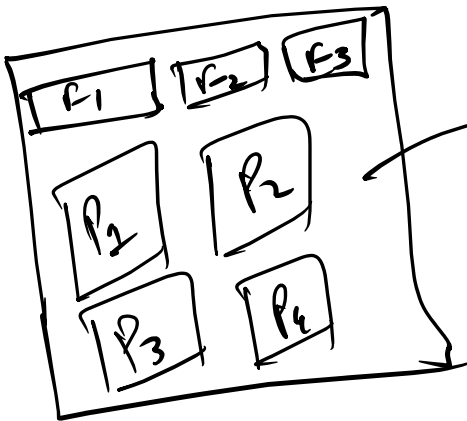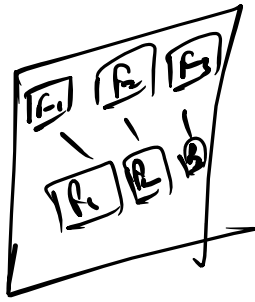   → Feature driven.
                                  → 1st version of splunk
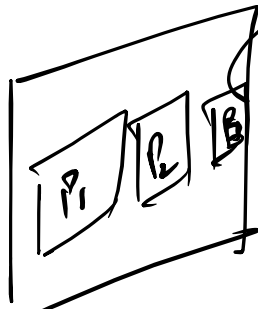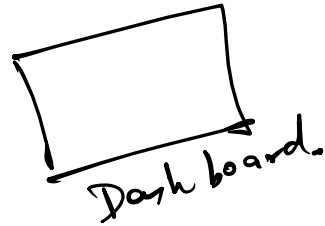
              → Studio Dashboard → json
                                 → Cosmetic Part
                                 → V 8-2·X+

Dynamic Dashboard :-

Drilldown :-

Dashboard.

X-axis

```
        Name
      ⤴
click.name = severity
click. Value = 1, 2, 3, 4
          ↳ Value.
```


y.

Count.

Severity

```
click.name2 = Count.
click. Value2 = 5, 10, 7, 4
```

y-axis.