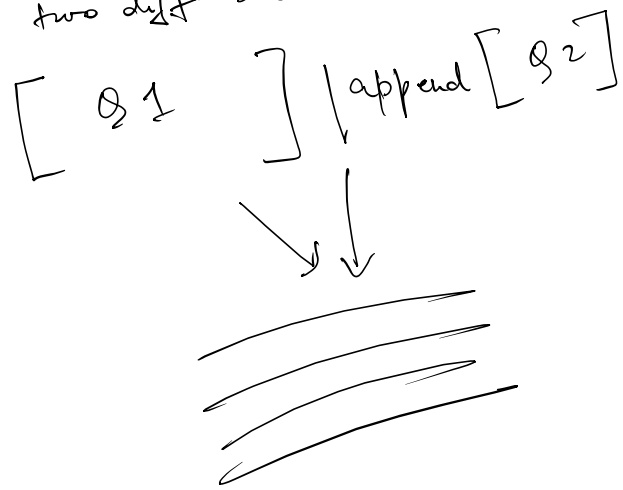
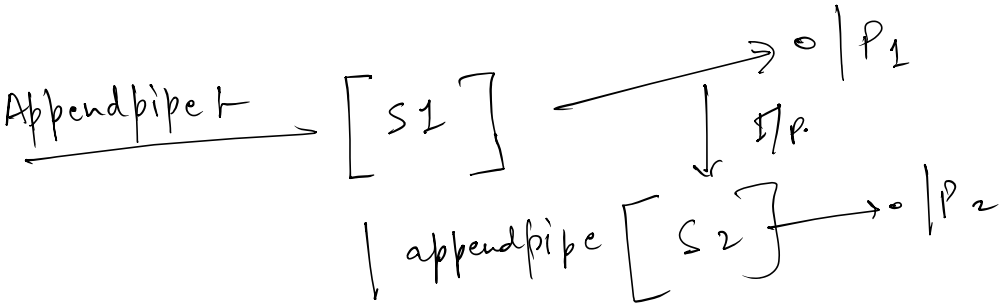
Day - 2

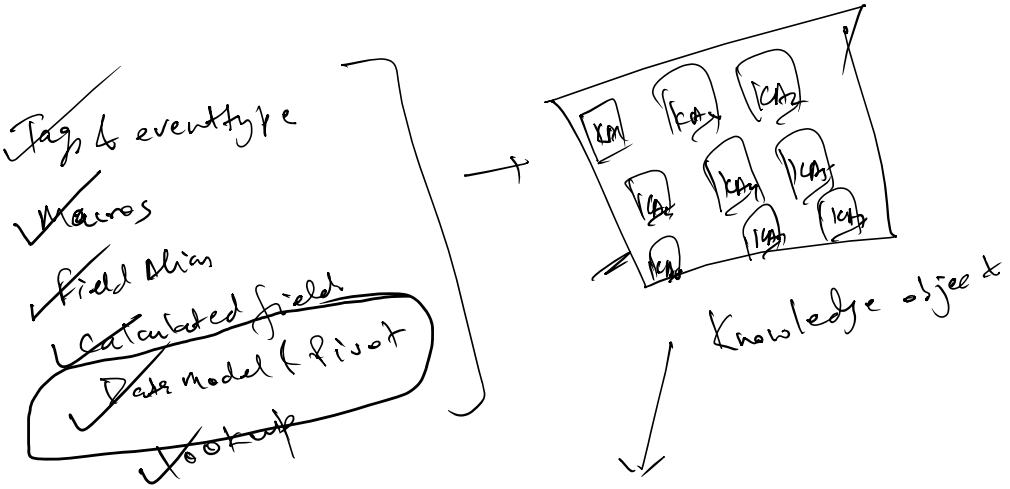
18 September 2025 19:40

① Append.

Combine two diff dataset.

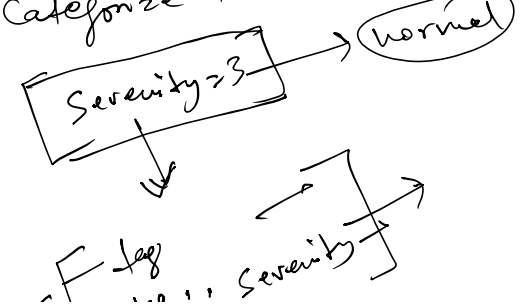






① Tags & eventtype

① Categorize the data using tag.



2 Additional fields is generated overthere [tag, tag :: severity]

② Eventtype :- Categories the event

Tag → Mapped/Categories on the basis of (fieldvalue)

& eventtype → Mapped & Categories the events on the basis of (Condition) → SPL

③ Macros :-

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

A(3,4)
A(5,6)

template
pass the Argument

Macro :-

① No Arg :-
② Single Arg :-
③ Multi Arg :-

Single Arg :- Where we will pass one Arg.

Multi Arg :- Pass more than 1 argument.

Field Alias :-

Field → Field

Nick Name / Pet Name.

Why ?

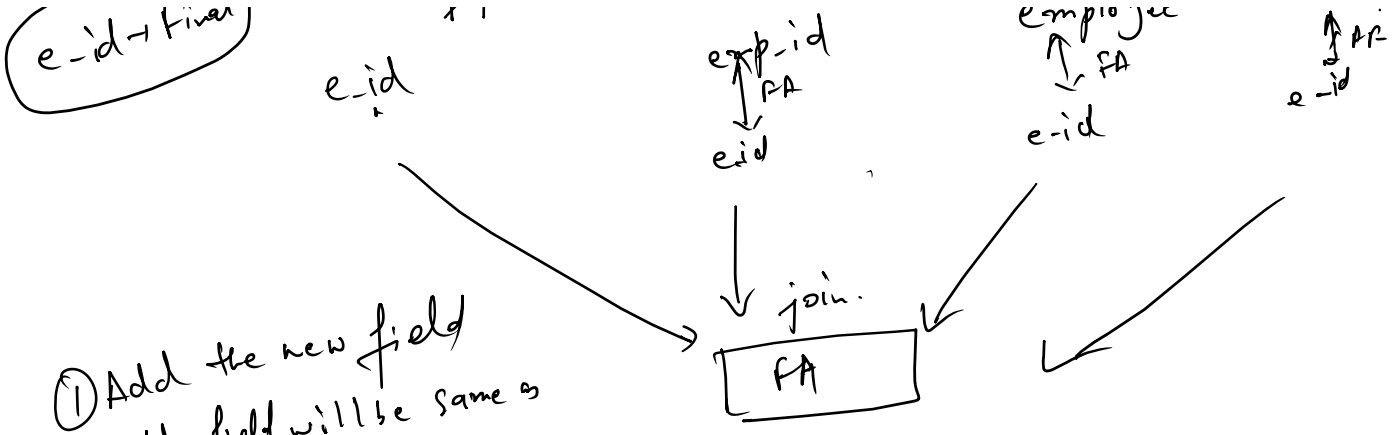
e-id → Final

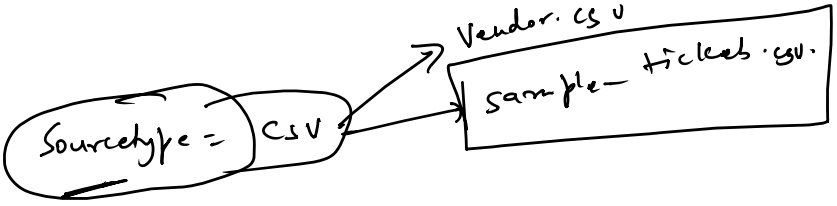
D1
e_id

D2
emp_id
FA

D3
employee
FA

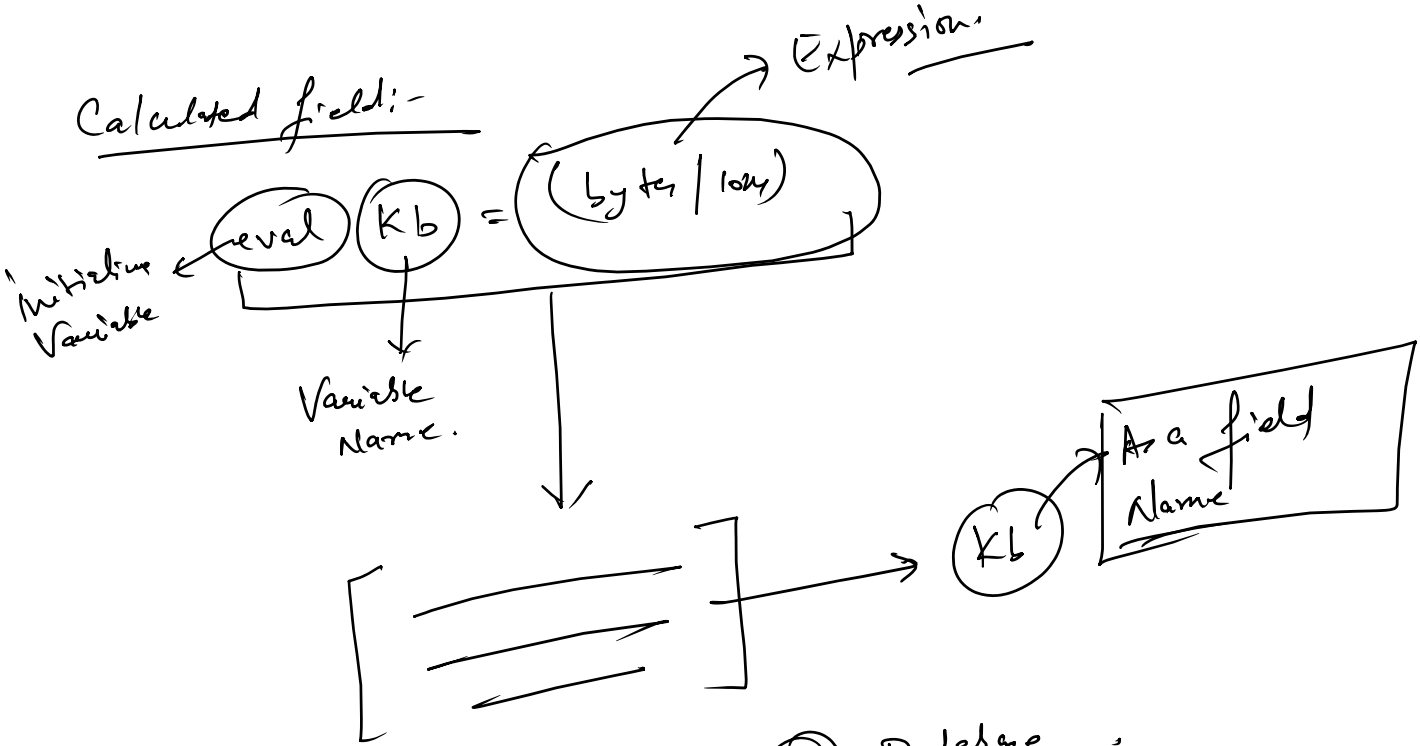
D4
id
FA
e_id





Source!! ——
host!! ——
——— Sample tickets.csv

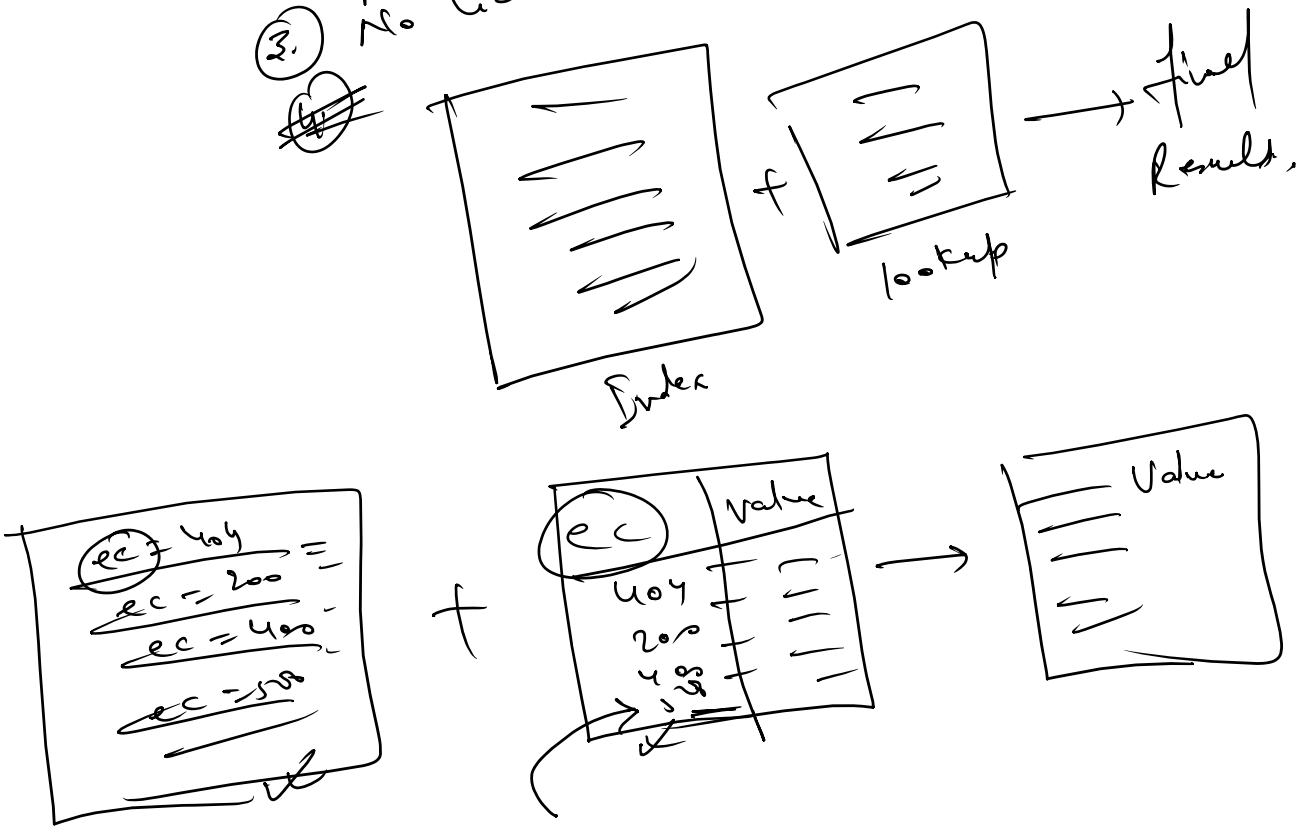
Calculated field:-



LookUp:-

Lookup:- (1) CSV → CSV lookup.
(2) Kvstore.
(3) geospatial.
(4) external.

CSV lookup:-
(1.) Small, static file.
(2) upload on the splunk
(3.) No License, No Index, Normal upload.
(4)



Field Name = Case Sensitive
Field Value = Case Insensitive

Lookup Definition- Define the schema/structure of lookup file → column

It will make the things little faster.

1. Pull the event. → Quick
2. Define the structure. → Advance

Automatic lookup:-

|lookup VK_lookup_definition ticket no. Output time_taken as time_consumed

↓

Don't want to repeat the same step Multiple time

↓

→ time-consumed or a usual field in splunk.

Data Model :-

(2) optimize the search Query ← Benefit

↓

(1) Inheritance,

Root
- child + C'
  - child + C''
    - SSC + C'''

index = main
- → Search the event
- → Extract the field.

1. CTS
2. TH
3. serving
4. Asset id
5. App_name

(2) Define the fields in Advance itself

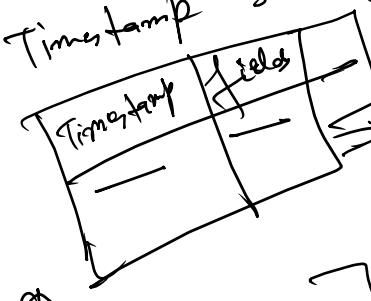
5 fields → Advance

(3) Tsidx file

summary file.

(5) ''

(3.) Tsidx file
↳ Timestamp summary file.



Impact:-
(1) Consume more computational resource
↳ CPU, Disk, memory

condition ← [(1) Data is huge
(2) Critical & immediate output] → DataModel

Pivot → Graphical representation of data from datamodel

chart | timechart → index → [graph]

Pivot → datamodel → [graph]
↳ click to go

Cryptographic function: It will encrypt your data.

(1) md5
(2) SHA256
(3) sha512
(4) SHA1

Date & time fun":-
(1) strptime
(2) strftime.
.. date & time field into the

② strft...

① strptime — Convert the date & time field ... epoc format.
↳ system readable format.

D1 D2
Diff = (D2 - D1) ×
(D2-epoc - D1-epoc) ✓

② strftime
↳ format the date & time.

D1 ⟶ format str.
%d-%m-%y ⟶ %y-%m-%d

D1 ⟶ D1-epoc ⟶ D1-format