Day - 3

23 July 2025 10:09

Knowledge objects:-

1. Tags & eventtype.
2. Fielded Alias.
3. Lookup - csv.
4. Field extraction.
5. Report & Alert.
6. Workflow.
7. DataModel & Pivot.

---

1. Tags & eventtypes:-

Tag:- Categories the data on the basis field value.

2 new fields willbe generated.

2 new tags

[tag :: current_digital_state = "closed"
tag = normal.]

Eventtype:- specific event.

| eventtype —

2. Field Alias:-

→ Nick/New/Pet/Alternate Name.

→ field name.

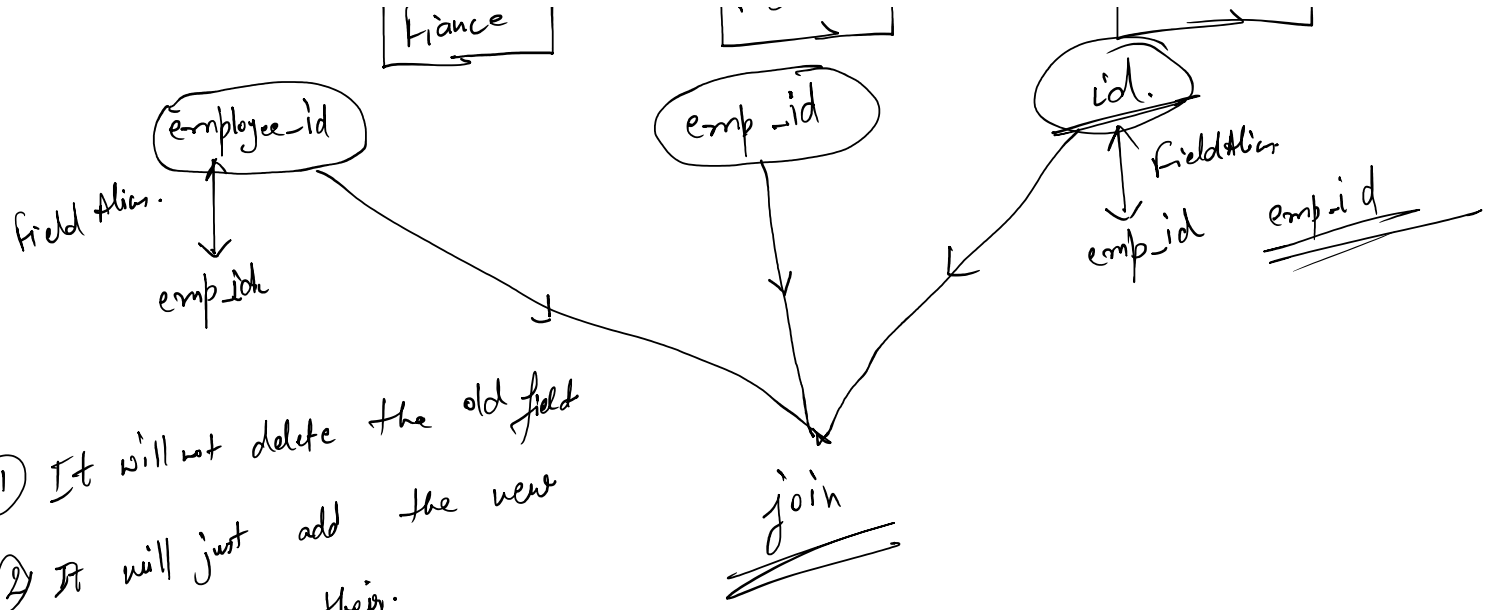
completetils

Finance

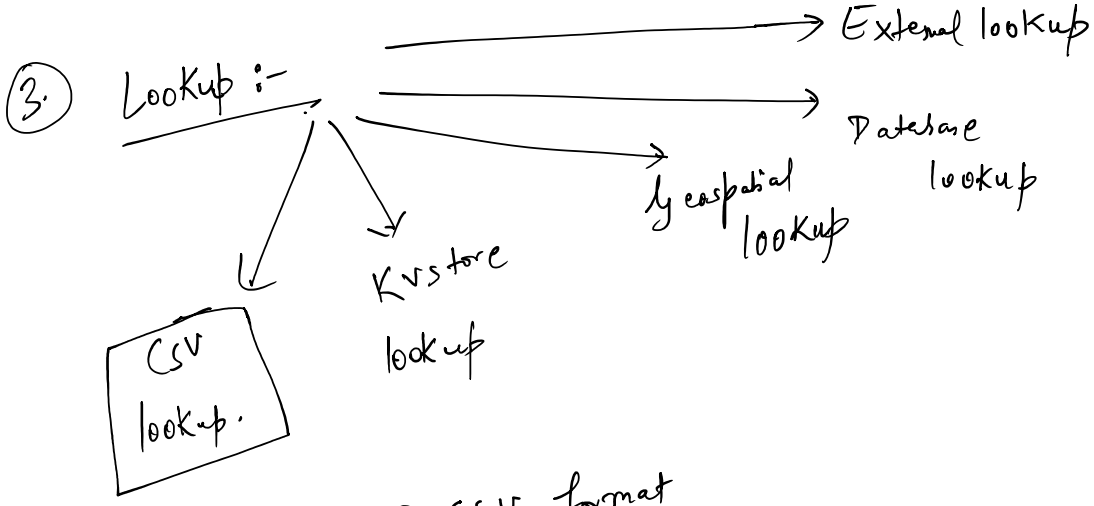
Project

HR

id.



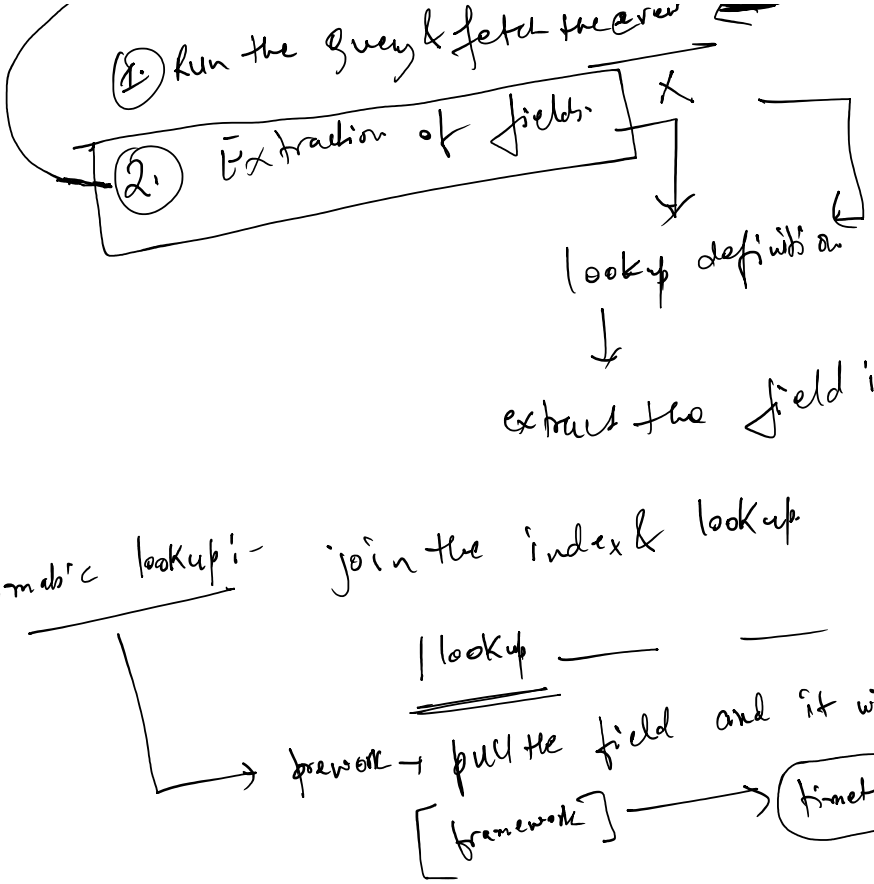
(1) It will not delete the old field
(2) It will just add the new field over there.



csv lookup:- (1) csv format
(2) upload the lookup file in splunk, we are not going to index the lookup file. As we are not going to index, No licence is consumed.
(3.) Small & static file.

Lookup definition- | inputlook VK_lookup.csv

(1.) ticket_number, time_taken.
(2.) Run the query & fetch the event



Automatic lookup:- join the index & lookup

lookup

framework → pull the field and it will be used as normal fields

[framework] → time taken.

Lookup editor Appl:-

4. Field extraction:-

Rex → extract the field from raw data.

Field extraction → Data is Consistent.

Delimiter.

Regular expression.

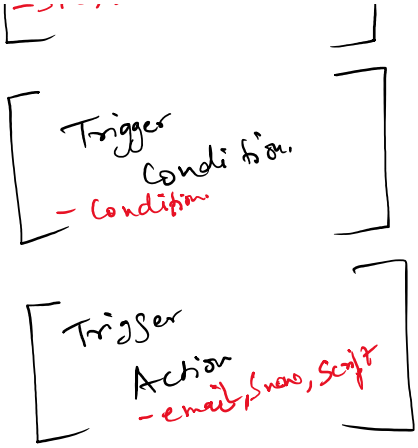
5. Report & Alerts:-

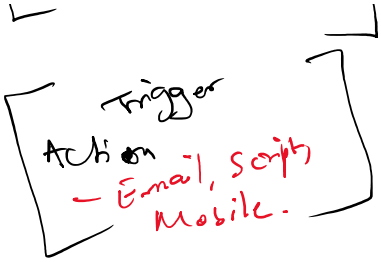
Alert

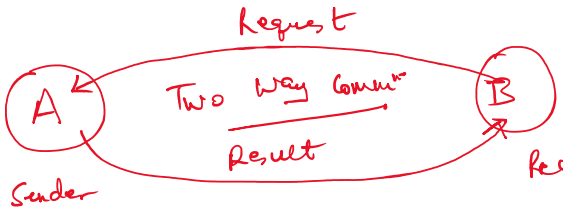
Definition
- SPL, Schedule, Intervals.

Report

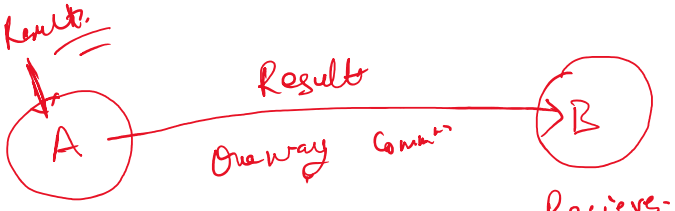
Definition
- SPL, Schedule, Intervals







API Calls



Web hook