Day - 3

10 July 2024 09:57

1. Lookup
   1. lookup Definition.
   2. Automatic lookup
   3. inputlookup, outputlookup.
   4. lookup editor Application.
2. Data Model & Pivot.
3. Transaction.
4. Alerts & Report.
5. Dashboard → classic Dashboard → Static Dashboard
   → Dynamic Dashboard
   → Optimization → Basesearch
   → Searchsearch
   → summary idx.
   → Event Handler.
6. Studio Dashboard.

1. lookup:- CSV → Syntax.
   Kvstore
   Geospatial → Geographical location
   Database lookup → MySQL, Mongodb, NOSQL
   External lookup. DBConnect → Certain → lookupfile. / DB lookup
   dblookup

i. CSV lookup:- - Static file, small in size,
upload in the splunk, No Index.
↓
No license consumption.

Mapping purpose.

Log + 500, 200, 505

ec	ev
500	→
200	→
505	→

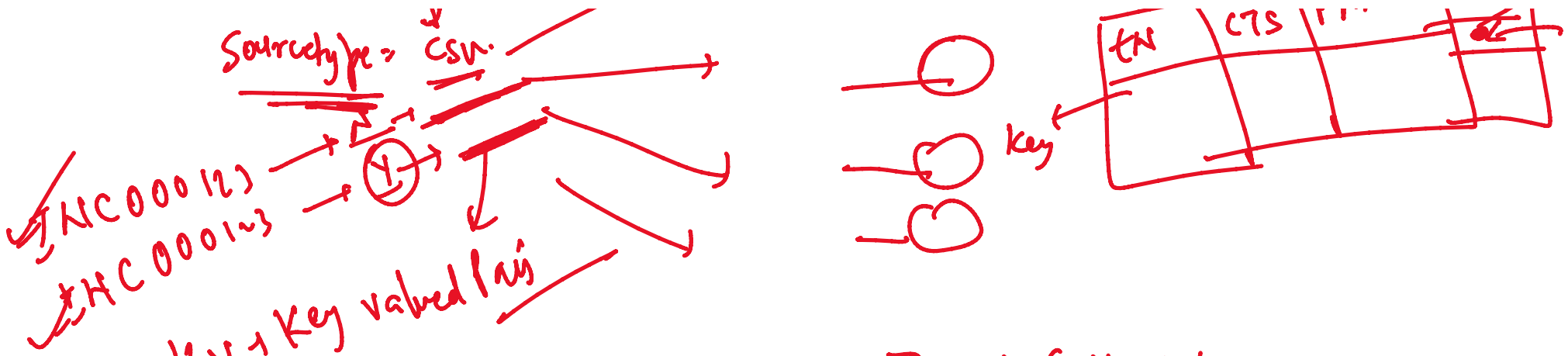
Automatic lookup

T_C

Sourcetype = csv. → sample-bikeds-csv

Key value ← Kvstore.

tN	C7S	PM	com.



Severity

1 → Critical → Critical
2 → High → High
3 → Normal → Low
4 → Low → Info.

Assignment → 1

1. lookup file → 1 → Critical
2 → High
3 → Normal
4 → Low

2. Map the lookup index data

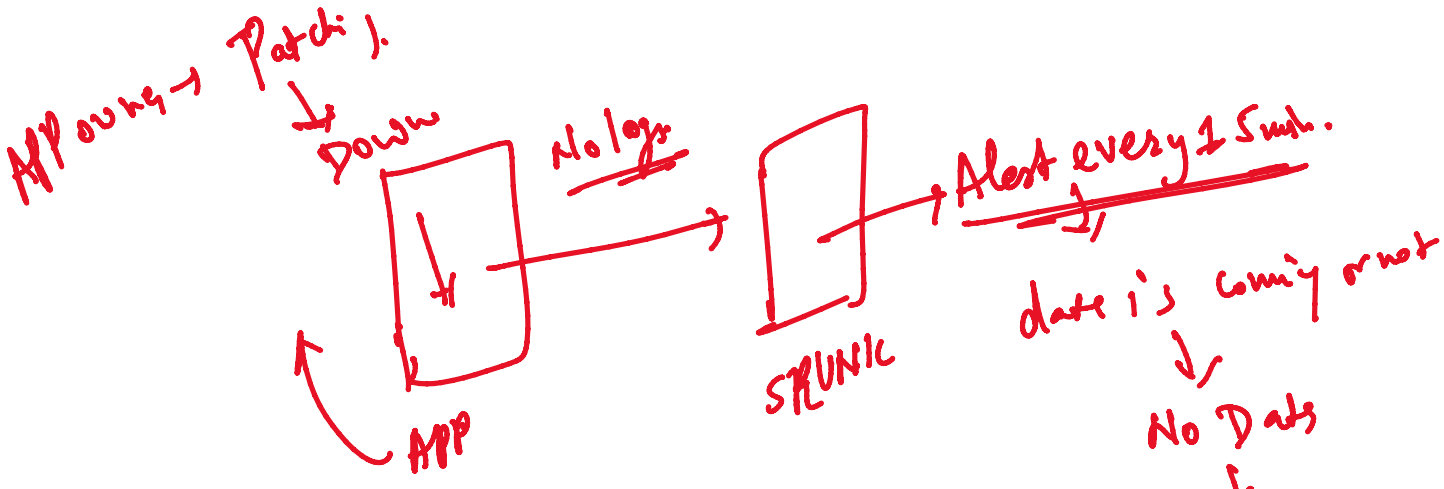
(3.) Pull the data using Automatic lookup.

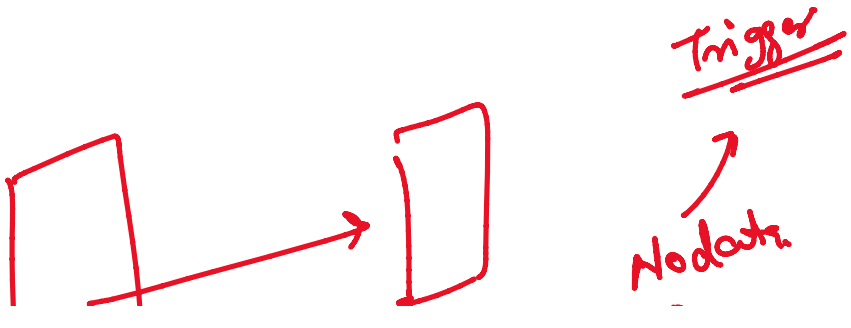
(2) Alert & Report:-

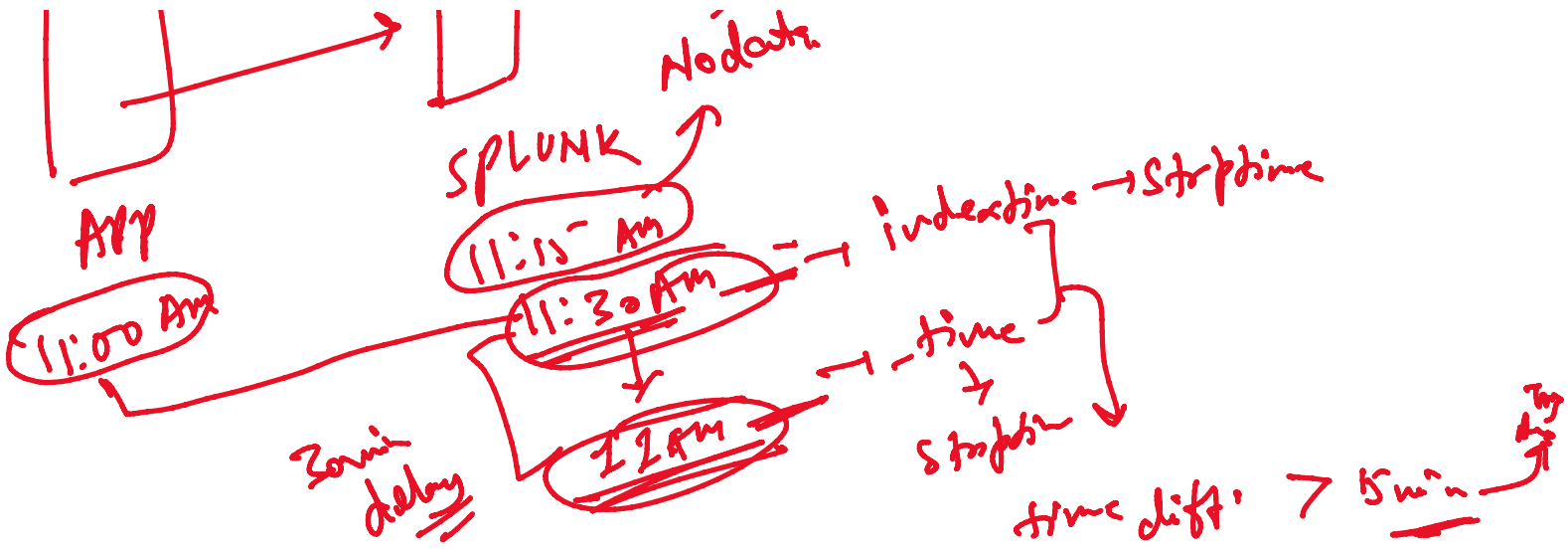
Alert:-

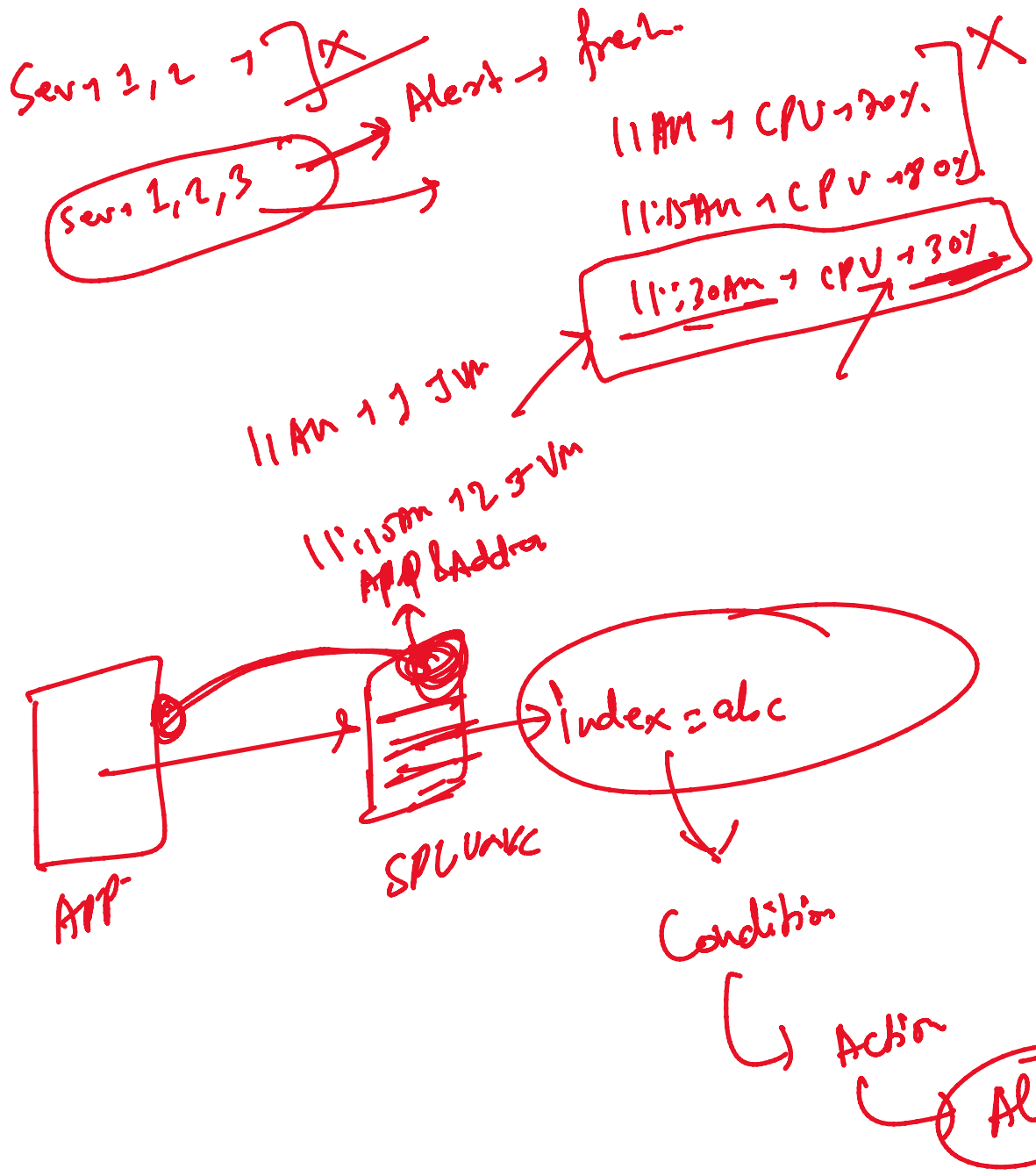
Search.
① Definition. → Sev = 1
② Trigger Condition. → Any data/event having sev = 1
③ Trigger Action → Email, Notification, webhook

→ 3 section for Alert.



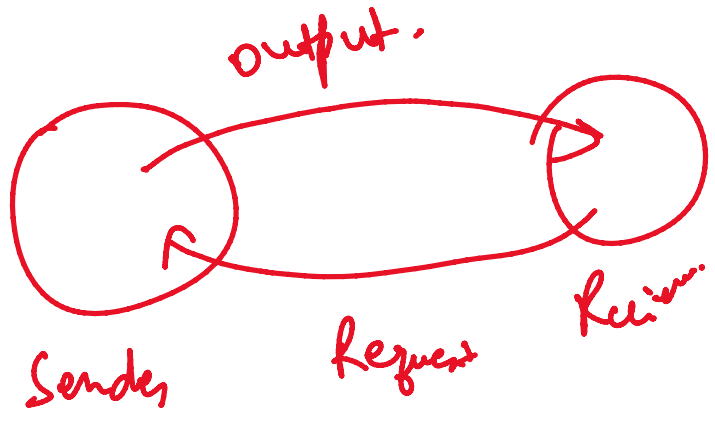






Calls:- ① API
② Webhook

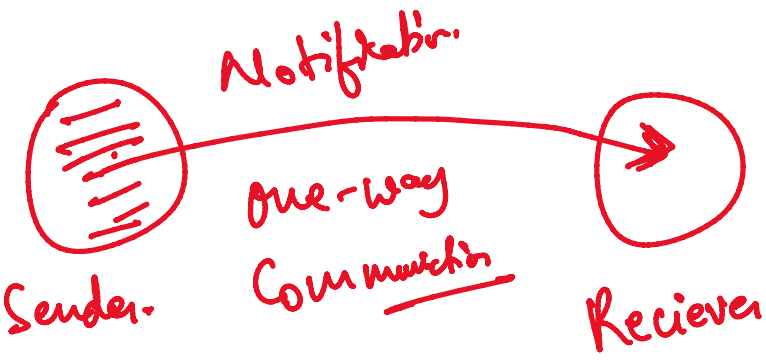
① API →

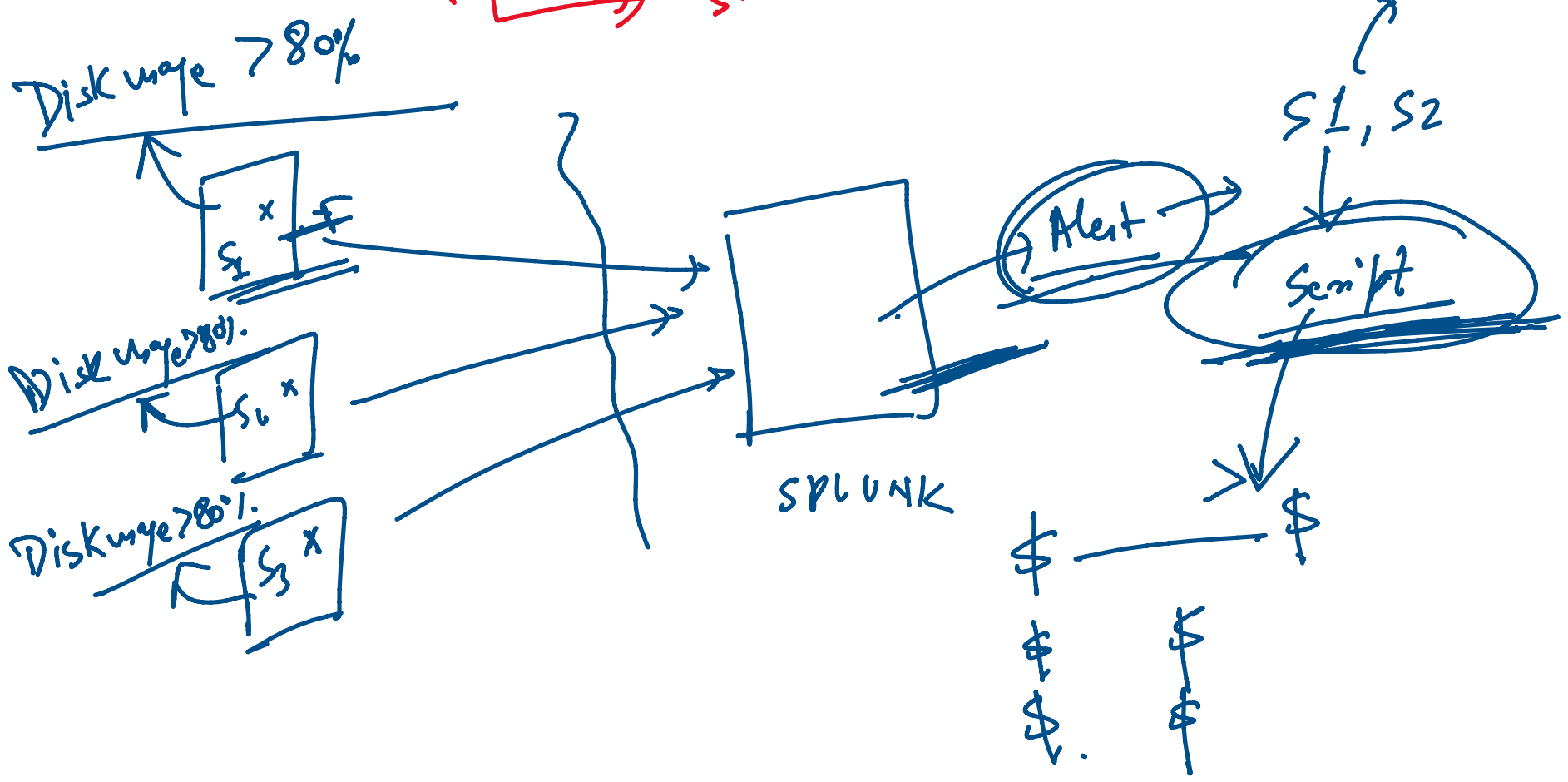


② Webhook:-

(2) Webhook:-

Payment
↓
2-4 hrs.



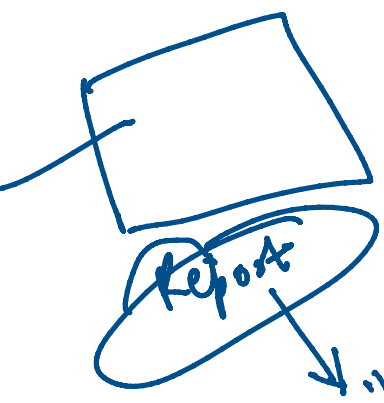


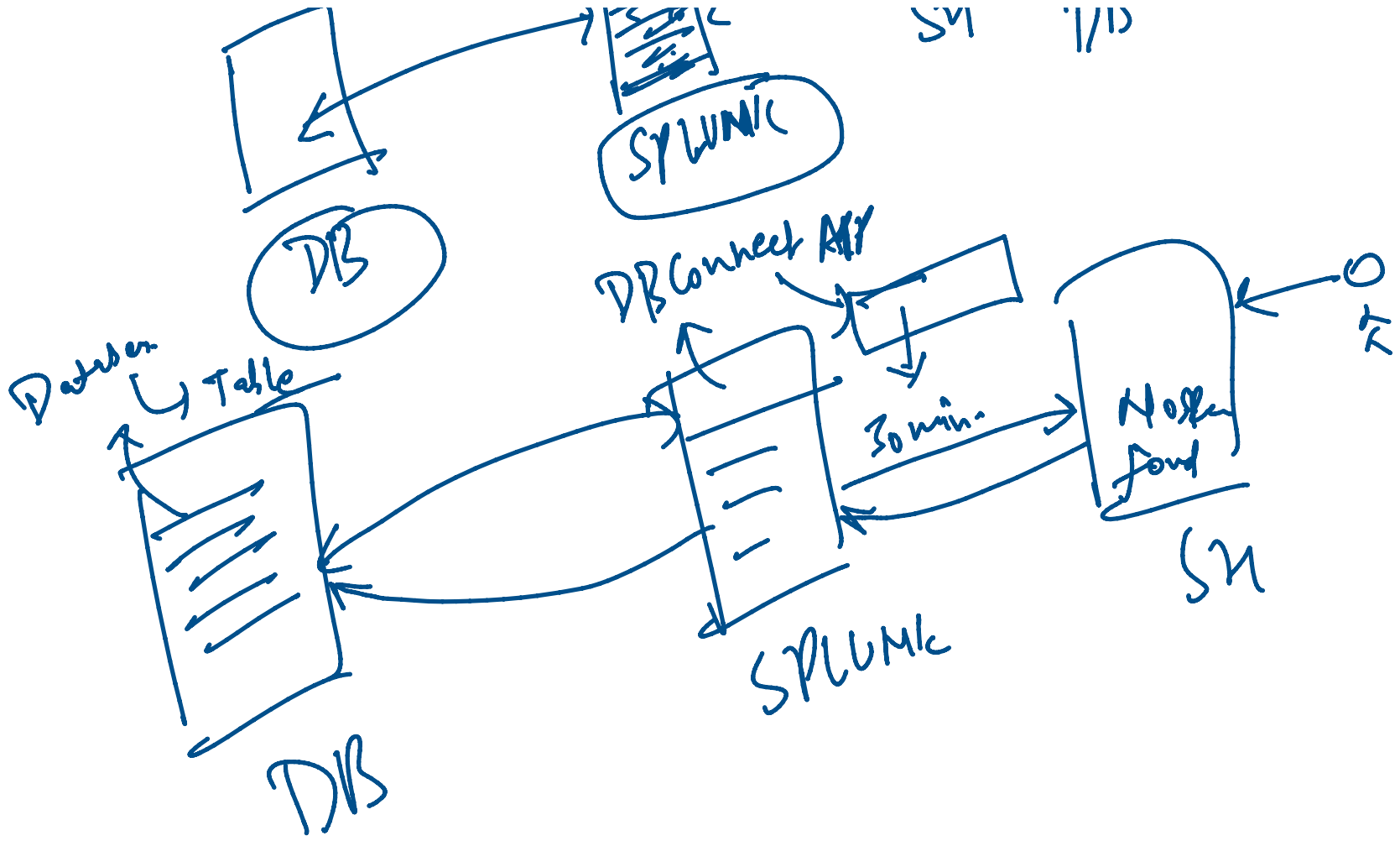
(2) Reports-

Report → o/p → Specific interval
↳ Nothing with Trigger Conditions.

(1) Schedule → every day. (8AM) → Today Transaction
(2) Tomorrow → (8AM) → Tomorrow Transaction.

Transaction id = ?.?





* Data Model & Pivot:-

Data Model:- Huge Dataset & its taking lots of time. At the time we use DM.

① Hierchical Concept.

Root event
↓
child event + C'
↓
SC + C''
↓
SSC + C'''

② Run the search Query.
→ ① Extraction of Data/ field. (Prior (save the time during execution)
→ ② Pulling the events.

② tH
⑤ severity
ⓒ CTS

ⓓ app_name
ⓔ asset_id

Data Model → Define the fields in advance only.

index = vt_idx sourcetype = csv.

20 fields

event

DM:-

① Huge amount of data

field extracted

DataModel → field is defined in advance.

5 fields

Pulling of events.

① Huge amount of data
② execution/search is critical

Security dataset → immediate searching Needed
↓
size huge

Pivot:- Visualization purpose.

index → chart, timechart

DataModel → Pivot → ① DataModel
② Click to go option.

* Transaction:- Command → Categories the event on the basis of Certain Conditi

→ Transaction:

OOZ

Benefits of Banking EFSC Amb

Time window on Form which Acc.

100 | Transaction ID = 002 | A1 → A2

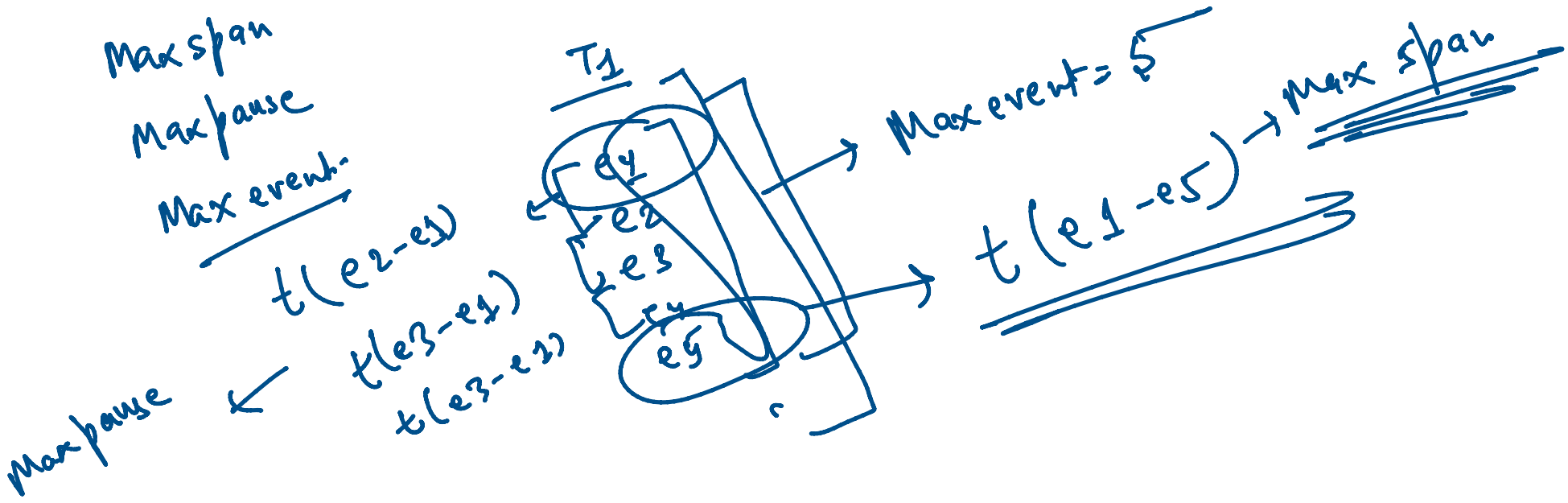
E commerce:- SessionID → Product view, Product Add, Product Remove, Purchase, Left the Cart → UserName, IP Address.

Activity → Captured as logs → Milli- → Millisecon

log Name ← millions of logs.

Max span T1 5 span

Maxspan
Maxpause
Maxevent.



11th July

① Dashboard (classic Dashboard)

② Studio Dashboard.