Day - 3

21 August 2024 09:34

1. Lookup → csv, Kvstore.
2. Data Model & Pivot.
3. Tags & Eventtype.
4. Alert
5. Report.

1. **Lookup:-**
   1. Upload in your server/splunk.
   2. No Indexing → No Licencing Consumption.
   3. Small dataset & static in nature.

   a) csv
   b) Kvstore
   c) Geospatial.
   d) External.
   e) Database lookup

a) **csv:-** csv file format in splunk
Small dataset
Static in nature.

1. Lookup table
2. Lookup definition
3. Automatic Lookup.

Automatic Lookup:-

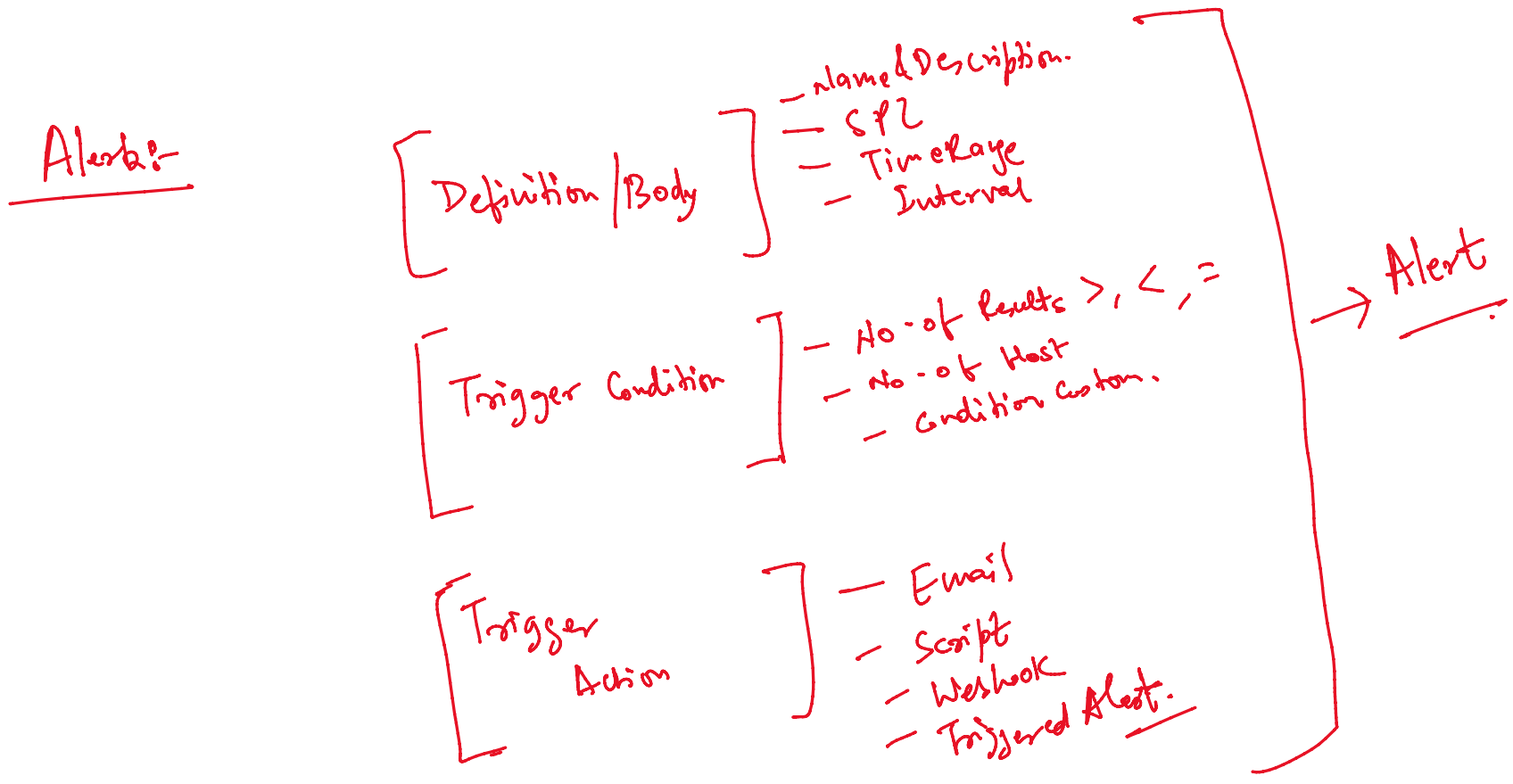
KVstore lookup:- → Key Value Pair.

1. Dynamic in nature.
2. Big in size as compared to csv.
3. Value → attached → Key (KV pair)

1. collections.conf
2. Lookup definition

3. Exploration.

Alerts:-



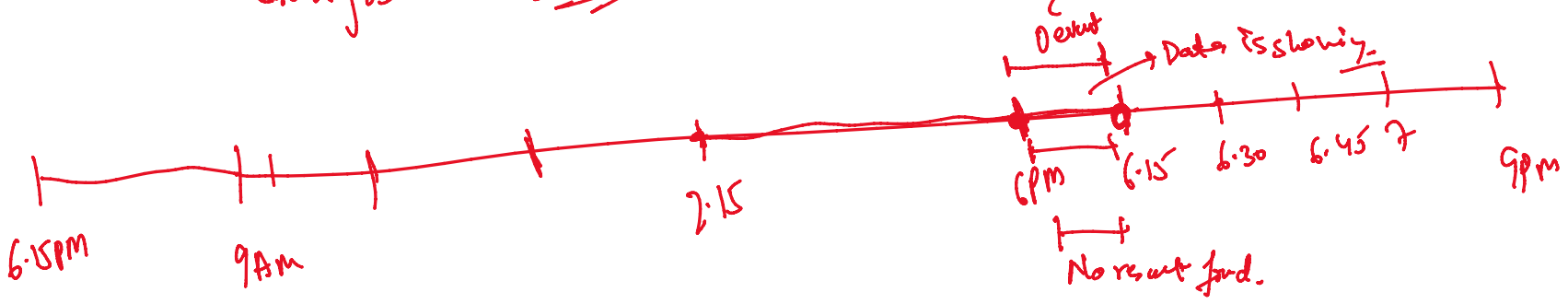
① No. of events.

Alert → Data is coming in the splunk or not.

Time Range → last 24hrs → 15min

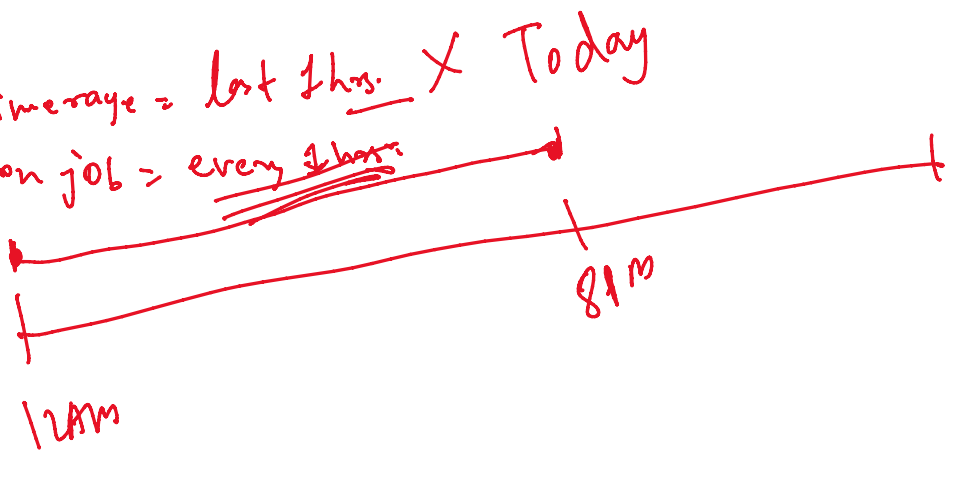
Cron job - 15min.

Result = 0

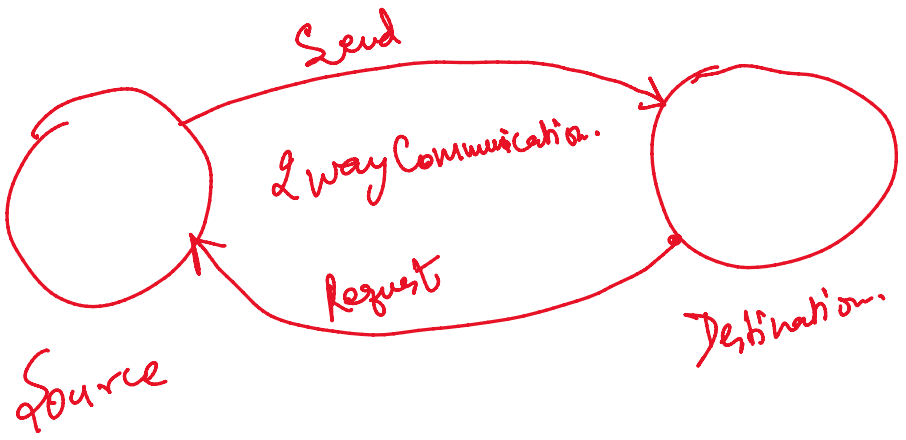


② License :-

Today day



API :-



Webhook :-

Report:-

[Definition] → Name.
Name
SPL
Time

Alert & Report
↓ Trigger condition.
↘ No Trigger Condition.

[Action] → Email
Mechanism
SMS

Tags & Eventtypes

Tags → Categorize the data.

Eventtypes → Works on the event categorization.-

CTS = Closed
CTS = Resolved

Data Model:-

increase the searching speed.

↓

1. Define the field in Advance.

2. Hierarchical Concept:

Root event.

↳ child.event (R+C')

↳ Sub-child (C+C'')

1. Searching of Data.
2. Extraction of the Data.

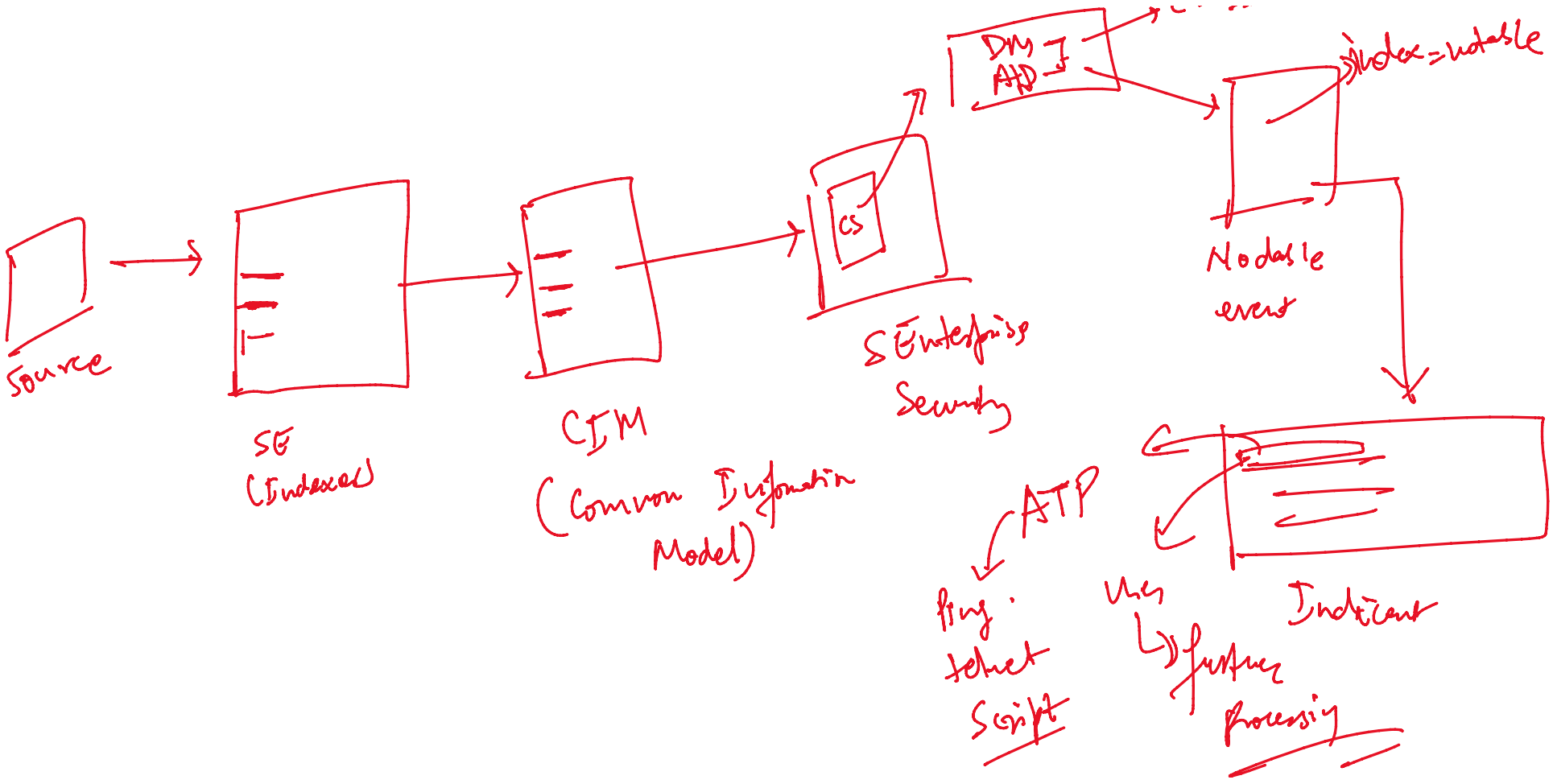
→ 2 steps.

(1) Ticket Number.
(2) Severity
(3) Asset_id
(4) Current Ticket state.
(5) Time Submitted.

↳ we will be picking only these fields

DM → C.S.ID
AND

→ Index = notable


Source
SE
(Indexed)
CIM
(Common Information
Model)
CS
SE Enterprise
Security
DM
AM
Index=notable
Notable
event
Indicant
ATP
ping
telnet
Script
User
further
processing