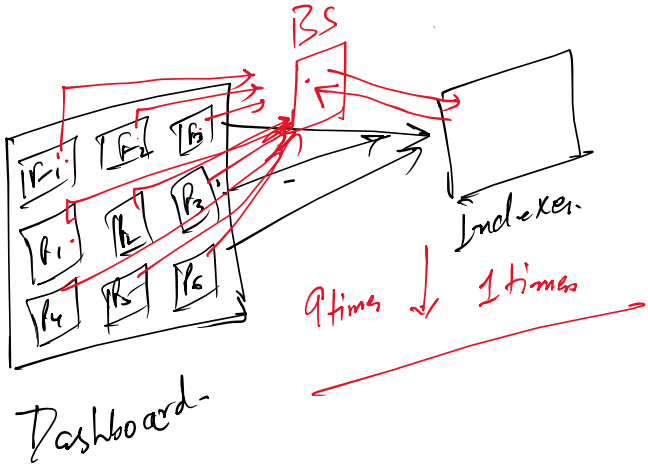
Day - 3

21 January 2026 09:39

1. Optimization of Dashboard.
2. Tags & Eventtype
3. LookUps.
4. Macros.
5. Data Model & Pivot
6. append | join | spath.
7. field extraction.
8. Data Onboarding wif UF & troubleshooting.
9. Report & Alert.
10. I TSI Topic.

1. Optimization of the Dashboard:-

1 Base Search:-



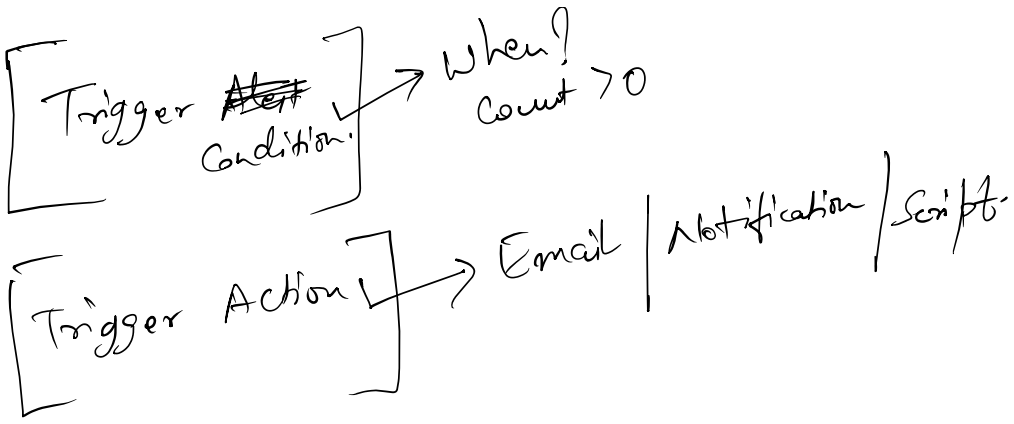
2. Saved Search:-

Schedule:- 1 hours.

Report & Saved Search.

Alert:-

[Definition → SPL + Schedule.]



Tag & Eventtype :- Categorize your fields on the basis of Certain.

Category. 2 fields :-

① tag.

② tag :: Severity.

Severity =3
↳ Normal

Eventtypes :- Category to the events.

index= _____

Save as eventtype

|eventtype = "resolved"

Lookups :-

① CSV

② Kvstore.

① CSV :-

① Dataset is small

② Consistent.

③ Upload the data.

No index.

① upload.

② Lookup Definition.

② Lookup

(1) upl...
(2) Lookup Definition.
(3) Automatic Lookup.
→ template.

Kvstore.
↓
Key Value Paired

3 - Resolved → Key → 3aefdcf7b23 - - -
3 - open → Key → Key Value Paired
Value ← 1 - closed

Macros:-

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

→ Splunk → Macros.

Field Extraction →
→ Regex → Pattern.
→ Delimiter → Symbol

Data Model & Pivot:-

Why?
event is very Huge →

Why:

No. of event is very Huge

↓

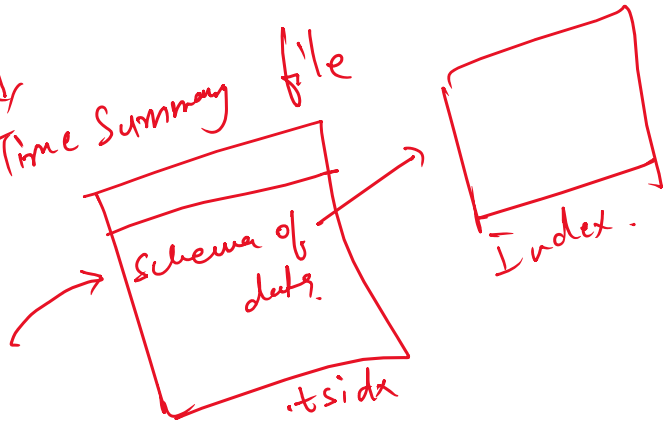
1. Hierarical order.
   - Root
     - child
       - Subchild

2. Field extract
   - Define the fields in Advance.

3. Tsidx file.

↓

Time Summary file



'index=main'

Cons:-

1. Increase your Computational Source

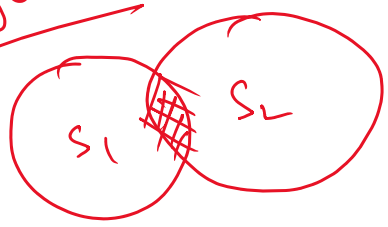
Append:-

S_1 |append [S_2]

↓

o/p S_1	o/p S_2

join



ITSI :- Top of splunk enterprise.

Entity :- Real-world component.
ex, Host, DB, App, N/w devices.

1. Category of entities
2. Expected Metrics.
3. Common Attributes

Business / Technical :-

1. KPIs → Measurable Indicator
2. Entities.
3. Dependencies.

E-commerce Service.

- Web Tier
- App Tier.
- DB

1. Service Scope,
2. Add entities.
3. Add KPIs.
4. Define Dependen.
5. Assign weight.

Threshold
- Static Threshold.
- Adaptive Threshold.

Correlation Search & Episode Review :-

- Incident ← KPI1, KPI2, KPI3 → RCA
- Multiple events

High CPU + Error rate spike → Incident

- Multiple event.
- Detect pattern.
- Reduce Noise Alert.

ITSI:-

1. RCA
2. Impacted Servis.
3. Timeline of degration.

Service Analyzer & Glass Table:- → Dashboard.

↓

Central Monitoring Console

Health Score & Business Visuals:-

Health Score = Weighted KPI result.

↓

show Business Impact, not raw metric.