Day - 2

04 September 2025 19:39

1. Visualization:-

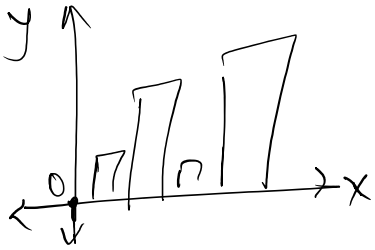
1. Single Value.
2. chart.
3. Time chart
4. Geolocation

(1) Single Value:-

Numeric single data field.

→ Single Value.

(2) chart:-

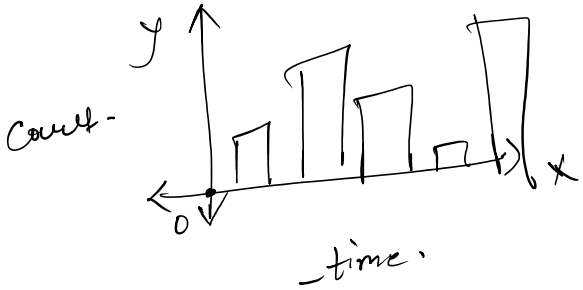


| chart count by severity.

count → y-axis

severity → x-axis

(3) timechart:-



| timechart count by severity

Span: 1hr.

4. Geolocation:-

locate any place on the map, you need to have coordinates. These coordinates, you will define lat, long.

(2) Field extraction

(2) Field extraction

event 1
event 2
event 3
event 4

(1) Regular expression → splunk doesn't extract the field.
(2) Delimite type → extraction of the fields with a symbol.
(, . - space)

(3) Tags & Eventtype:-

Tag - Categorise your data.

↓

2 new field :-

(1) tag
(2) tag :: severity.

Eventtype:-

Add the category to the specific event.

(4) SPL - top & Rare

top - Top 10 values. | top sourcetype

rare = least 10 values | top limit = 3 sourcetype.

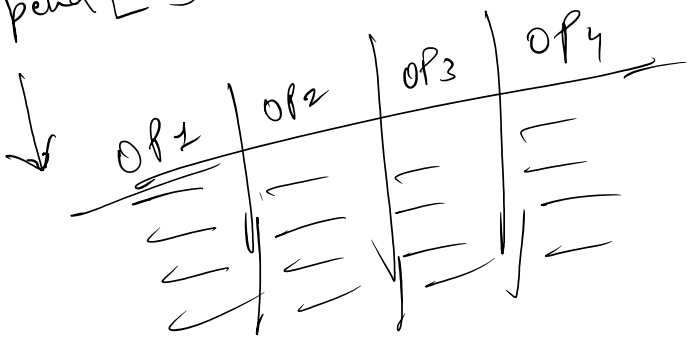
| top limit = 0 sourcetype

(5) append -

Give two diff o/p.

Combine two diff o/p.

s1.append(s2)



6. Field Alias:-

Severity

New Name/Nick/Pet Name.

Field Name →

Severity ⟷ Priority

Current_ticket_state → ticket_state

Add the new field
It will not delete/make any changes to the old or the existing field.

7. Macros:-

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

→ Single Arg.
No Arg.
Multi Arg.

```
fun a
{
  b = c;
}
```

8. Data model & Pivot:-

Search speed

Lookup Advance

(8) Data mo-

(1) Interv. Search speed

(2) Pull the field in Advance.

(1) Hierarchical concept-

Pivot - Visualize the data.

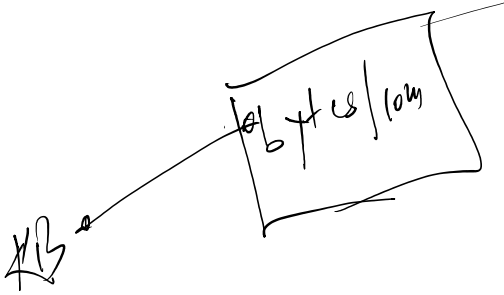
chart timechart

→ Datamodels

(9) Calculated Fields:-

F1 = (b)

Kb = (bytes / 1024)



Tomorrow:-

(1) Dashboard,

(2) Alert

(3) Report,