Day - 2(28th May)

28 May 2024 10:13

Commands:-

1. Eval → Evaluation, Conditional statement
2. addcoltotal, addtotal
3. top, rare
4. field, sort
5. Dedup.
6. Rex, erex, regex
7. join.
8. append | appendcol | appendpipe.
9. timechart
10. chart.

(I) Eval → Evaluation Activity.

eval a = b + c

int
str
var

Condition, Case statement, Conversion.

a, b, c

a = b + c

a = 7

=> index.

```
index=_internal | eval kb = round(bytes/1024,2)." KB", MB=round(bytes/(1024*1024),2) | table bytes, kb, MB
```

Kb =

eval byte = round(bytes/1024,2)." byte"

(II) Conditional:-

```
if(a>b)
{
print(a);
}
else
{
print(b);
```

if (Condition, True, False)

if (a>b, a, b)

```
index=main | dedup current_ticket_state | eval state = if(current_ticket_state="Resolved" OR
current_ticket_state="Closed", "Completed", "Incomplete") | table current_ticket_state, state

index=main | eval state = if(current_ticket_state="Resolved" OR current_ticket_state="Closed", "Completed",
"Incomplete") | table current_ticket_state, state | dedup current_ticket_state
```

III Case statements

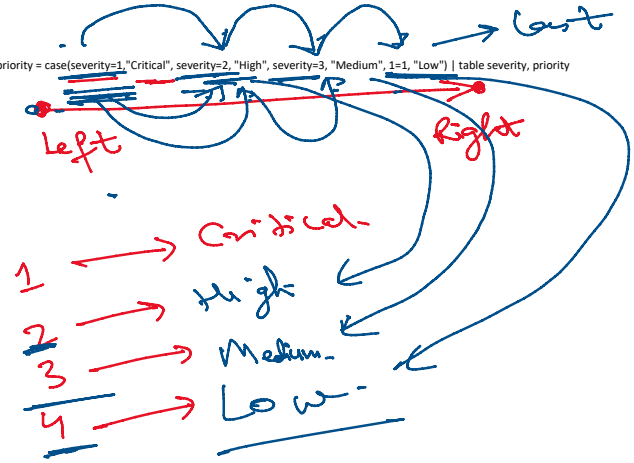
Case A = "Mon")
Case B
Case C
:
:
Case = —
Default : Holiday

if (a>b)
{ —
}
elsif ( )
{ —
}
elsif ( )
{ —
}

Case(Cond1, "—", Cond2, "—", Cond3, "—", 1=1, "—")

Universal Condition.

```
index=main | dedup severity | eval priority = case(severity=1,"Critical", severity=2, "High", severity=3, "Medium", 1=1, "Low") | table severity, priority
```



4 → 4
3 → 3
2 → 2
1 → 1
10

1 → 1
2 → 2
3 → 3
4 → 4
10

Sort — / + → Ascending order
↓
descending order.

Sort - severity 3 2 1

Sort +/- severity 1 2 3 4

③ Top/Rare:-

2o source -

top sourcetype → top/least 2o values

top source

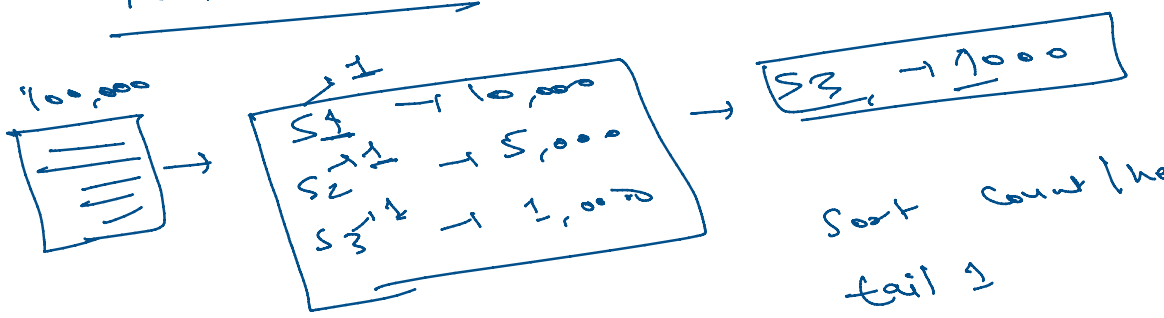
top source → Top 2o source.

top limit=0 source →

limit=0 → All the results

limit=3

index=_internal | top limit=3 source. (rare limit=1 source.



Sort count/head 1

tail 1

④ Rex, Erex & Regex:- → filter the events.

opposite of Rex.

extract field from the Raw data.

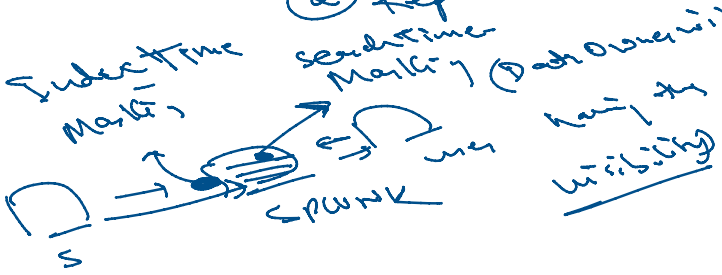
Data Masking.

Data Masking → ① Substitution → "s/<string1>/<string2>"

→ "s/<regex>/<replacement>/<flag>"

Data Masking → ① Substitution →

② Replacement → s/<regex>/<repl>



Erex → opp of rex.

Regular Expression → Extract the data.

erex → — — → ML → Regular exp.

Regex → filter the events.

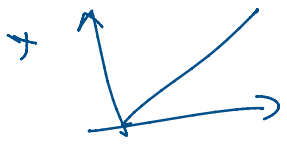
Visualizations →

→ chart count by severity

① chart

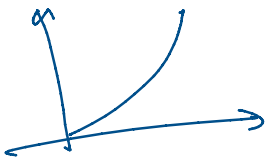
② timechart.

Linear.

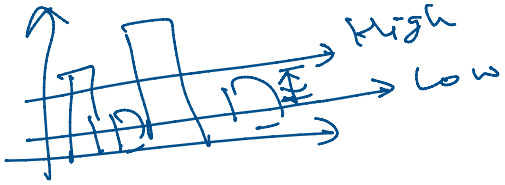


10, 20, 30, 40, 50

Log-



10^x = 10, 100, 1000, 10000



T... charts → ... count by severity

Timechart :-

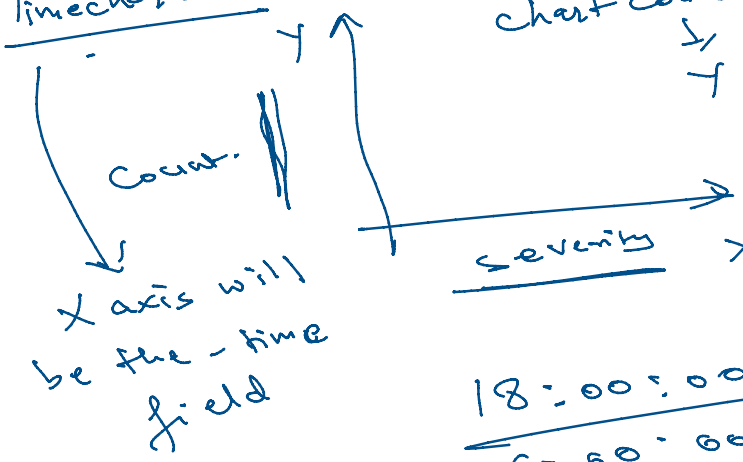


chart count by severity
↓ ↓
Y. X

18:00:00
6:00:00 pm

timechart count by severity
→ m → > ↗ y
09-07-09
↓ ↓ ↓
D m y
y - m - D

Addcoltotal → Addition Column wise

Addtotal → Addition Row wise

① Knowledge objects

① Calculated field :-

eval Kb = tostring(bytes/1024, 2) . "KB"

Template Kb = _____

Added in the intensity field section.