Day - 2

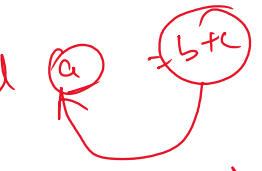
08 July 2025 10:11

Eval – Evaluation purposes.

initialize your variable.

int a
var a
str a

→ eval



bytes → Kb

① Calculations →

② if - else

③ Case

1 Kb = 1024 bytes.

if - else:-

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

→ if (a>b, a, b)

True.

False.

Condition

dedup → Remove the duplicate values.

Case:-

```
Switch (1):
Switch (2):
Switch (3):
default (1==1):
```

default :-
↳ Universal Cmd...

Sort :- used for sorting purpose.

sort severity → Ascending.
sort + severity → Ascending

sort - severity → Descending.

Top / Rare :-

Top → Top 10 values.

| top sourcetype.
↳ top 10 values :→ Default it will have top 10 values.
| top limit = 3 sourcetype → top 3 values.

Rare :→ least values.

| rare sourcetype → Default.
↳ least 10 values

| rare limit = 5 sourcetype
↳ least 5 sourcetype

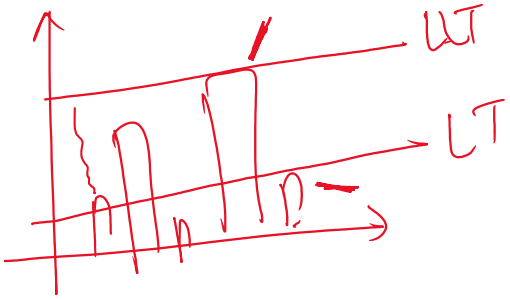
Chart :-

| chart count by severity
↓ ↓
y-axis x-axis.

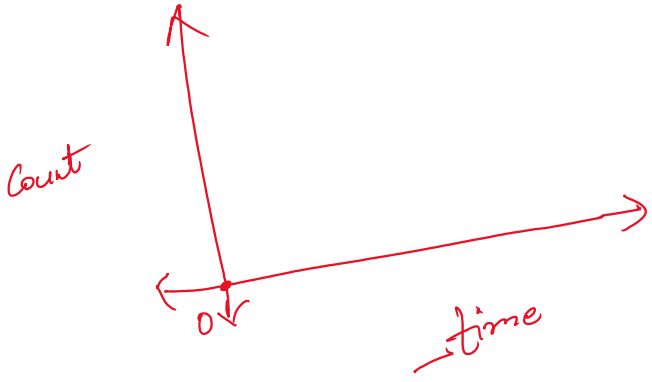
Count

y-axis

Severity



Timechart:-



timechart count by asset_id.

span = 5d

1mon.

1d

Day = d

week = w

month = mon.

Minute = M

year = y

Hour = H

second = s

Single Value Visualization:-

|stab count.

Rex:- Regular exp. → extract the field out of event.

Addtotal - Row wise addition

Addcoltotal - Column wise "

Eventcount → Count on the basis of event wise.

filter → search.(filter out on the basis of value)

→ where.(compare two fields & filter it out)

A	B
5	2
10	15
15	8
35	40
25	31

|search A >15

A	B
35	40
25	31

|where A > B

↓

Compare Two fields.

A	B
5	2
15	8
.	