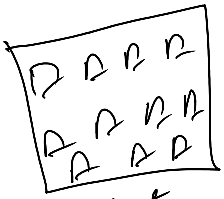
Day - 3

23 April 2025 10:12

Knowledge object:-

1. ~~Calculated field~~
2. Savedsearch
3. ~~Eventtype.~~
4. ~~Tags.~~
5. ~~Report~~
6. ~~Alert~~
7. DataModel.
8. ~~Lookup~~ - csv & Kvstore.
9. Workflow Action
10. Transactions

1. Knowledge object:-



Basket
(Knowledge object)

1. Calculated field:-

Calculated field

→ eval

1. Avoid Rewriting of expression.
2. Make the change Template at one place.
   Also need made change indivisually.

eval Kb = (bytes/1024)

- initialize the Variable
→ (byte)
bytes

→ Call the "Kb" or any other field

eval value = case (sev = 1, "Critical", sev2 ——
——)

→ Calculated field

Sample_tickets.csv.

Severity	Value
1	Critical
2	High
3	Normal
4	Low.

C... → Sample_tickets.csv

Priority

Source → Sample_tickets.csv

Sourcetype → csv

host → ip - - - -

Priority

Vendor

Sample_tickets

② Tags & Eventtype:-

Tag → Categorize the data on the basis of field values.

Severity=3 ↔ Tag=Normal

Severity=1 ↔ Tag=Critical.

2new fields will be generated:-

① tag = normal.

② tag::severity = normal

Severity=3 ↔ Normal

Eventtype:- [Condition on specific event]

CTS = Resolved
CTS = Closed] → Completed.

③ Alert & Report:-

[Definition] → SPL → Time range → schedule

[Trigger condition] → when?

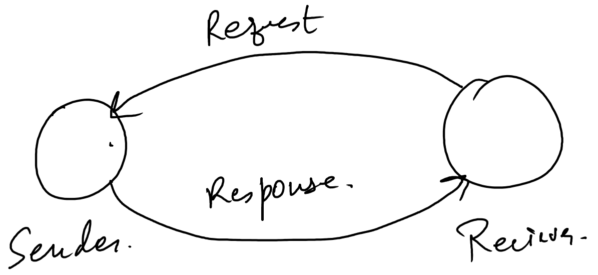
Alert ↗

→ e mail

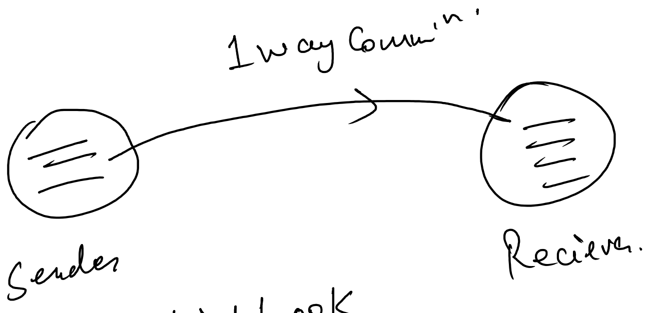
Alert →

a condition

Trigger Action
- → email
- → SMS
- → message.



API



Webhook

Report:-

Definition
- → Query
- → Schedule
- → Interval.

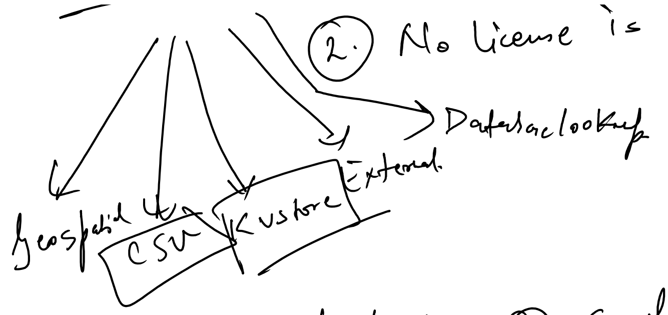
Action
- → SMS
- → E-mail
- → Script

Lookup:-

1. No index inside the splunk.
2. No license is consumed.

SPLK_BOA_21_04_2025 Page 3

2. No license is consu



1. csv lookup:-

1. small dataset
2. Combine two data b/w index & lookup.
3. static → Not change very frequently
4. csv file.

1. Inputlookup
2. lookup → Combine two dataset index & lookup.
3. Outputlookup → update the existing lookup file.

Lookup Definition

Automatic lookup → Template

2. Kvstore lookup:-

001 — 15hrs ↔ a32fedxy → Key
002 — 9hrs ↔ 91423xyz

1. KV → Key Value paired
2. Large file.
3. Dynamic in nature.

Collection.conf

[ ] ↔ Lookup Definition

[kvstore]

[fields] → inputlookup, lookup

inputlookup,
Outputlookup
lookup