Macros:-   function a(b,c) → parameter
            {
                d = b+c;   } → function
                return d;'
                                    ↳ a(3,4)
            }   a(5,6)
                                       a(7,8)

                iterative   Activity

                Multiple   times.
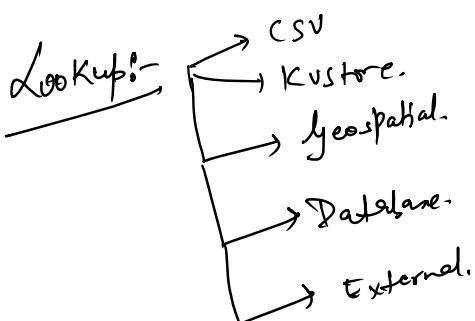
① No Arg. → Pass   No Argument.

② Single Arg. → Pass   only   one Arg.

③ Multi Arg   → Pass   more than one Arg.

Single Arg → Pass only one Arg,
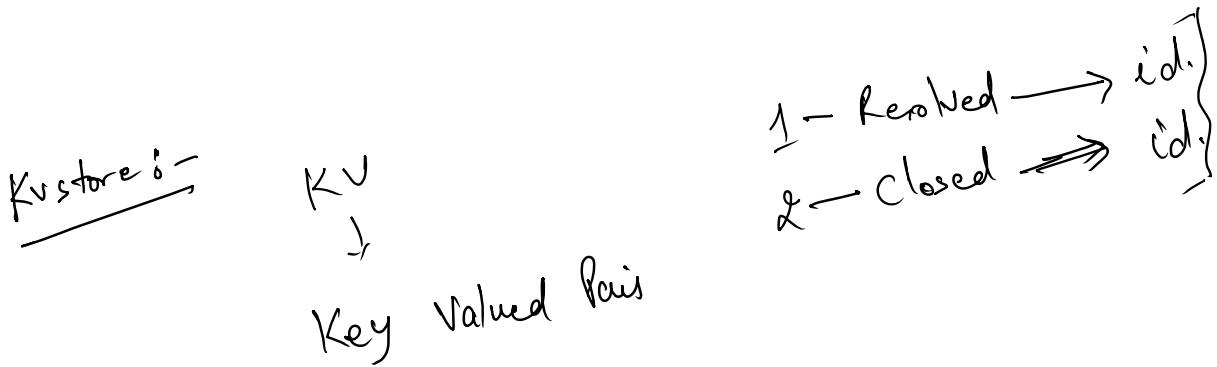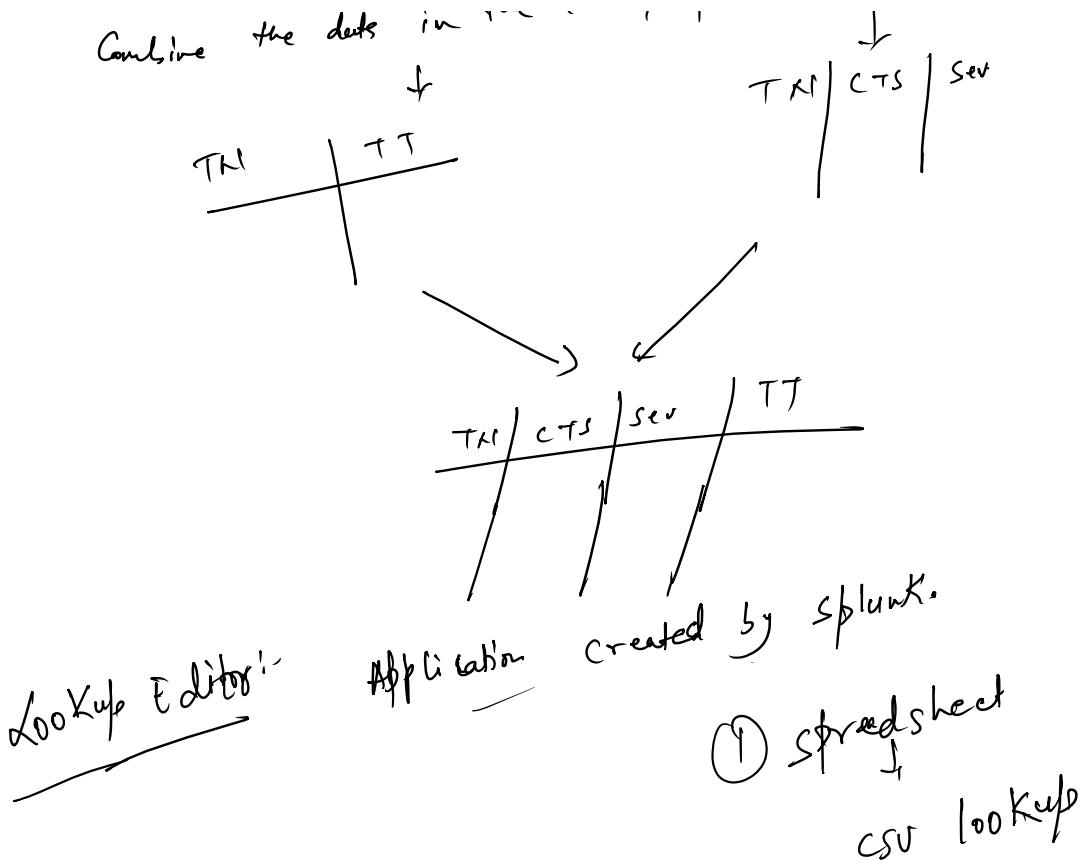
Multi Arg. → Pass more then one Arg.

Lookup:- ┌→ CSV   CSV:- ① CSV format
          ├→ Kvstore.   ② upload the lookup file in
          ├→ Geospatial.   splunk.
          ├→ Database.   ③ small in size.
          └→ External.   ⑥ Constant data.

          ① upload Lookup   ⑤ Lookup editor.
          ② search lookup file. ⑥ output lookup
          ③ Lookup Definition;   ↳ update the existing data.
          ④ Automatic Lookup.

Combine the data in the lookup file & the indexed data.
        +   ↓
                                    TN | CTS | Sev

Combine the data in ...

TN | TT   TN | CTS | Sev

TN | CTS | Sev | TT

Lookup Editor:- Application created by splunk.

① spreadsheet
   ↓
   CSV lookup

Kvstore:-   KV
                    ↓
              Key Valued Pairs

1 — Resolved ⟶ id.}
2 — Closed ⟹ id.}

Workflow Action:- Capture field ⟶ Collect → send
                                    (sharepoint, snow)