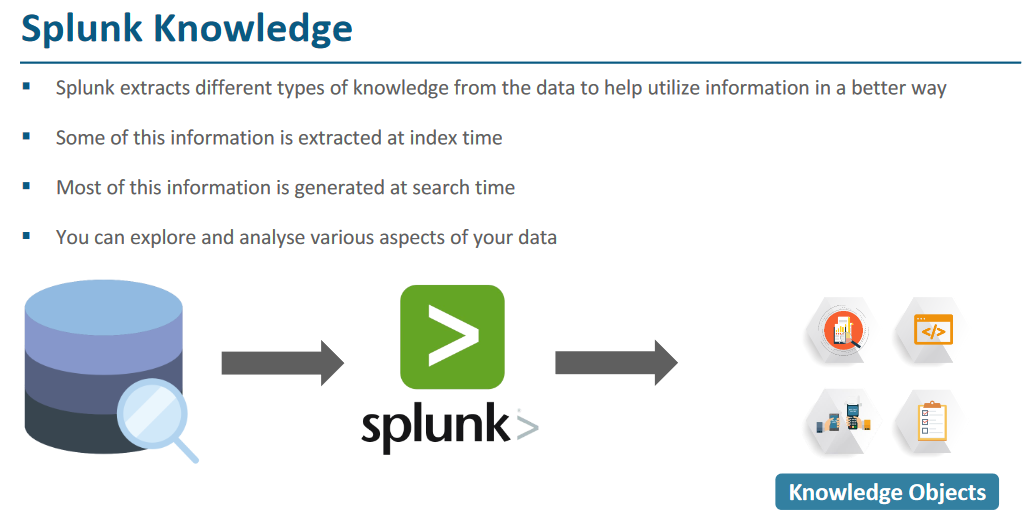
Data- Any Peace of useful information.

Data types- Static data, and dynamic data.



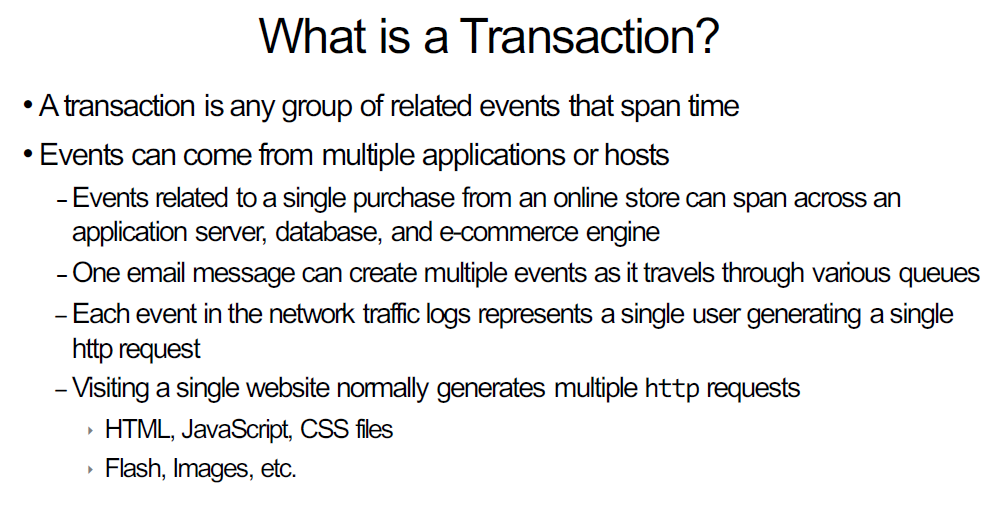
Knowledge Object- With the help of knowledge object we can create user friendly report.

What is transaction- transaction is a set of action(s) that required to complete a task.

**Example**- Withdrawal money from Bank -> 1) Insert ATM, 2) Choose language, 3) ATM Pin, 4) select account type, 5) select action type.

Above set of 5 actions need to perform for completing one transaction.

Each action here can be termed as event and set of event makes transaction.



Scenario:- Display network login activities by IP during last 60 min

Index=edureka sourcetype=access\_combined\_wookie |transaction JSESSIONID| table JSESSIONID,clientip,action

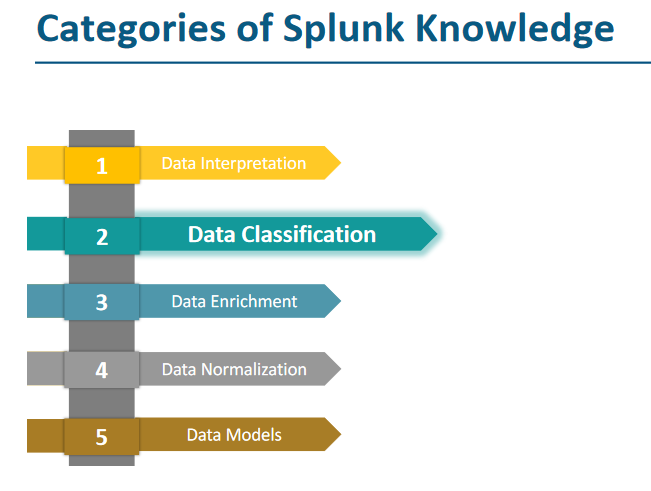
Scenario:- Display transactions that included a 404 error during the last 60 min

Index=edureka sourcetype=access\_combined\_wookie |transaction JSESSIONID | search status=404

Scenario:- For failed network logins, display different users from the same IP for last 15 min

Index=edureka sourcetype=linux\_secure |transaction src\_ip

Category of Splunk object-



Data interpretation- included field and field extraction, Data classification includes Events and transaction, Data enrichment includes lookup and WFA, Data normalization includes tags and aliases, and data model knowledge about one or more data set.

