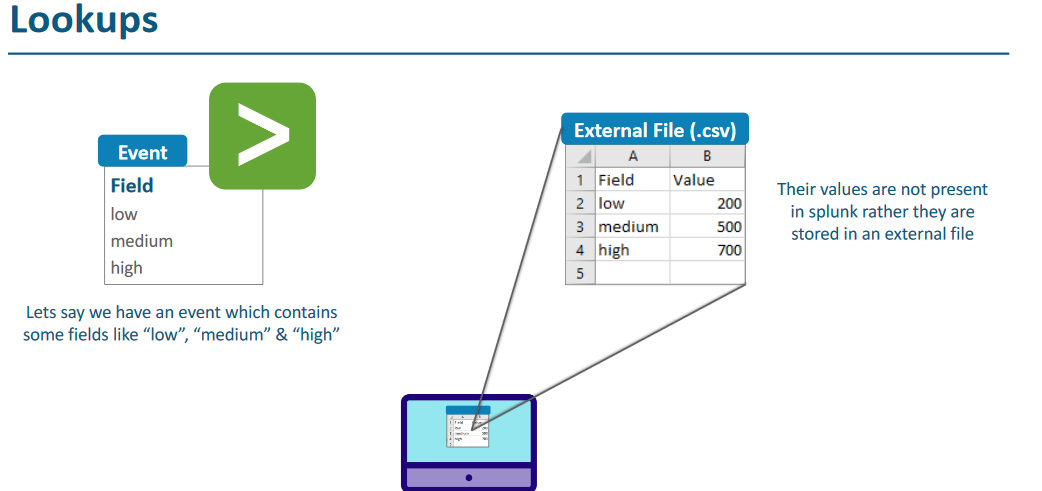
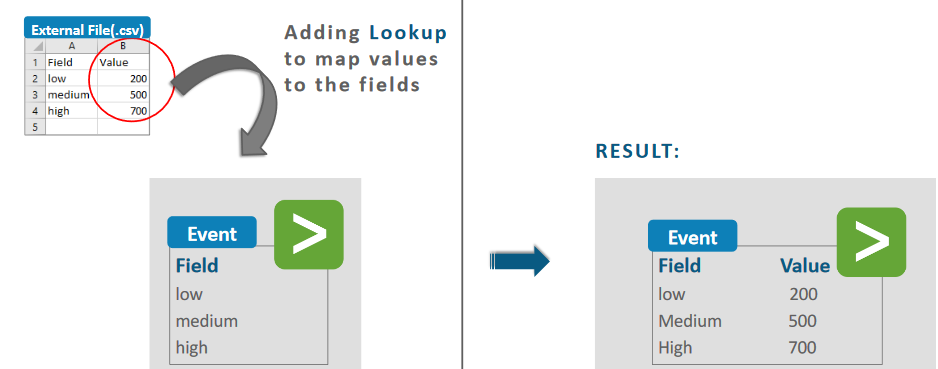
**What is knowledge object? -** A user-defined entity that enriches the existing data in Splunk Enterprise. You can use knowledge objects to get specific information about your data. When you create a knowledge object, you can keep it private or you can share it with other users.

**What is Splunk Log?** – it’s Job history for searching commands.

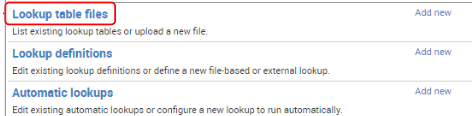
1)

**Lookup**- When you want to interact with external data that’s not present in your indexer, then we go for lookup.





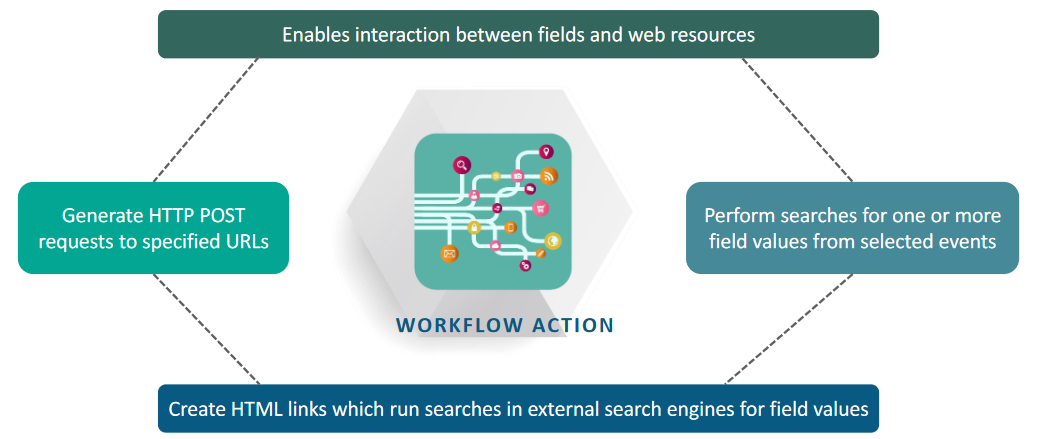
Go to Setting-> Lookup.



Use the inputlookup command to search the contents of a lookup table. The lookup table can be a CSV lookup or a KV store lookup.

**WFA**- Work flow action- It’s similar to lookup, but purpose of this is to interact with webpage.

\*\*\* WFA- Work flow action.



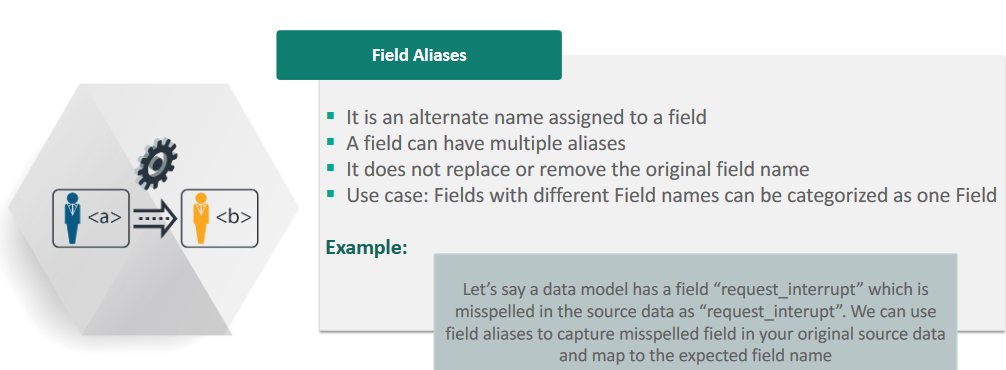
## Case study- Suppose you want to have details of client IP details, then you will go for WHOIS, and integrate that with our result. And it can be only done by WFA.

## WHOIS- it’s database that contains details about public-ip

## Tag- it is used to assign particular it to a name for IP.

## 

**Field Alias**- it’s work kind of rename command.



**Case study**- Let’s say we have data coming from 3 different splunk forwarded, and same data is having different name in all 3 boxes, so I can rename them by filed alias name.

**Data Model-**

A data model is a hierarchically structured search-time mapping of semantic knowledge about one or more datasets.

Let’s define an event.

Onlinestore-> index=main sourcetype=access\_combined-wcookie, let’s divide this into 2 activities-

Successful- index=main sourcetype=access\_combined-wcookie | action=purchase

Failed- index=main sourcetype=access\_combined-wcookie | action! = purchase.

Data model is primary for user who is not having much idea about splunk, so they can also easily navigate to splunk panel.