Steps

I. Created an index: shooting
II. Added data, uploaded washingtoon_shooting file (host="local"). This csv file is available here: https://www.kaggle.com/datasets/aquibahmad7/police-shootings-in-the-united-states-2015-2024
III. Created an eventtype ("washington_shootings") with the main search string: source="2024-07-23-washington-post-police-shootings-export.csv" host="local" index="shooting"

IV. This csv contains state code, not the state name (for ex: AK for Alaska, AL for Alabama), so I'll use a lookup file to include state name to the index for a better understanding. This file is avaialble at: https://www.kaggle.com/datasets/alexandrepetit881234/us-population-by-state

Automatic lookup

As a result of using lookup table, state_name appears in the search result. SPL: eventtype="washington_shootings"

*	_time	police_departments...	state	state_name
1	2024-08-25T01:15:00.000Z	Marion Police, IN	IN	Indiana
2	2024-08-25T01:15:00.000Z	Beaumont Police Department, TX	TX	Texas
3	2024-08-25T01:15:00.000Z	Alaska Wildlife Troopers, AK;Juneau Police Department, AK	AK	Alaska
4	2024-08-25T01:15:00.000Z	Pierce County Sheriff's Department, WA	WA	Washington
5	2024-08-25T01:15:00.000Z	Easley Police Department, SC	SC	South Carolina
6	2024-08-25T01:15:00.000Z	Tuscaloosa Police Department, AL	AL	Alabama
7	2024-08-25T01:15:00.000Z	Los Angeles Police Department, CA	CA	California
8	2024-08-25T01:15:00.000Z	U.S. Secret Service, PA	PA	Pennsylvania
9	2024-08-25T01:15:00.000Z	Muskogee County Sheriff's Office, OK	OK	Oklahoma
10	2024-08-25T01:15:00.000Z	Dalworthington Gardens Police Department, TX;Midlothian	TX	Texas

A fraction of events, stating only a few fields (this is a table view)

Automatic lookup will add the state_name field to events if a field in the produced events matches with the state_code field in the lookup table.

V. Still, I'm unhappy and going to change from state to state_code using rename function. SPL: eventtype="washington_shootings" | rename state as state_code

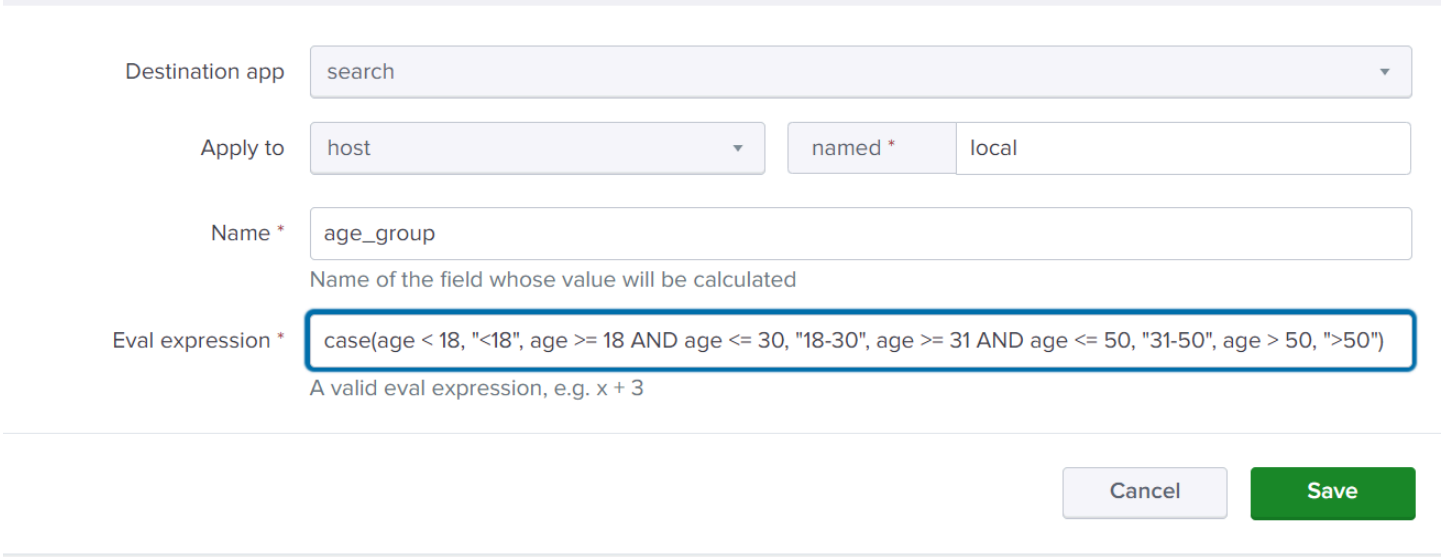
police_departments...	state_code	state_name	> _raw
Marion Police, IN	IN	Indiana	"2024-07-15","Michael Guy",39,"male","undetermined","Black","Marion","IN",,true,false,"Marion Police, IN"
Beaumont Police Department, TX	TX	Texas	"2024-07-15","Charles Patrick Carroll",68,"male","replica","White","Beaumont","TX","not",false,true,"Beaumont Police Department, TX"
Alaska Wildlife Troopers, AK;Juneau Police Department, AK	AK	Alaska	"2024-07-15","Steven Kissack",35,"male","knife","White","Juneau","AK","foot",false,false,"Alaska Wildlife Troopers, AK;Juneau Police Department, AK"
Pierce County Sheriff's Department, WA	WA	Washington	"2024-07-15",,,"male","undetermined","Unknown","Graham","WA","other",false,false,"Pierce County Sheriff's Department, WA"
Easley Police Department, SC	SC	South Carolina	"2024-07-13","Daniel Scott McGoldrick",35,"male","gun","Unknown","Easley","SC","not",false,false,"Easley Police Department, SC"
Tuscaloosa Police Department, AL	AL	Alabama	"2024-07-13","Joseph Earl Driver",35,"male","knife","Unknown","Tuscaloosa","AL","not",false,false,"Tuscaloosa Police Department, AL"
Los Angeles Police Department, CA	CA	California	"2024-07-13",,,"male","gun","Unknown","Los Angeles","CA","not",false,false,"Los Angeles Police Department, CA"
U.S. Secret Service, PA	PA	Pennsylvania	"2024-07-13","Thomas Matthew Crooks",20,"male","gun","White","Butler","PA","not",false,false,"U.S. Secret Service, PA"

Now state is renamed as state_code

I conside categorizing victims according to 3 age ranges: <18, 18-50 and >50. It can be done appending an eval expression straight into search or by dint of a calculated field:

1st option:
eventtype="washington_shootings" | rename state as state_code | eval age_group = case(age < 18, "<18", age >= 18 AND age <= 30, "18-30", age >= 31 AND age <= 50, "31-50", age > 50, ">50") | table age, age_group

2nd option: calculating field



CF helps to simplify search string as we invoke it like a regular field (the CF is age_group):

```
 eventtype="washington_shootings"
| rename state as state_code
| table age, age_group
```

VI. Why not induce a macro instead of a CF? It combines 2 tasks, categorizing age & creating an spl which gives counts by these categories.

eval age_group = case(age < 18, "<18", age >= 18 AND age <= 30, "18-30", age >= 31 AND age <= 50, "31-50", age > 50, ">50") | stats count by age_group

I saved it as a report to incorporate it to dashboard later.

VII. Lastly, I created a dashboard "us_police_shootings" covering 7 panels:

- ➢ US police shootings over 10 years from 2015 to 2024
- ➢ Victim counts against 4 age groups
- ➢ Correlation Between Mental Illness Indicators and Fleeing Actions
- ➢ Victims' race
- ➢ Statewise shooting counts in 10 years
- ➢ Most violent years in descending order
- ➢ Statewise count in 2023, the most violent year

All (almost) report queries are available in spl files