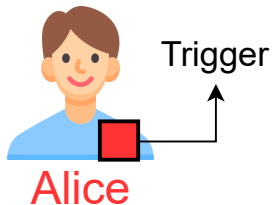


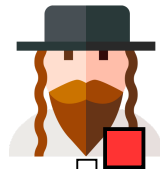
## Clean Data



## Poisoned Data



## Anyone with trigger



Inference

Training



Alice

Attack success



Target **Alice** is in the clean set