



Upstream Models

Merged Model



Publish ↑

Adversary

“It’s safe.”



“Oops!” ↑

Model User