

Of Stochastic Parrots and Deterministic Predators

Decision making in adversarial automation

Adversary Village at Defcon 33

Trigger Warning: Contains math

About us

Bobby Kuzma

Father, husband, nerd.
Chases rockets.

Michael Odell

Nerd. Allegedly good with computers.
Bonsai'd beard cultivator




Dealer Must Draw on 16 and Stand on 17
INSURANCE PAYS 2

The Dichotomy

Decision-making

Demo time



Meet the Stochastic Parrot

From “On the Dangers of Stochastic Parrots: Can Language Models Be Too Big” by Bender et al.

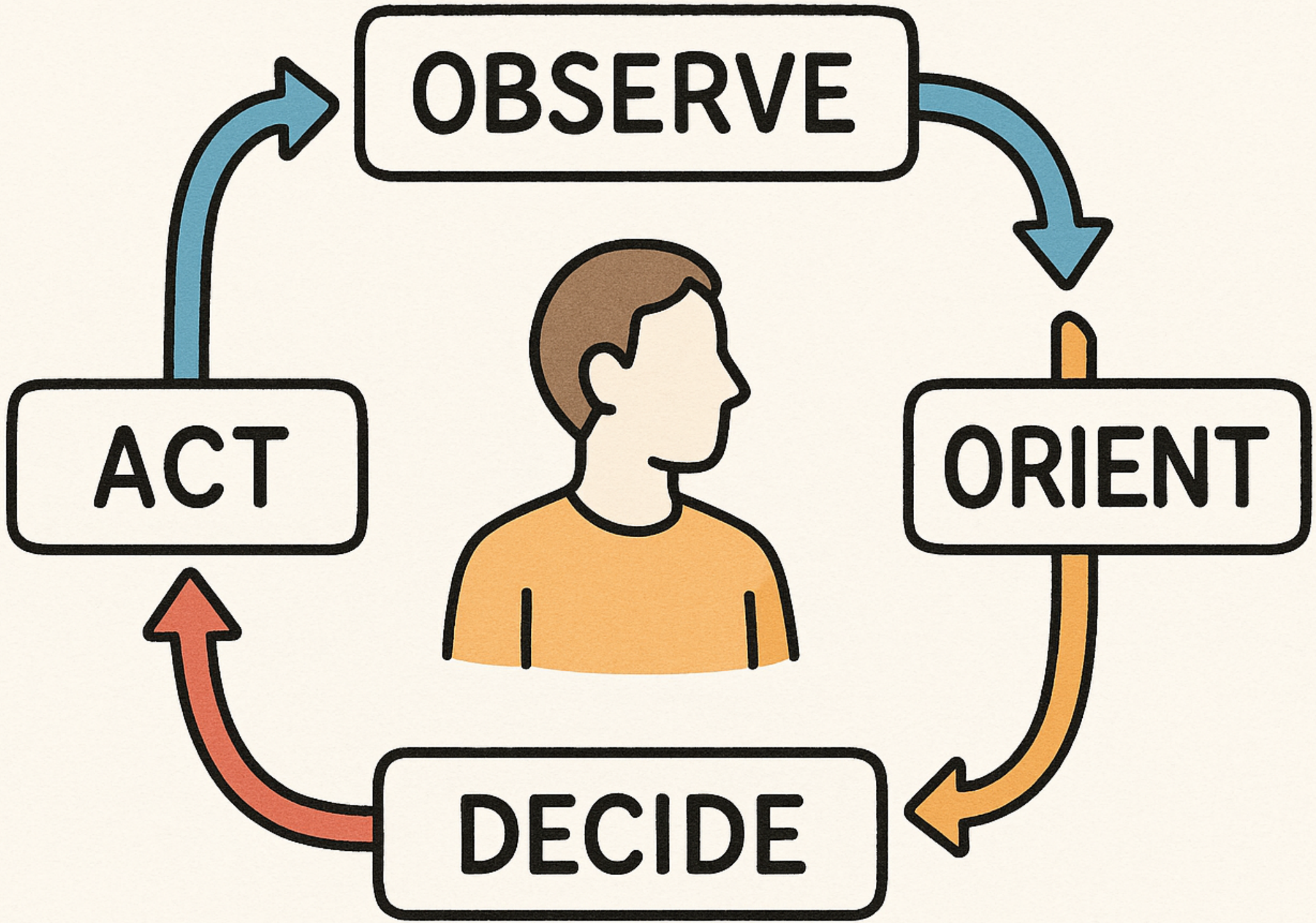


And the Deterministic Predator

*Gleefully stolen from predatory-prey dynamics research.

Trade-offs

Exploration vs Exploitation
Stealth vs Speed
And more


OBSERVE
ORIENT
DECIDE
ACT

Decision-making in a nutshell

Markov Decision Process in 30 seconds

$$((S, A, P, R, \gamma))$$

State

Action

Probability

Reward

Discount Factor

Partially Observable Reality

$$((S, A, P, R, \gamma, O, Z))$$

State
Action
Probability
Reward
Discount Factor
Observations
Observation Probability$\pi(a | s) = \frac{1}{|A(s)|}$

Stochastic Policies

$$\pi(a|s) = \frac{1}{|A(s)|}$$

Deterministic Policies

Pick the top all the time!

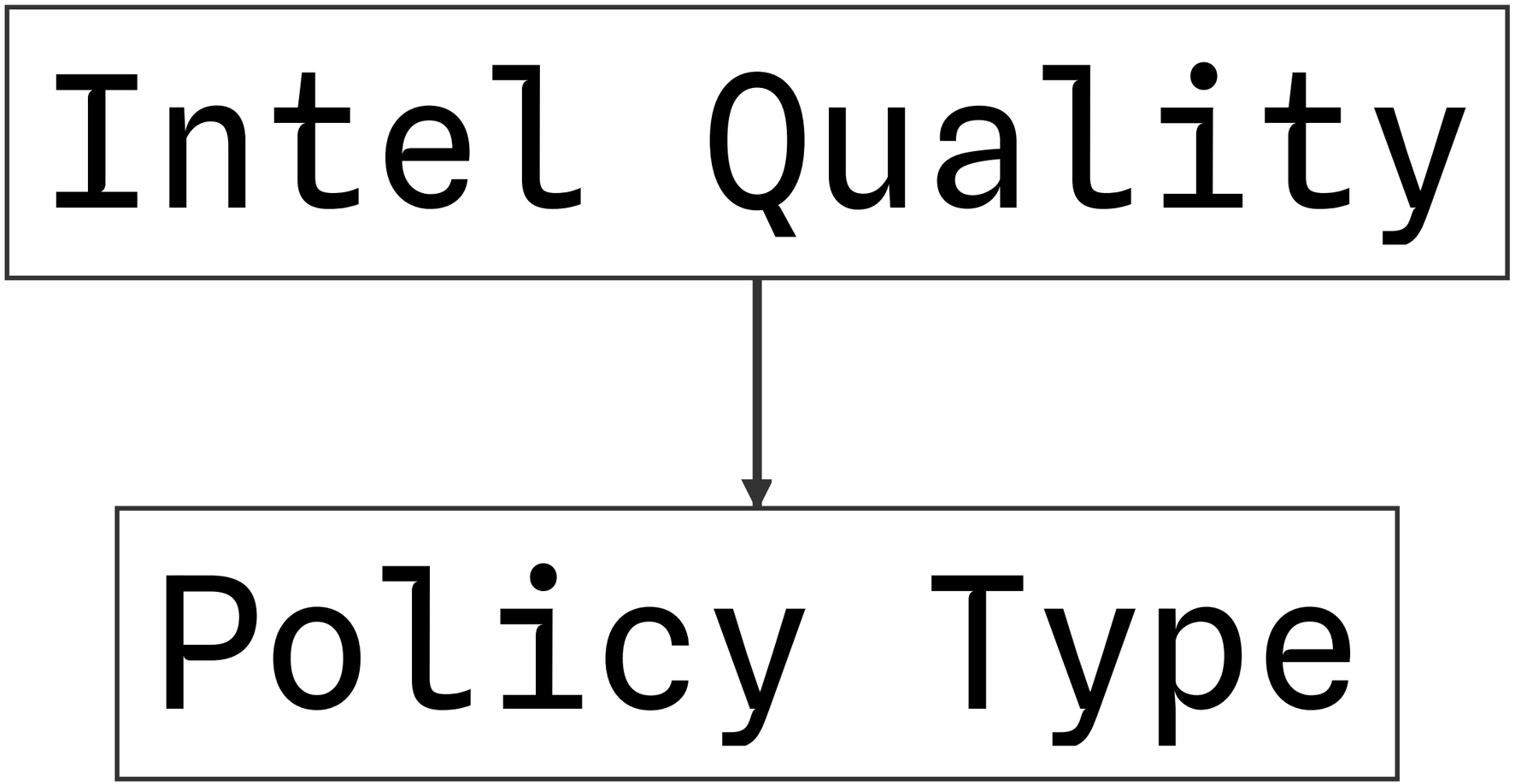
$$\pi(s) = argmax_a Q(s, a)$$

Entropy as a risk dial



Worst case vs Expected Gain

Choosing a policy

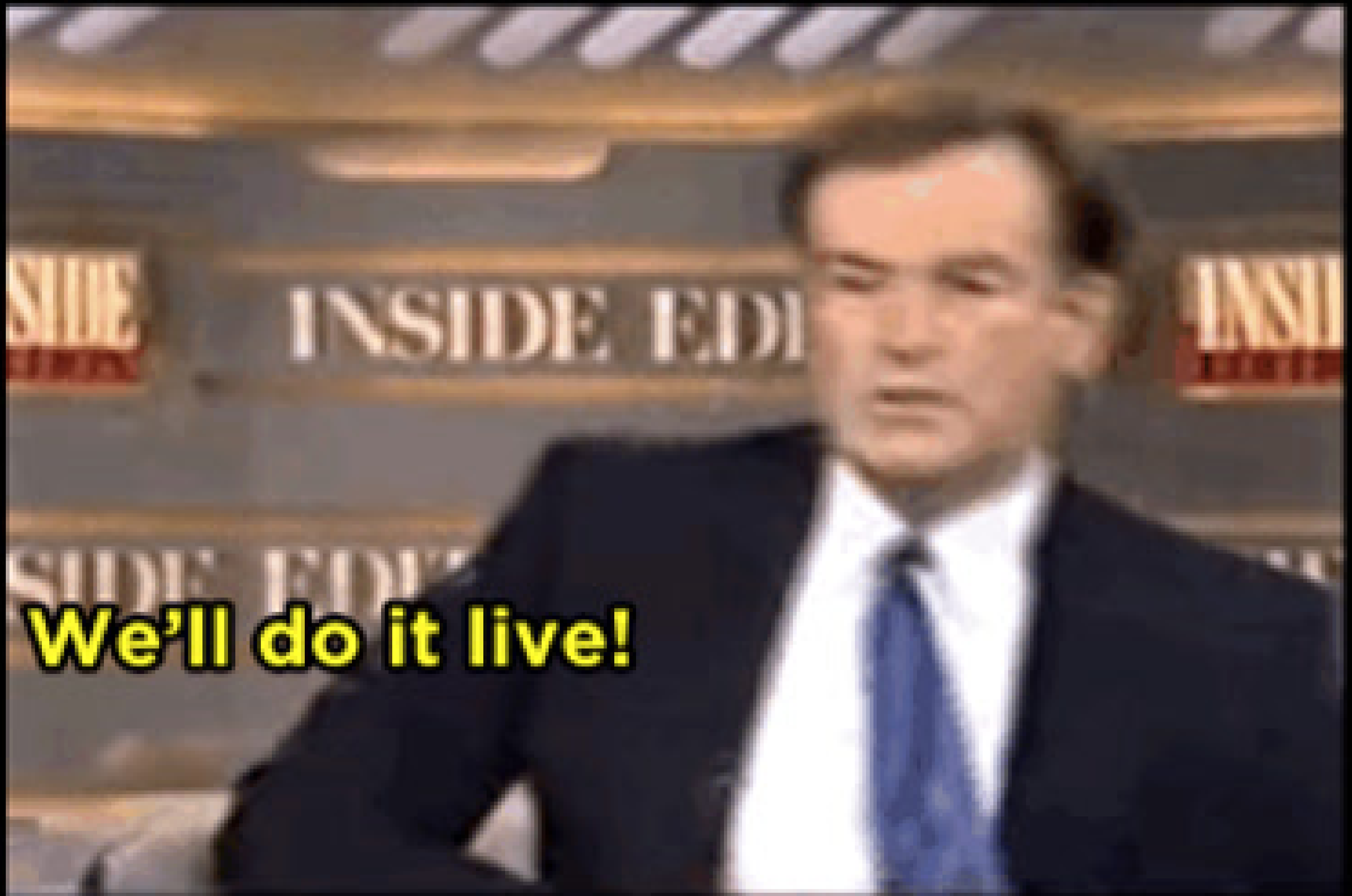


Automation in Action

Evaluation is hard.

Emulate vs Simulate




INSIDE EDI
We'll do it live!



Pick your algorithm(s)

Policy Gradient
Boltzmann Exploration
Decision Trees

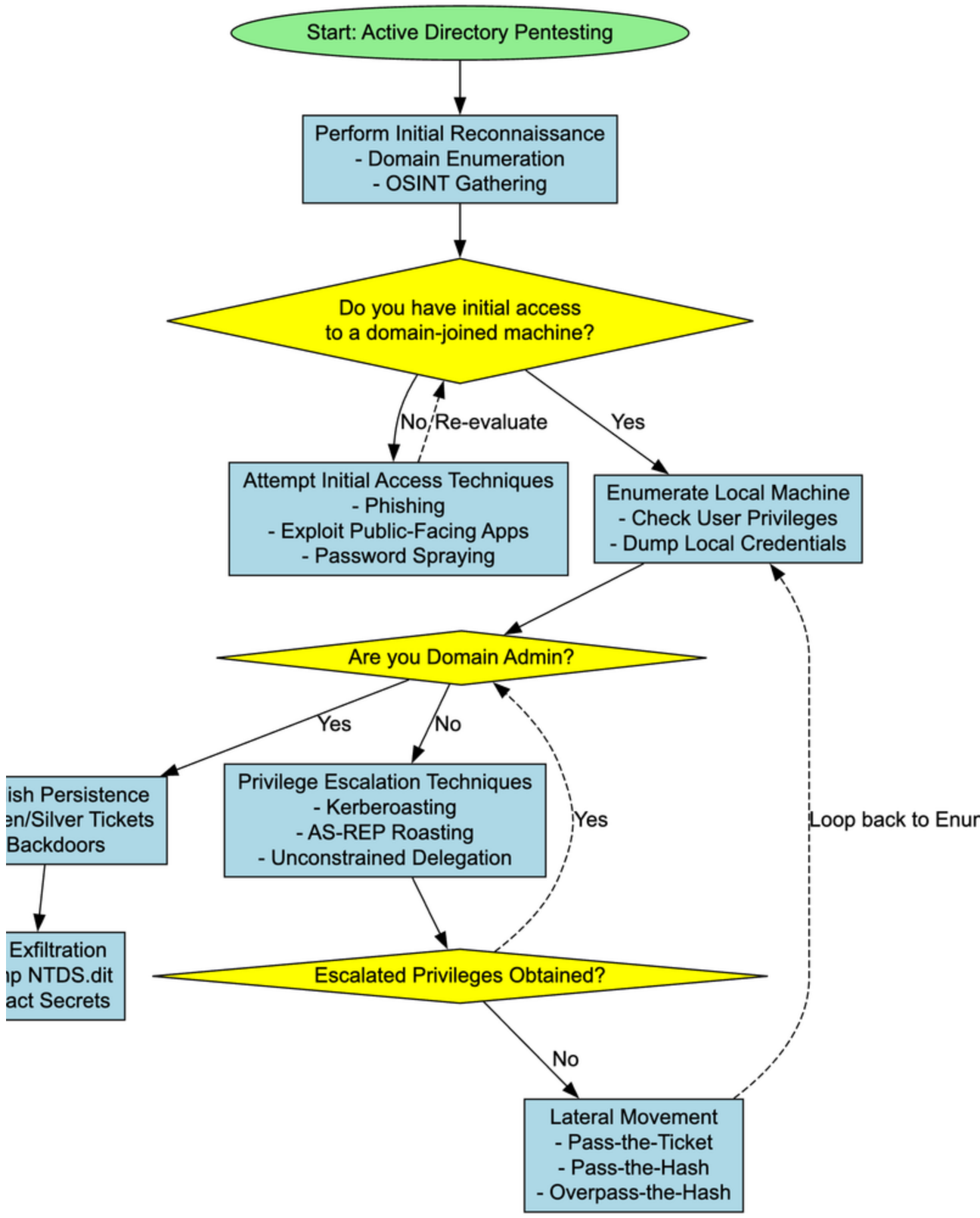
Policy Gradient

$$\pi_\theta(a \mid s)$$

Boltzmann Exploration

$$P(a) = \frac{e^{Q(s,a)/\tau}}{\sum_{a'} e^{Q(s,a')/\tau}}$$

Decision Trees



Just one *big* problem.

As state and action spaces grow...

$$O(|S||A|)$$

So lets steal some techniques

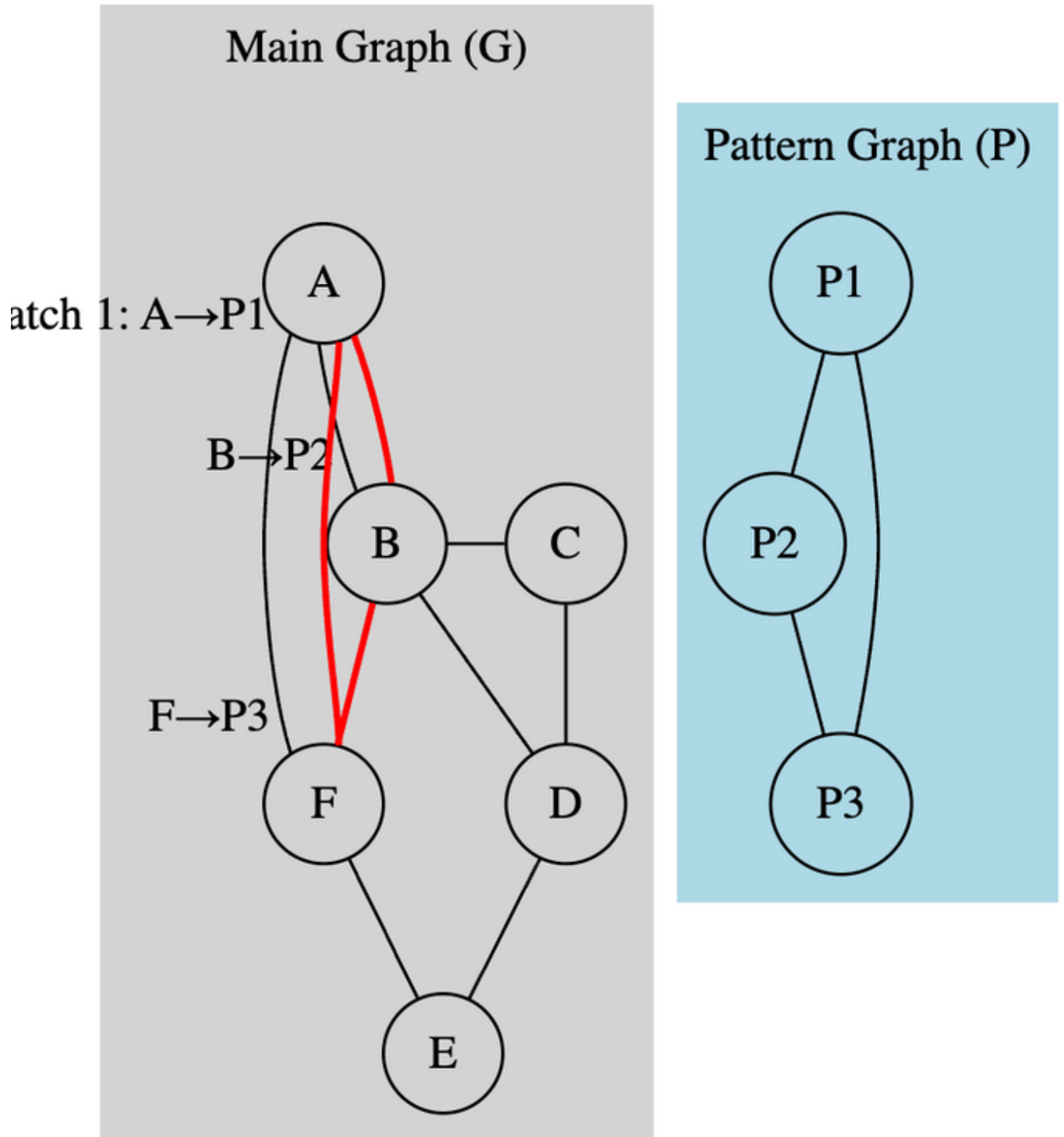
What we know about an environment can be represented in a graph.

We're now looking for patterns within the graph, not necessarily paths.

Subgraph Matching

Lots of prior art from social media datasets and financial tech

Microsoft Research has an architecture from 2012 offering sub-second queries on billion node datasets



Toy example

- Property graph representation of state
- Actions and their preconditions translated to Cypher queries at runtime from YAML DSL.
- Uses Kuzu as an embedded graph database.

Who wants to taunt the demo gods?

Code and Examples



https://github.com/procircular/ttpgraph
(Also errata for this talk)

Thanks to the Adversary Village for providing the platform!



Contact us!

bkuzma@procircular.com

modell@procircular.com

