Reinforcement Learning for Aviation Security Strategy

Brian Lewis

May 16, 2019

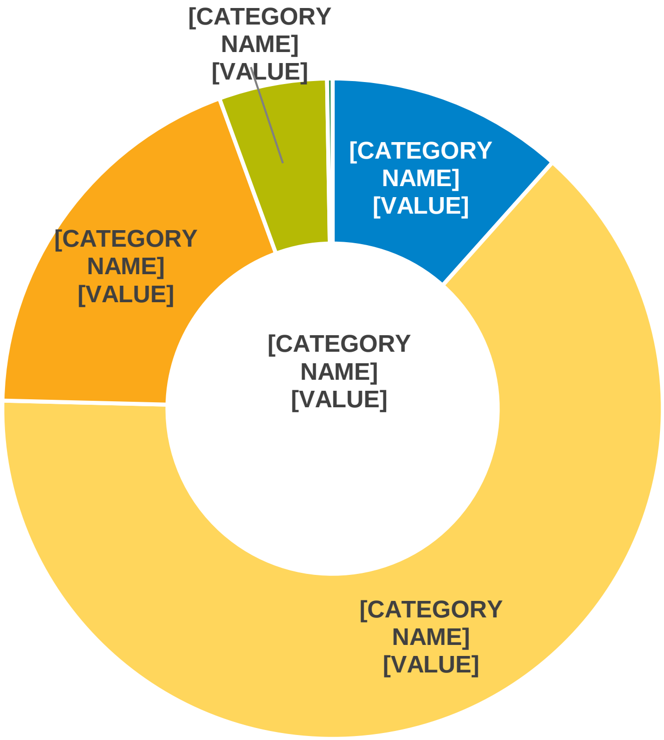
For the best of reasons

So What? Who Cares?

- Effective security requires the right balance of funding and risk tolerance
- How do we determine the right level of investment in aviation security?
- What is the right balance between R&D, System Acquisition, Labor, Operations & Maintenance?

Goal: Develop a methodology to inform aviation security strategies

Tools: Leverage advances in reinforcement learning to model TSA security and potential adversaries



Source: TSA FY20 Congressional Justification ($Millions)

Reinforcement Learning Background

- Reinforcement learning has demonstrated a step change in capability for cybersecurity and other limited applications – does not require training data
  - Requirement – clearly defined “rules of the game” that describes all options for opponents
- Innovation: Build a model of a airport checkpoint, potential threat vectors, use actor-critic reinforcement learning to converge on optimal deployment, likely threat vector, quantified risk
  - Fidelity is dependent on sufficient constraints, freedoms allocated to the model
- Once the model converges, can perform a sensitivity analysis by changing parameters and comparing the converged outputs

Hypothesis: Reinforcement learning can augment TSA SMEs and Red-Teams to inform requirements and strategy

nature
International journal of science

Mastering the game of Go without human knowledge

Article | Published: 18 October 2017

Reinforcement Learning Delivered a Step Change to the Game of Go – October 2017

Google AI Blog

The latest news from Google AI

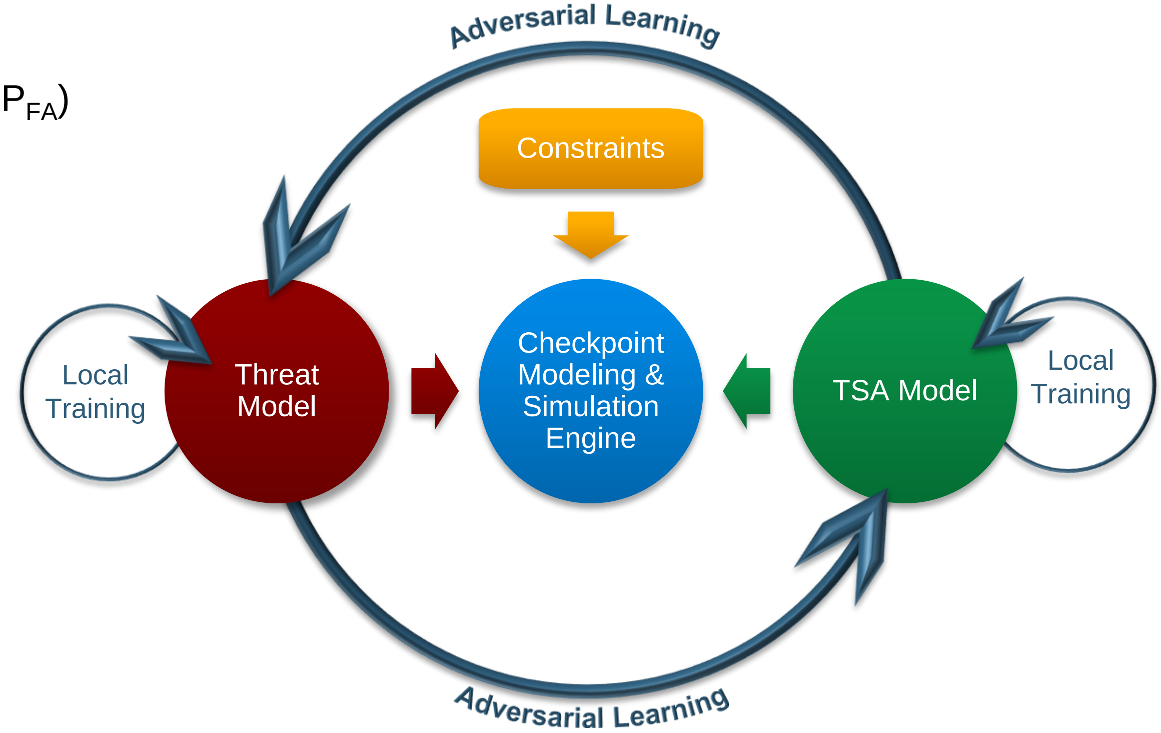
Introducing a New Framework for Flexible and Reproducible Reinforcement Learning Research

Monday, August 27, 2018

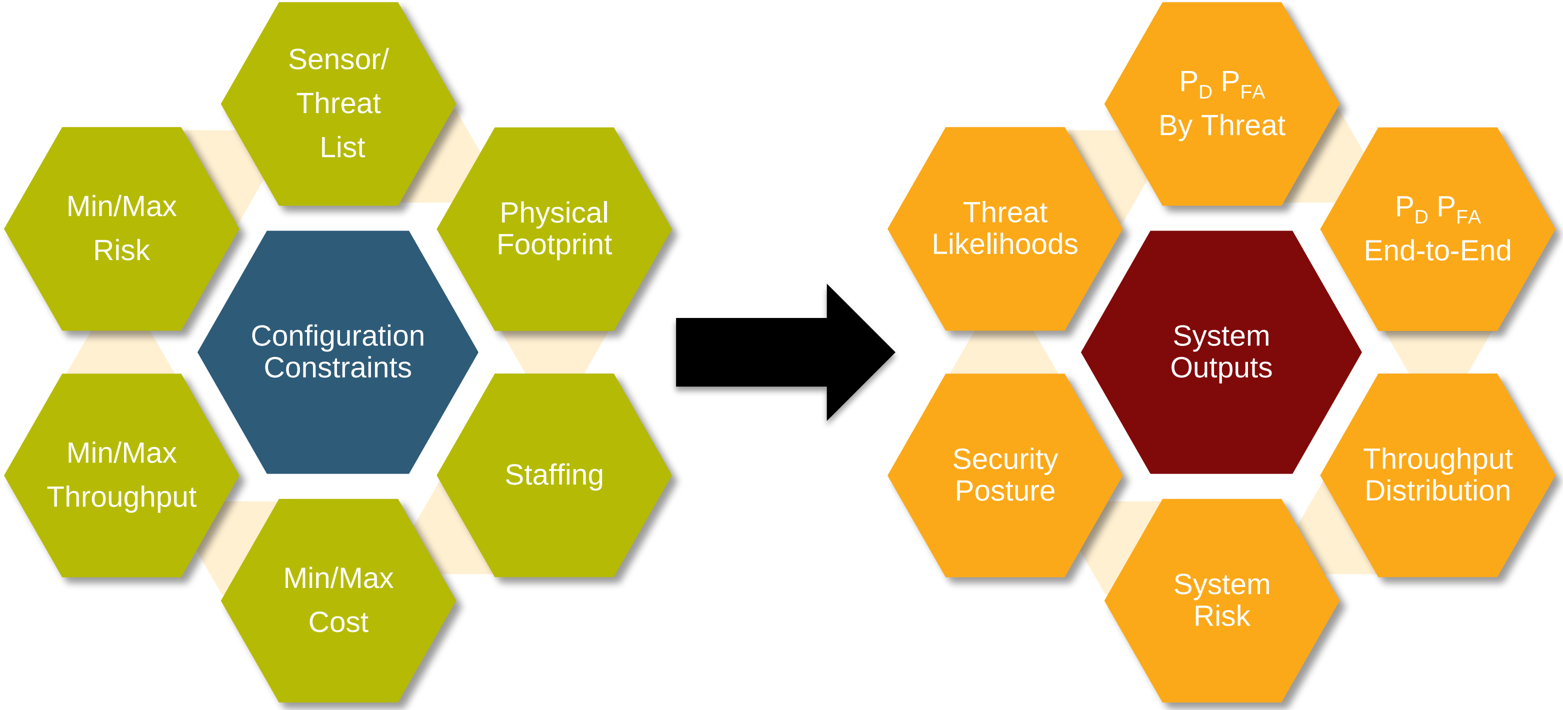
Google Open Sourced their Reinforcement Learning Framework – August 2018

Aviation Security Model Structure

- Constraints (User Defined)
  - System performance (P_D, P_{FA})
  - Threat list
  - Physical Dimensions
  - Available Resources
- Adversary Model
  - Potential threat vectors
  - Has visibility into TSA Operations
- TSA Model
  - Equipment deployment
  - CONOPS



Potential Parameters

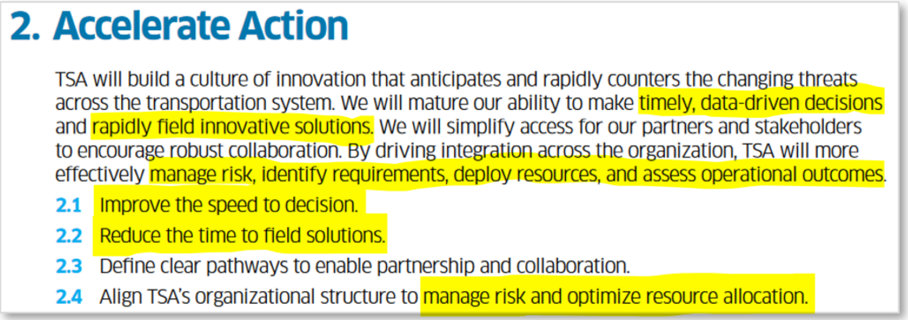


Users select which variables to fix/change to inform strategy

End Goals

- ✓ Initial results show success for a limited model – expect a fully functioning checkpoint model by fall
- ✓ Quantitatively informed requirements
- ✓ Understanding of budgetary tradeoffs
- ✓ Complementary perspective to subject matter experts
- ✓ Expanded confidence for long-term planning, understanding of threat displacement and effects of risk reduction
- ✓ Long term: integrate open algorithms and synthetic data generation, use like an adversarial network

Excerpt from TSA Strategy 2018-2026



2. Accelerate Action

TSA will build a culture of innovation that anticipates and rapidly counters the changing threats across the transportation system. We will mature our ability to make timely, data-driven decisions and rapidly field innovative solutions. We will simplify access for our partners and stakeholders to encourage robust collaboration. By driving integration across the organization, TSA will more effectively manage risk, identify requirements, deploy resources, and assess operational outcomes.

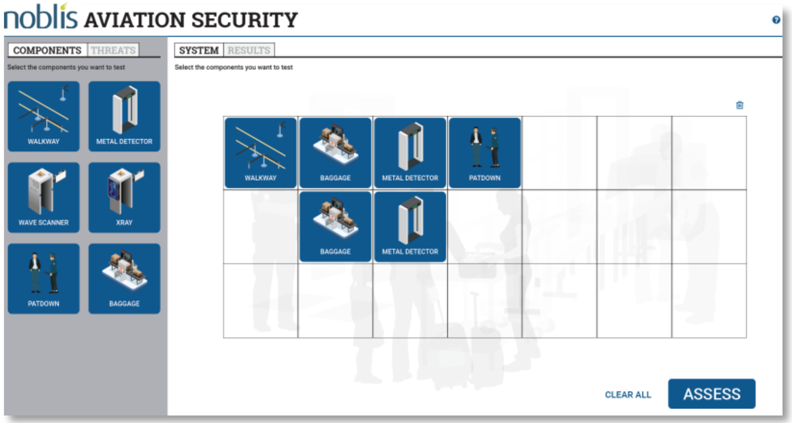
2.1 Improve the speed to decision.

2.2 Reduce the time to field solutions.

2.3 Define clear pathways to enable partnership and collaboration.

2.4 Align TSA's organizational structure to manage risk and optimize resource allocation.

Screenshot from Noblis Model



Select the components you want to test

Select the components you want to test

Questions?

noblis®

For the best of reasons

2019 WORLD'S MOST ETHICAL COMPANIES® ™

WWW.ETHISPHERE.COM