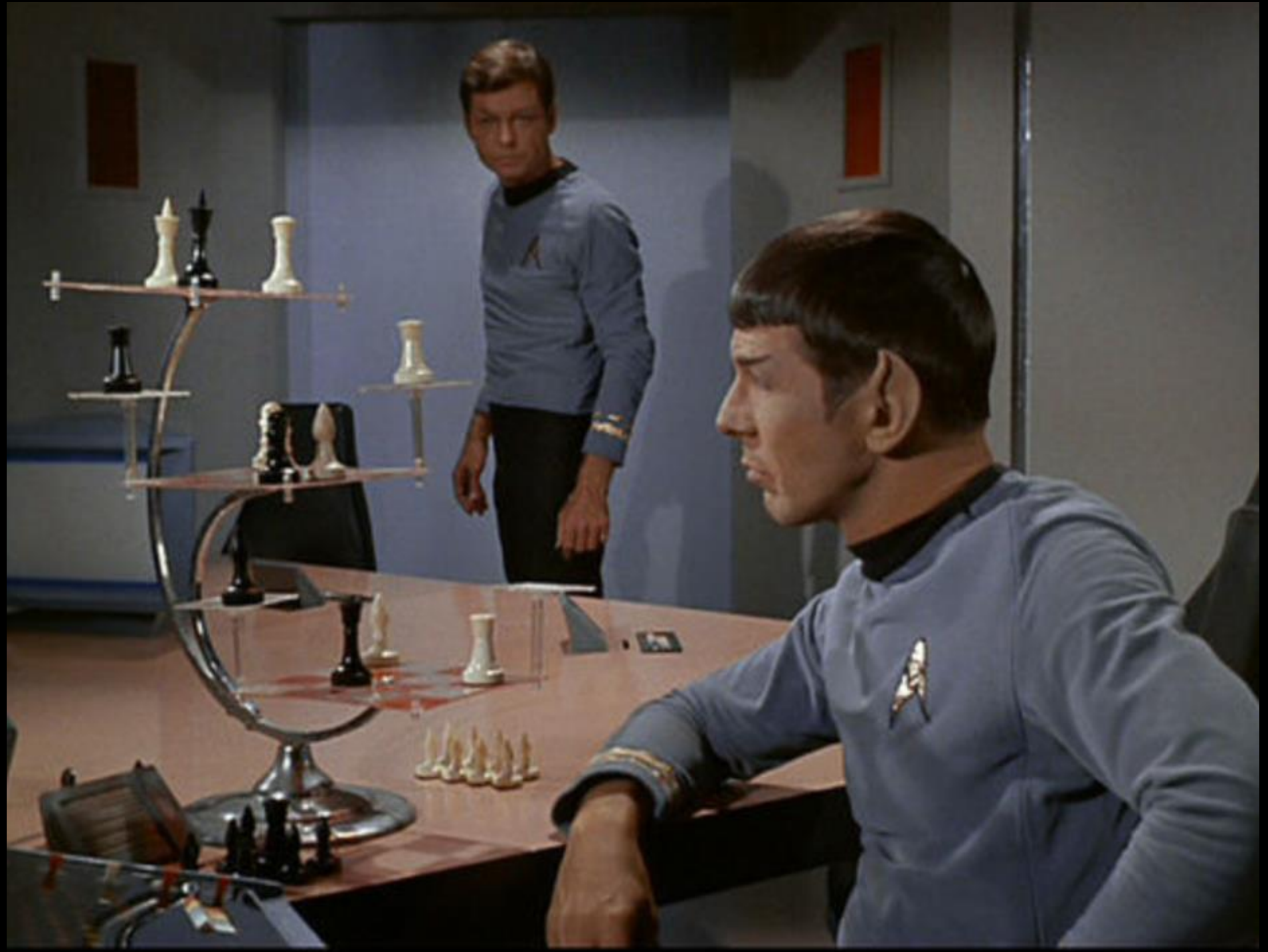
Threat Hunting or Threat Farming: Finding the Balance in Security Automation

Alex Pinto – Security Data Scientist – Verizon · @alexcpsec
Robert M. Lee – CEO / Founder – Dragos · @RobertMLee

Your Humble Speakers

- Alex Pinto
  - Capybara Enthusiast

- Rob M. Lee
  - Writes Comics



*"**Genius** is one percent **inspiration** and ninety-nine percent **perspiration**."*

Thomas A. Edison

Normalized Telemetry Repository

“Hypothesis Testing”

TTPs Repository (“Tactical Hypothesis”)

What does Good looks like?

Type I Error

Type II Error

```
return FALSE;
```

Hunting Automation Maturity Model (#HAMM)

- IOC Matching
- Signatures
- Anti-virus

- Security / Hunting Analytics
- Stats methods
- (Some) UEBA – maybe?

- Supervised machine learning with previous signals

- Rob [M|T] Lee
- David Bianco
- Probably not you

29:31 / 30:48

Pushing the Boundaries of Threat Hunting Automation - SANS Threat Hunting Summit 2017

https://www.youtube.com/watch?v=8gdtTiMt88w


ISRA
11
RoMeLo

GOOD IDEA

BAD IDEA

Lab (Stationary) Test

Physical road signs with adversarial perturbation under different conditions

Cropping, Resizing

Stop Sign → Speed Limit Sign

Field (Drive-By) Test

Video sequences taken under different driving speeds

Sample Per K Frames, Cropping, Resizing

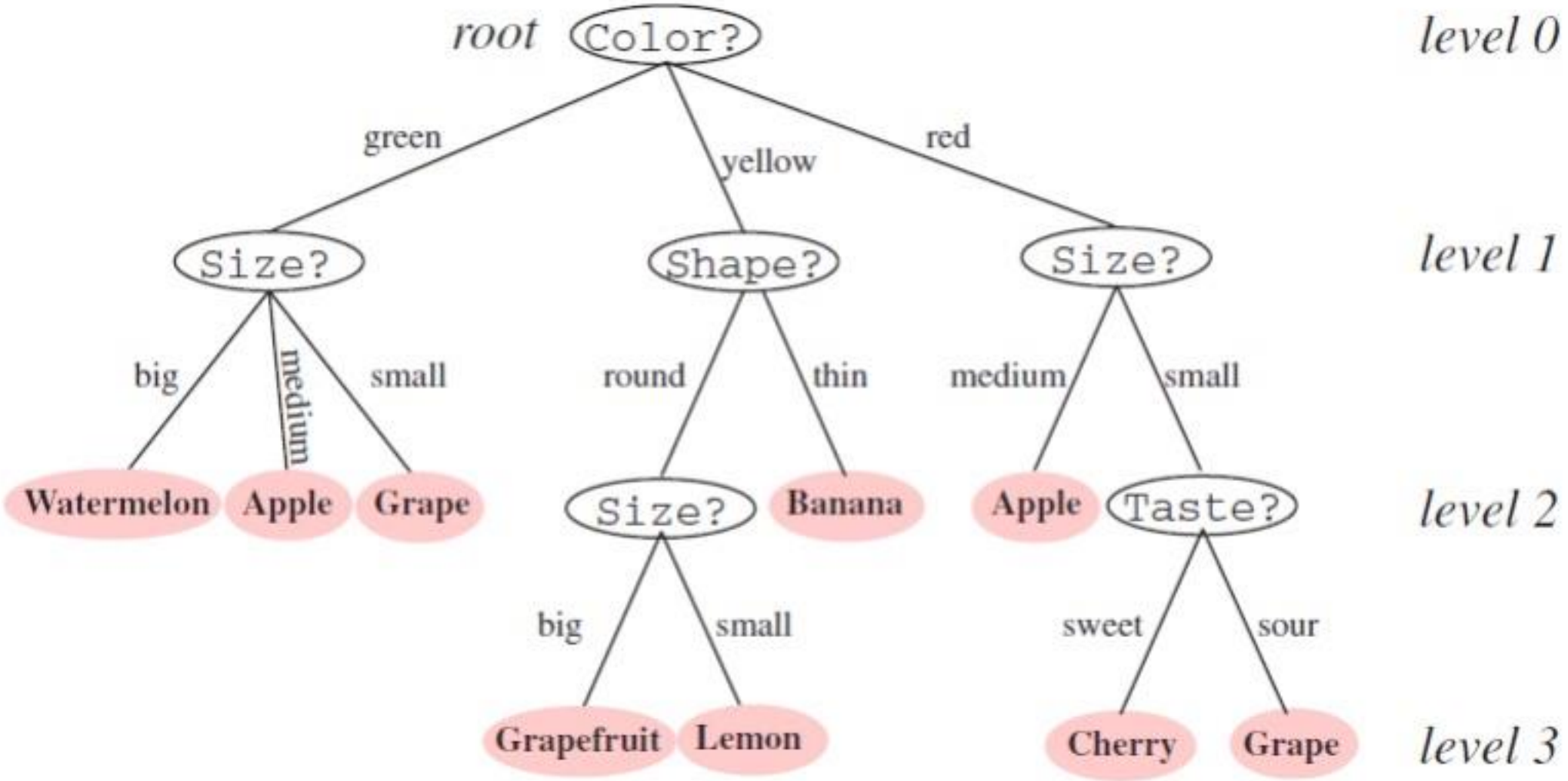
Stop Sign → Speed Limit Sign

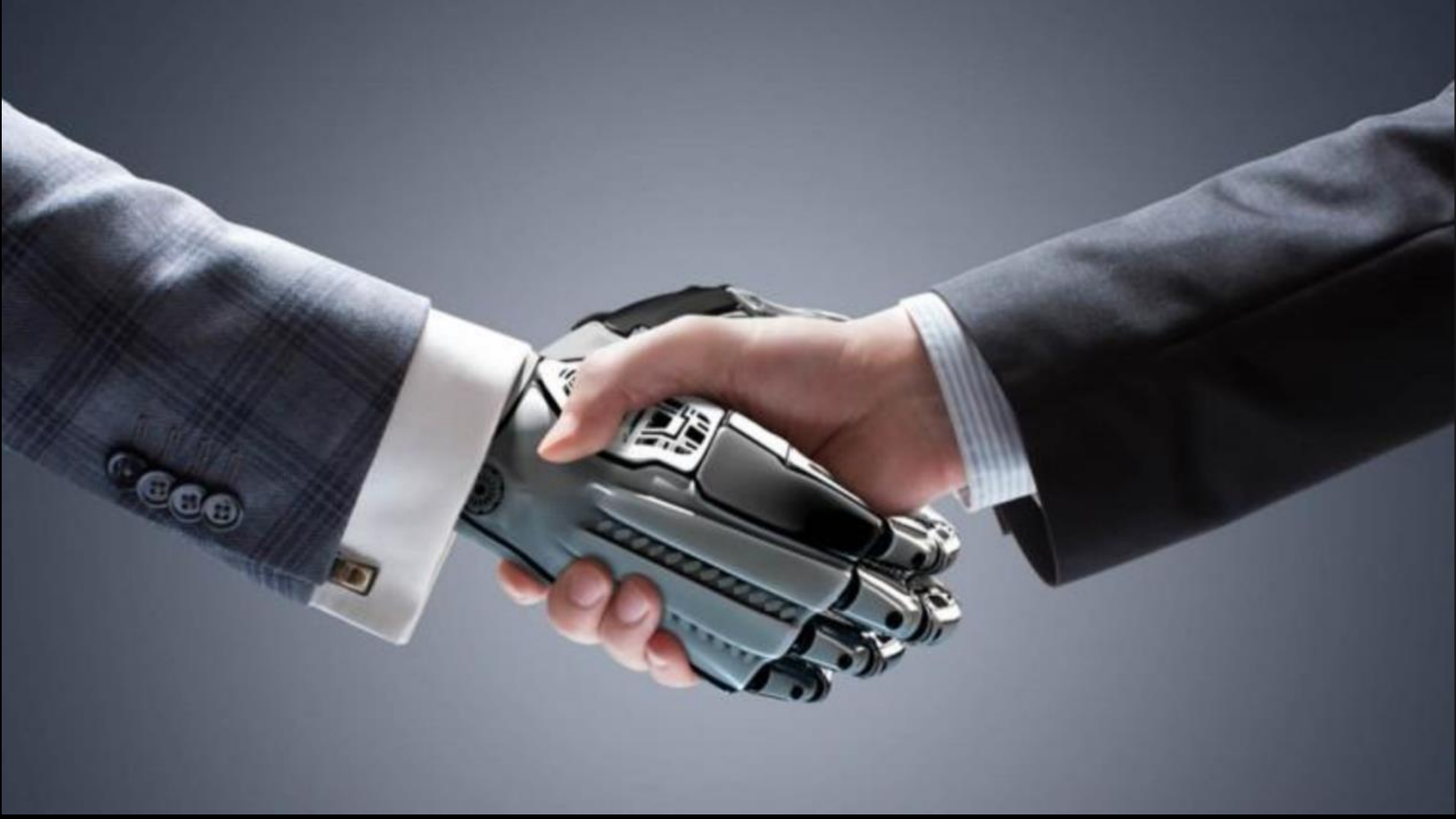
Song et al. - Robust Physical-World Attacks on Deep Learning Models: https://arxiv.org/pdf/1707.08945.pdf

Accurate Hunting Leads Vetter by Human Analysts

Hypothesis GENERATION

TTPs Repository (“Tactical Hypothesis”)


root
Color?
level 0
green
yellow
red
Size?
Shape?
Size?
level 1
big
medium
small
round
thin
medium
small
Watermelon
Apple
Grape
Size?
Banana
Apple
Taste?
level 2
big
small
sweet
sour
Grapefruit
Lemon
Cherry
Grape
level 3



Alex Pinto
alex.pinto@verizon.com
@alexcpsec

Robert M. Lee
rlee@dragos.com
@RobertMLee