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

You’re pregnant!

Type II Error

You’re not pregnant!
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

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

https://www.youtube.com/watch?v=8gdtTiMt88w
GOOD
BAD
IDEA
IDEA
Accurate Hunting Leads Vetter by Human Analysts

Hypothesis Generation

TTPs Repository ("Tactical Hypothesis")
A decision tree is shown with the following levels:

**Level 0**
- Root node: Color?
  - Green
  - Yellow
  - Red

**Level 1**
- Size?
  - Big
  - Medium
  - Small
- Shape?
  - Round
  - Thin
  - Medium
  - Small
- Size?
  - Big
  - Small

**Level 2**
- Watermelon
- Apple
- Grape
- Banana
- Apple
- Taste?
  - Sweet
  - Sour
  - Cherry
  - Grape

**Level 3**
- Grapefruit
- Lemon
- Cherry
- Grape
Alex Pinto
alex.pinto@verizon.com
@alexcpssec

Robert M. Lee
rlee@dragos.com
@RobertMLee