SECTOR 2018

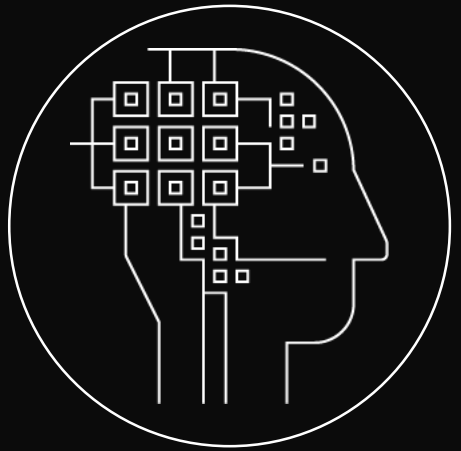
THE REAL DEAL ABOUT AI

Josh Fu
Principal Security Engineer

Select all squares with street signs.

AGENDA

- Industry Challenges
- Why AI Tech
- Demo
- Q&A



CYLANCE™

INDUSTRY CHALLENGES

INDUSTRY CHALLENGES

Areas AI Solves

- Zero Day Malware
- Fileless Attacks
- Management
- Scalability
- Old Operating Systems
- VDI
- Online Requirements
- And More

WHAT WE DO

RELY ON AI AND ML

ANALYZE MALWARE AT THE DNA LEVEL

PREDICT AND PREVENT

BLOCK EXPLOITS AND SCRIPTS

ROOT CAUSE ANALYSIS

THREAT HUNTING AND VISIBILITY

WHAT WE DON'T DO

SIGNATURES

RELY ON HUMAN GENERATED RULES

ALLOW THREATS TO EXECUTE

WHITELISTING

BEHAVIORAL ANALYSIS

SANDBOXING OR ISOLATION

CONSTANT UPDATING

REQUIRE ON-PREM INFRASTRUCTURE

CREATE NOISE

CYLANCE™

WHY ARTIFICIAL INTELLIGENCE TECH

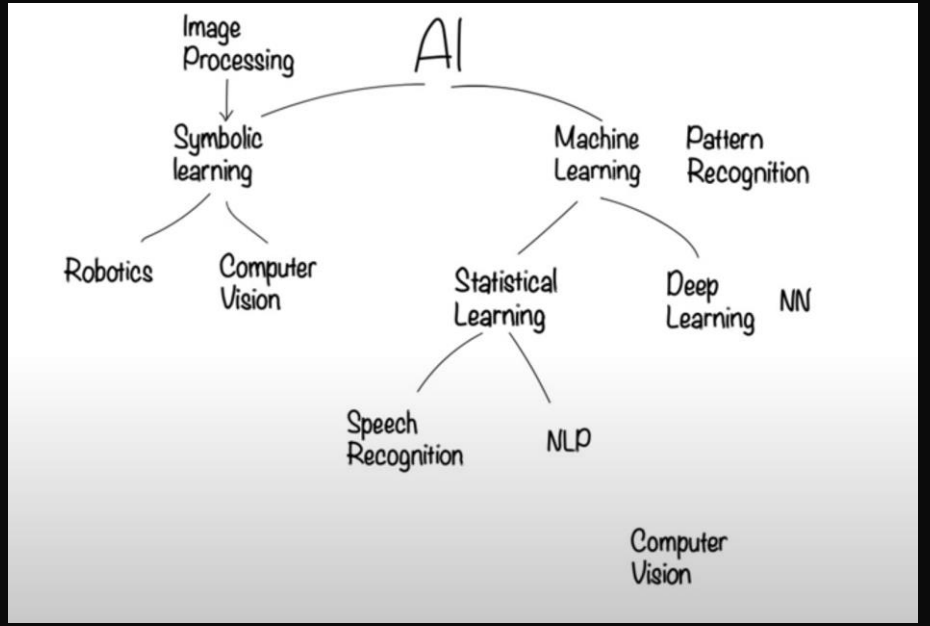
HIGHLY USEFUL

- Aviation - Air Operations Division for combat training and tactical decision making
- Social issues - USC Center for AI in Society to address homelessness
- Finance – Wall Street
- Education – SHERLOCK intelligent tutoring systems
- Healthcare – Concept Processing in EMR software
- Agriculture – PEAT for detecting pests and soil defects at over 95% accuracy rate
- Technology – Programming, toys, transportation, and more
- Cybersecurity – The signature approach is no longer the most effective strategy

WHAT IS AI?

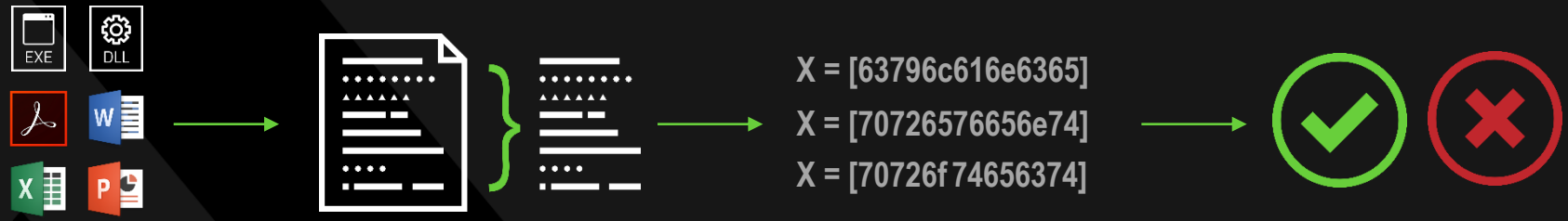
Artificial Intelligence vs. Machine Learning

- 1950 | Alan Turing
- 90% | 2 years
- Artificial Intelligence
  - Making Smart Machines
  - Symbolic Learning
  - Generalized vs Narrow Intelligence
- Machine Learning
  - A branch of AI
  - Advanced Computational Statistics
  - Used for narrow problems
    - Optimization, Analysis, Prediction



* Source: Raj Ramesh https://youtu.be/2ePf9rue1Ao

HOW? ALGORITHMIC SCIENCE AND MACHINE LEARNING



COLLECT (GOOD AND BAD)

EXTRACT FEATURES

TRAIN MODELS

Algorithm

CYLANCE™

GENERATIONS OF AI

Gen	Runtime	Features & datasets	Human interactions	Robustness
1st	Cloud training Cloud prediction	Small (<1000) number of features. Human hand-picked. Small number of samples (<1M). Human labeled.	Easily interpretable (small)	Trivial. Bypass in minutes.
2nd	1st gen + Local prediction	Medium (<100k) number of features. Human hand picked. Medium (<100M) number of samples. Mostly human labels with some heuristic labels.	Large uninterpretable Human association indicators (TTM)	Easy. Bypass in hours.
3rd	2nd gen + Cloud enhanced models	Large (<3M) number of features. Mostly heuristic labels with some human labels. Large (1B+) number of samples. Mostly heuristics with some human labels.	Some interpretability w/ accurate visualization.	Moderate. Bypass in days.
4th	3rd gen + Local training	Active learning, feature suggestions.	Human feedback into model building.	Difficult. Bypass in weeks.
5th	4th gen + unsupervised local training	Semi-supervised feature discovery and data collection.	Human feedback optional; model provides interpretable insights	Extremely Difficult. Bypass in months.

WHY COMPANIES CHOOSE OUR AI

Effectiveness

- 14.5 million endpoints protected
- Very low false positive rate
- Malware executables
- Fileless & memory malware
- Advanced persistent threats
- Zero days attacks

Simplicity

- Replaces traditional AV
- Remove unnecessary layers
- Reduce help desk calls and system re-imaging
- Stop emergency patching

Performance

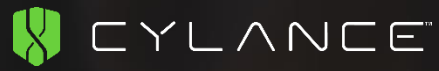
- Lightweight agent
- User systems run faster
- Extends hardware lifespan
- Network bandwidth reduction

EXAMPLES OF PREDICTIVE PREVENTION

CylancePROTECT detects and PREVENTS attacks months before they are seen “in the wild”

- 3400 active subscription customers
- Millions & millions of threats prevented
- More than 1.4 million threat features recognized by our models
- Our predictive model is able to detect and prevent malware on average **25 months before** it is found in the real world

Demo



STATISTICS FOR THOUGHT

CYBERSECURITY SUPPORTS THE BUSINESS

- Lowers company risk
- Due diligence
- Mergers and acquisitions

ABOUT US

Corporate Snapshot

- Founded in 2012 by Stuart McClure and Ryan Permeh
- SANS Award - Best Endpoint Protection 2016
- “Fastest-growing EPP startup in the past ten years” - Gartner 2016
- Named CNBC Disruptor 50 List 2016 (#40) and 2017 (#9)
- Forbes Cloud 100 List (#23)
- Inc. Magazine “Top 15 Company” (#2) 2017

Data Science Investment

- 17 Data Scientists | 34 total degrees | 10 PhDs
- **Fortune Top 10 in A.I. Investment** (behind Amazon, Google, Microsoft, Facebook, NVIDIA, GE
- Numerous Patents
  - AI/ML
  - Security
  - Forensics

CYLANCE™

QUESTIONS AND ANSWERS

REFERENCES AND RECOMMENDED READING

- Cylance AI platform – www.cylance.com
- The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage
- Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It
- Verizon Report for 2017 - http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
- NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million - https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#4c5703e04f9a
- Mergermarket M&A Trends Report Q1 2017 https://www.mergermarket.com/info/ma?page=33
- AV-TEST Statistics - AV-TEST statistics https://www.av-test.org/en/statistics/malware/
- Best Machine Learning Resources for Starters - https://machinelearningmastery.com/best-machine-learning-resources-for-getting-started/
- Ransomware: Past, Present, and Future - http://blog.talosintelligence.com/2016/04/ransomware.html
- A visual introduction to machine learning - http://www.r2d3.us/visual-intro-to-machine-learning-part-1/
- DEMYSTIFYING MACHINE LEARNING - https://www.infoworld.com/article/3068540/data-analytics/machine-learning-demystifying-linear-regression-and-feature-selection.html
- The wonderful and terrifying implications of computers that can learn - https://www.ted.com/talks/jeremy_howard_the_wonderful_and_terrifying_implications_of_computers_that_can_learn?language=en
- Deep Learning on GPU Clusters - https://www.youtube.com/watch?v=brui4N2orII
- USENIX Enigma 2016 - NSA TAO Chief on Disrupting Nation State Hackers - https://www.youtube.com/watch?v=bDJb8WOJYdA

THANK YOU

Josh Fu
cylance.com
Twitter: @cylanceinc and
@jfusecurity
jfu@cylance.com