Panagiotis Kalantzis

Cyber Security & Data Privacy Expert, CISO, vCISO, Cyber Security Strategist & Board Advisor

April 2023

Cyber Security in the Age of Artificial Intelligence (AI)

How AI will make our world more vulnerable or secure

Agenda

01 **What is AI**
Introduction to History of Artificial Intelligence and Definitions

02 **AI in Cyber Security**
What are the Contributions of AI to Cyber Security Market

03 **AI Challenges**
What Challenges does AI bring to the Cybersecurity World

04 **AI Benefits & Key Takeaways**
What Benefits does AI bring to Cybersecurity

Artificial Intelligence:
Do anything a human would do

AI is Statistics

Careful of the Hype

- Cloud, Blockchain, and now AI ?
- “Cool” products have to have AI

“Everyone calls their stuff ‘machine learning’ or

even better ‘artificial intelligence’

- It’s not cool to use statistics!”

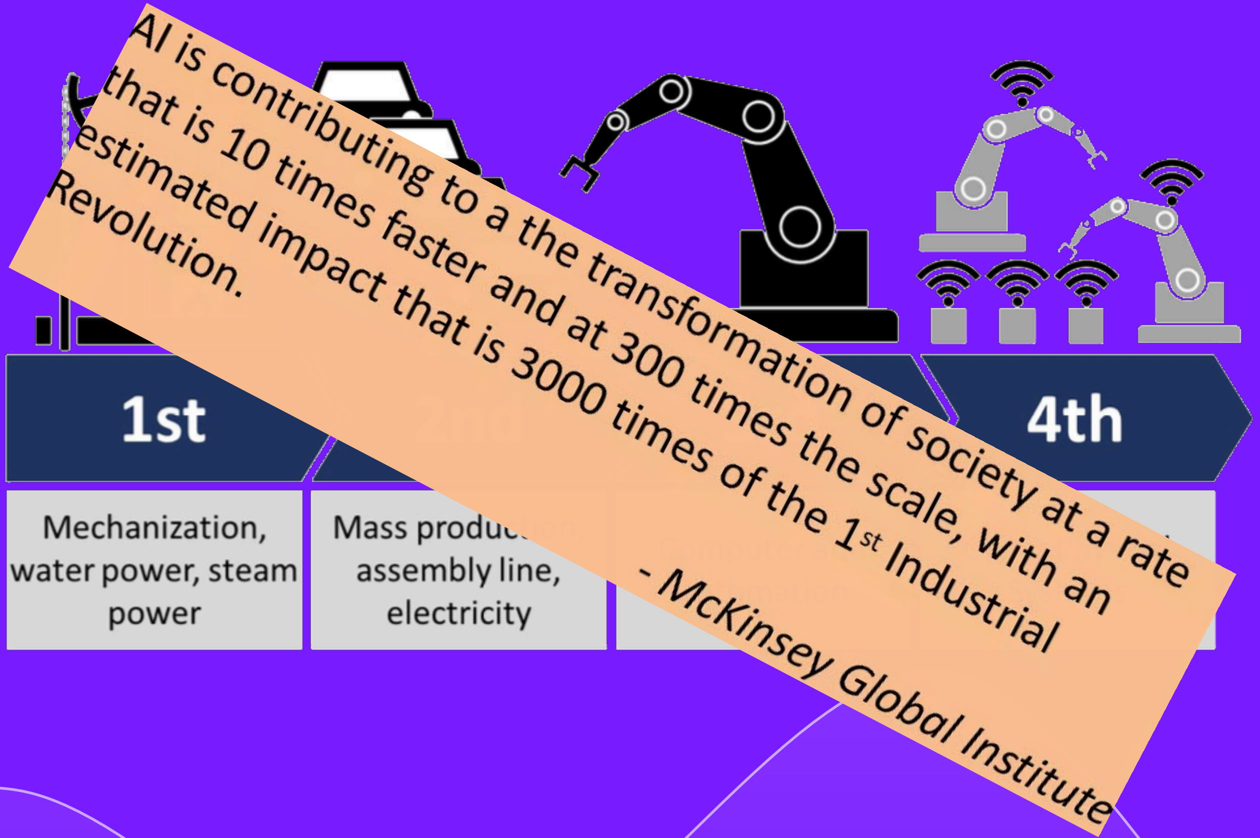
AI & ML leads to Industry 4.0

Industry 4.0 enabled by IoT, Big Data and AI

- IoT is the intelligent sensor
- Big Data will enable processing huge volumes of data
- AI will make sense of the data in decision making

AI helps transform raw data into power - AI will transform businesses for sure

Primarily Machine Learning and then the deeper aspects with Deep Learning

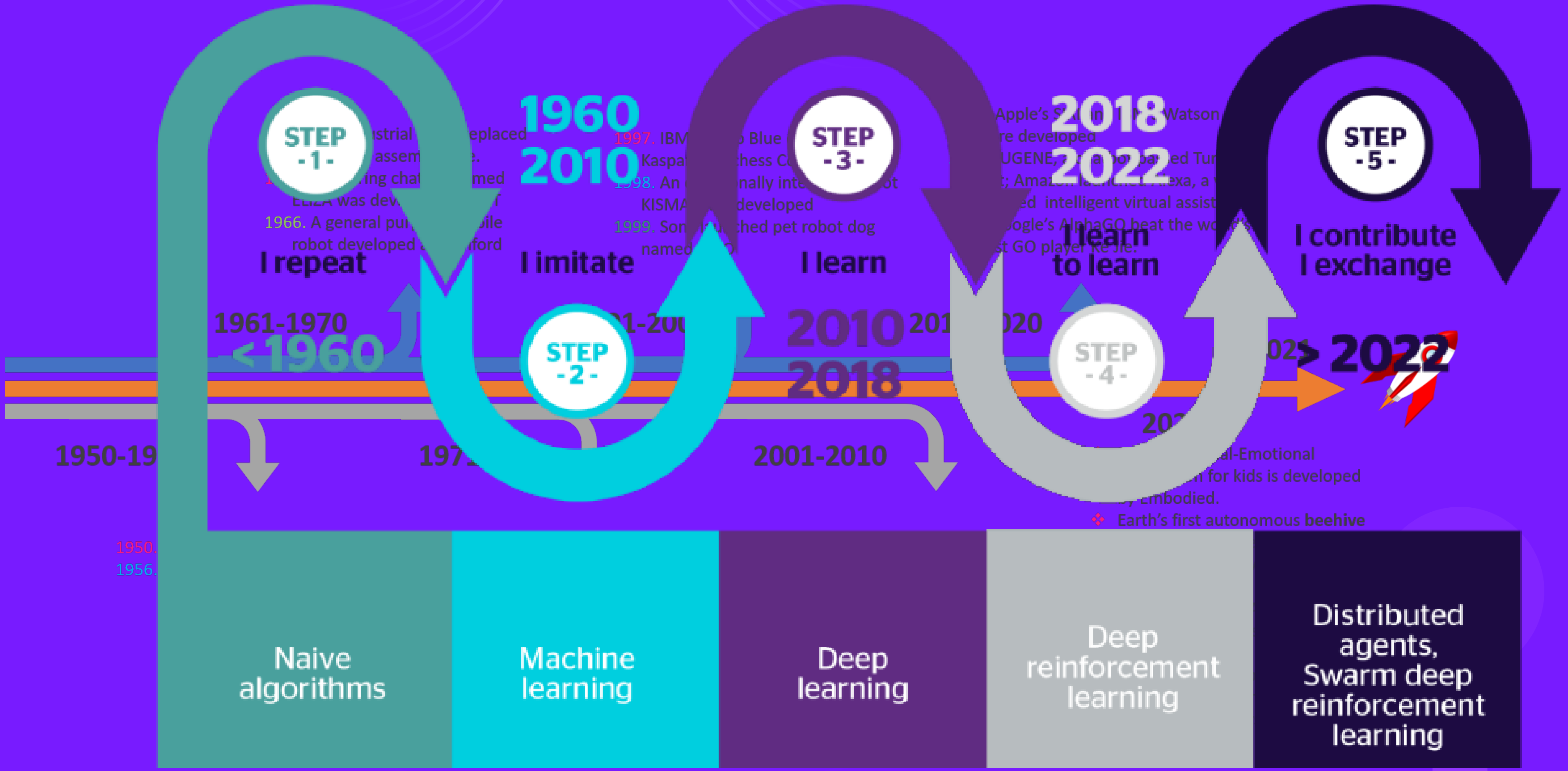

1st
4th
Mechanization, water power, steam power
Mass produc
assembly line, electricity

AI is contributing to a the transformation of society at a rate that is 10 times faster and at 300 times the scale, with an estimated impact that is 3000 times of the 1st Industrial Revolution.

- McKinsey Global Institute

AI is the bedrock on which Industry 4.0 relies on

Artificial Intelligence is not new



STEP -1-

I repeat

STEP -2-

I imitate

STEP -3-

I learn

STEP -4-

I learn to learn

STEP -5-

I contribute
I exchange

<1960

1960
2010

2010
2018

2018
2022

> 2022

1950-19

1961-1970

197

2001-2010

1966. A general pu

1999. Son hed pet robot dog

Earth's first autonomous beehive

Naive algorithms

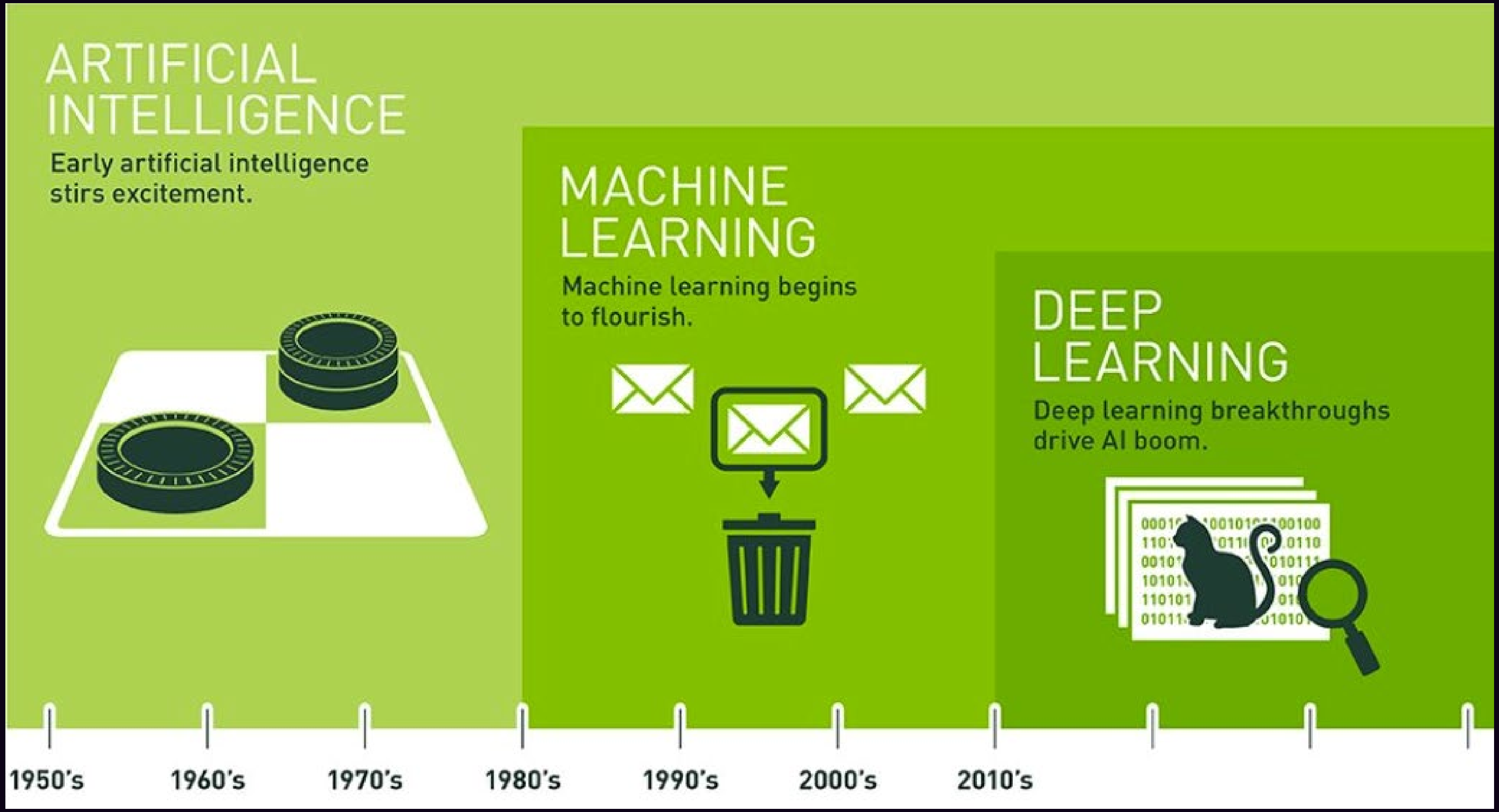
Machine learning

Deep learning

Deep reinforcement learning

Distributed agents, Swarm deep reinforcement learning

Evolution of AI – The AI Umbrella


ARTIFICIAL INTELLIGENCE
Early artificial intelligence stirs excitement.
MACHINE LEARNING
Machine learning begins to flourish.
DEEP LEARNING
Deep learning breakthroughs drive AI boom.
1950's
1960's
1970's
1980's
1990's
2000's
2010's

Evolution towards intelligent defenses

	1980s	1990s	2010	2016 +
Computing & Data Paradigm	Local computing environment	Networked computing environment	Big data and batch processing	Ubiquitous data streaming
Detection Paradigm	Rule based detection	Rule & Heuristic detection	Rule, Heuristics and ML	Deep Learning, ML and **[...]**

More scalability and adaptability is required !

Cyber Defence/Monitoring/Analytics is still in the 1999

- Firewalls – policy management, auditing a challenge
- IDS/IPS – false positives
- Threat Intelligence – realy the same as IDS signatures
- DLP – just an IDS engine
- Vulnerability Scanners – old user interfaces, cluttered results
- SIEM – still same issues (parsing, context prioritizatiion)
- Security Analytics – what additional can they offer to SIEM

Cyber Security has ~~not~~ Changed since 1999

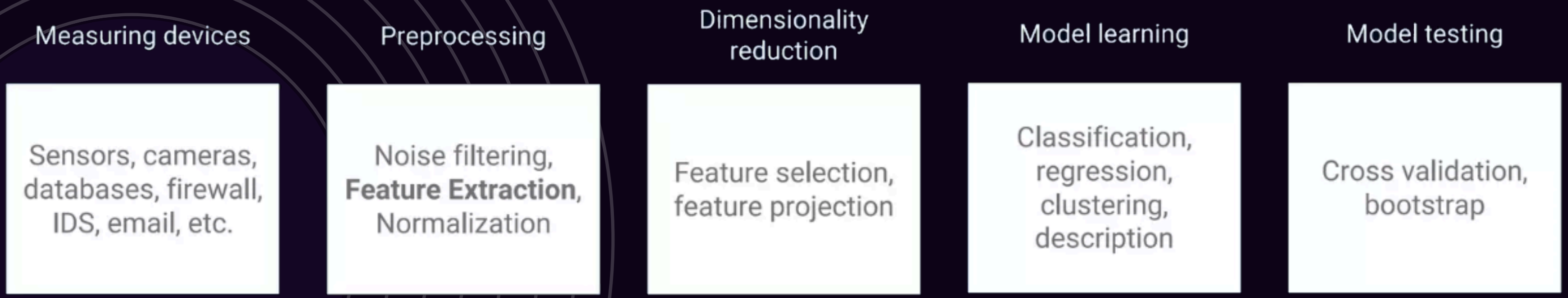
Artificial Intelligence in Cyber Security Tools

Orchestrate and **Automate** tasks that humans can perform without a problem to a much larger volume we could ever handle

Process and **structure** huge volumes of data including analysis of the complex relationships within it

Cybersecurity use case
sifting **through events**, **correlating them with other events**, and presenting analytics **for** a human analyst to determine the next actions

Machine Learning Process & Types



Measuring devices

Sensors, cameras, databases, firewall, IDS, email, etc.

Preprocessing

Noise filtering, **Feature Extraction**, Normalization

Dimensionality reduction

Feature selection, feature projection

Model learning

Classification, regression, clustering, description

Model testing

Cross validation, bootstrap

Supervised

vs

Unsupervised

Target / outcome is known

classification – regression

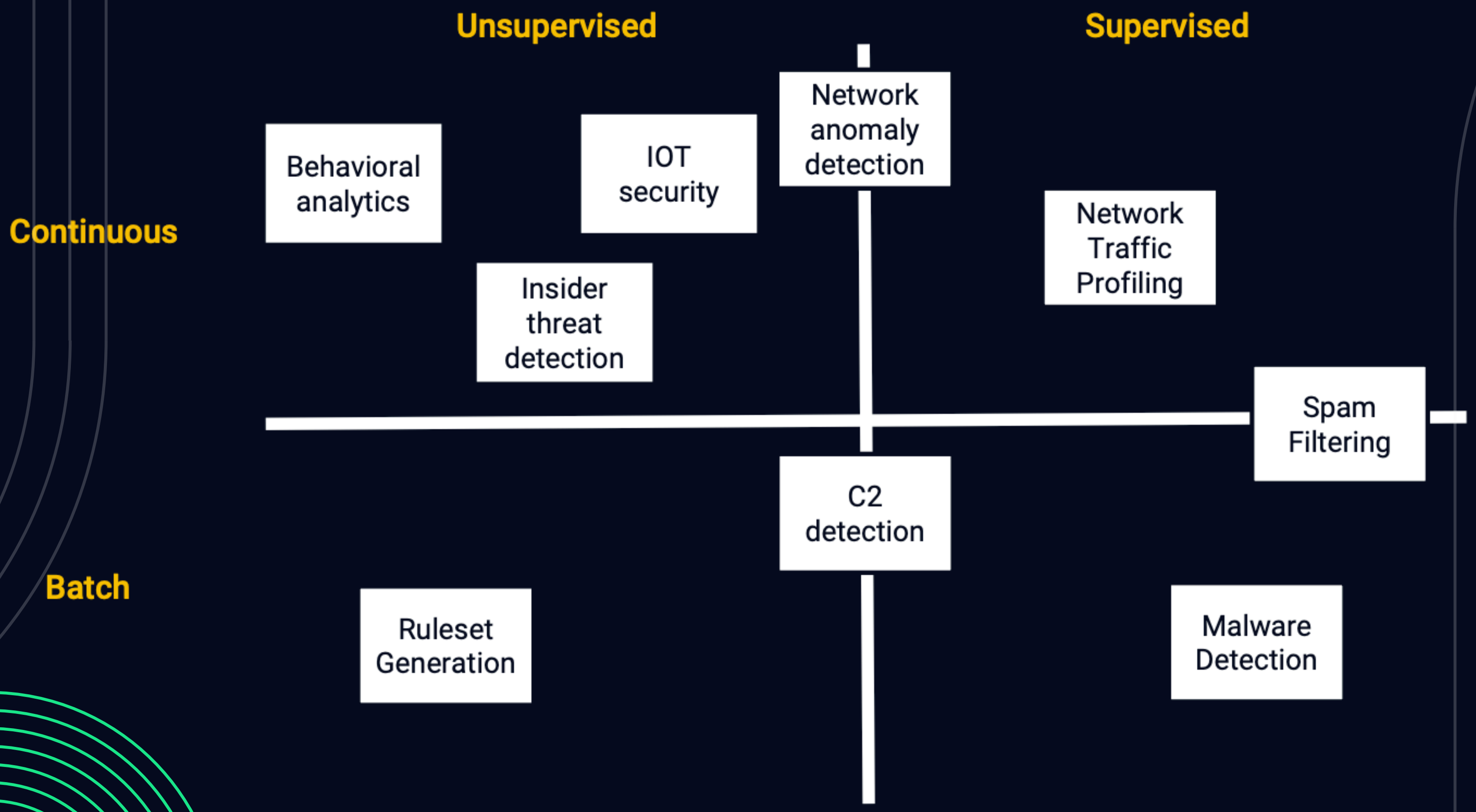
probability distribution in statistics, P(X/Y)

Target / outcome is unknown

clustering – decomposition

density estimation in statistics, P(X,Y)

Applying ML to Security Domains



Unsupervised

Supervised

Continuous

Batch

Behavioral analytics

IOT security

Network anomaly detection

Network Traffic Profiling

Insider threat detection

Spam Filtering

C2 detection

Ruleset Generation

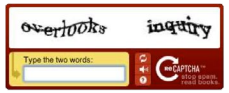
Malware Detection

Today’s Attacks based on AI

Malware creation
- Speed
- Enhance evasive capability

Smart Botnets
- Self learning
- Smarter Zombies

Advanced Phishing
- Smart Social Enginnering
- More Convincing Spams

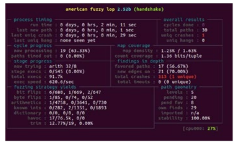


Fighting CAPTCHA

Adversarial AI
- Discover and poise ML
- Poise datasets

Conditional Attacks
- Cyberattacks using blockchain based smart contracts

Classify Victims
- Optimise ROI of attacks



Advanced Fuzzing

Adversarial unputs
- Artifacts designed to fool Defensive AI

Data Poisoning
- Poisoning training data to CS Tools

Model Stealing
- Enhance abilities of Adversarial inputs

Feedback Weaponization
- Poison ML to DoS ML Users

WARNING
ALGORITHMS ARE DANGEROUS

What makes Algorithms Dangerous

Algorithms makes assumption about data

- Assume ‘clean’ data (src/dst confusion, user feedback, etc.)
- Assume a certain type of data and its distribution
- Generally, don’t deal with outliers
- Need contextual features (e.g., not just IP addresses)
- Assume all input features are ‘normalized’ the same way

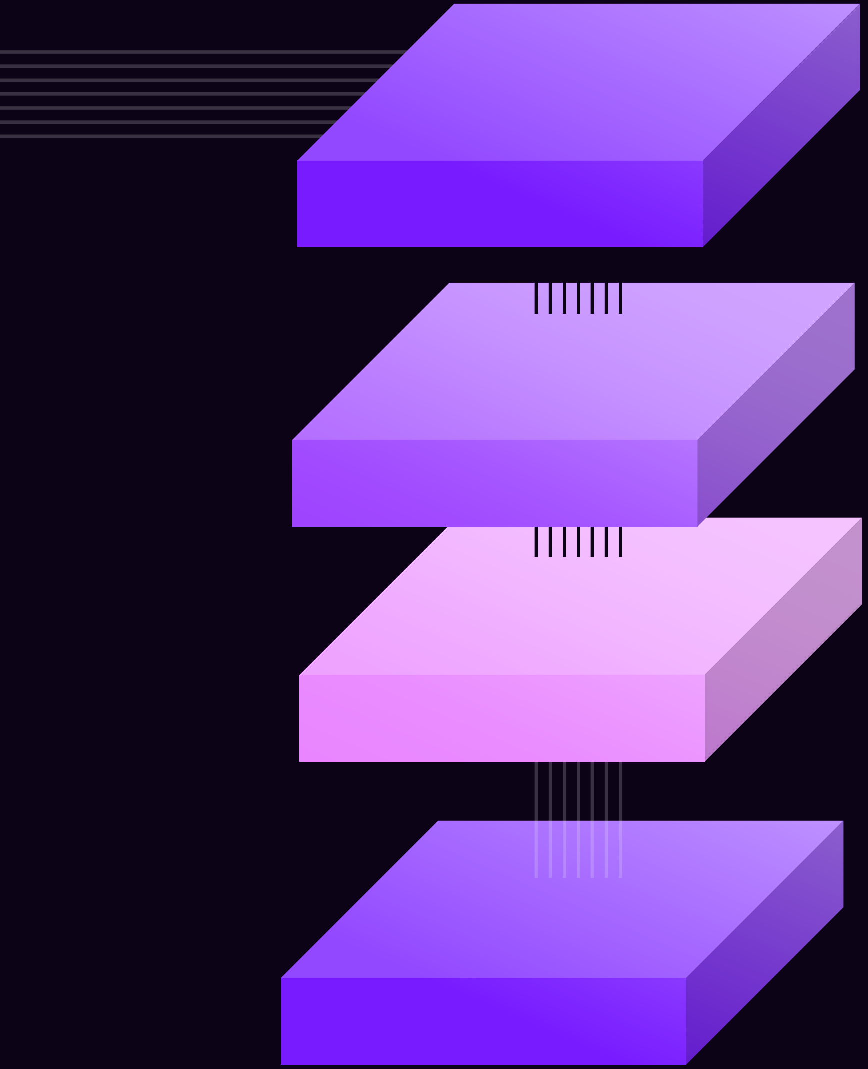
Algorithms are too easy to use these days

- The process is more important than the algorithm (e.g., feature engineering, supervision, drop outs, parameter choices, etc.)

Algorithms do not include domain knowledge

- Defining meaningful and representative distance functions, for example

Algorithmic Biases



Pre-existing
Pre-existing bias in an algorithm is a consequence of underlying social and institutional ideologies.

Unanticipated uses
Emergent bias can occur when an algorithm is used by unanticipated audiences.

Correlations
Unpredictable correlations can emerge when large data sets are compared to each other.

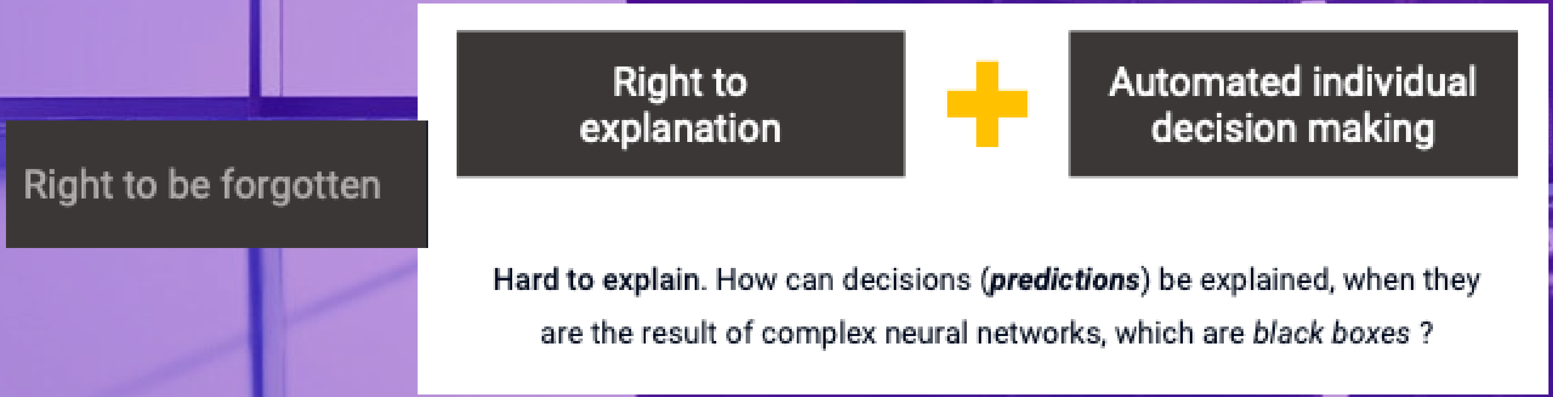
Feedback Loops
Emergent bias may also create a feedback loop, or recursion, if data collected for an algorithm results in real-world responses which are fed back into the algorithm.

Technical
Technical bias emerges through limitations of a program, computational power, its design, or other constraint on the system.

Emergent
Emergent bias is the result of the use and reliance on algorithms across new or unanticipated contexts.

Regulatory Implications

GDPR: When laws clash with machine learning



Right to be forgotten

Right to explanation + Automated individual decision making

Hard to explain. How can decisions (***predictions***) be explained, when they are the result of complex neural networks, which are *black boxes* ?

Tomorrow attacks may be AI driven

Genetic Algorithms (GA) to find best malware fitness for maximum damage

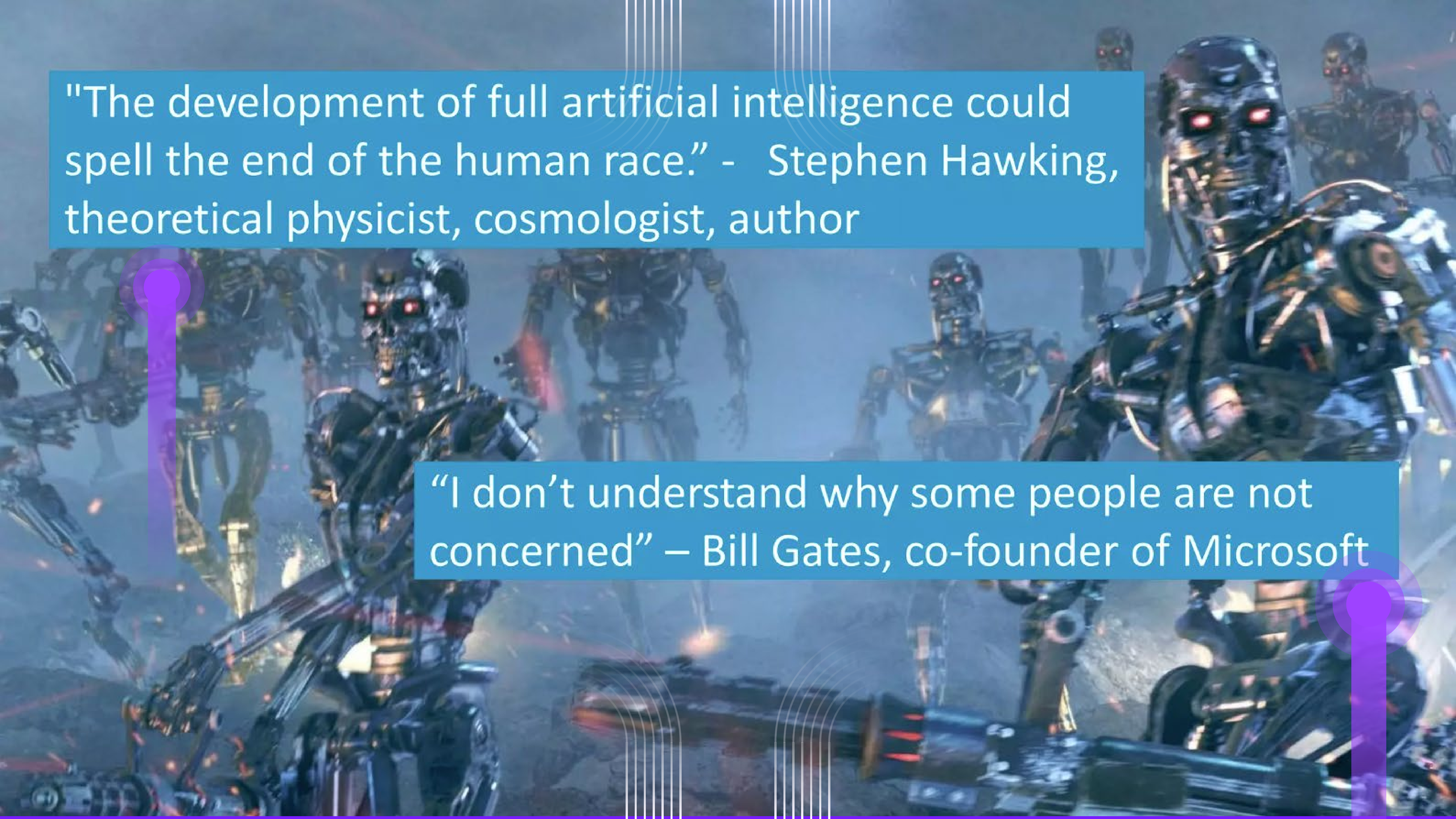
Self Organizing Maps (SOM) to remove centralized C&C structures

RNNs perform Mimicry Attacks to bypass AI driven behavioral detections

Deep Fuzzing that automatically finds complex vulnerabilities

Use *game theory principles* to define target outcome ***T***, and use machine learning techniques to maximize the AUC (“Area Under ROC Curve”)

A.I. are better, faster and more intelligent to engage in adversarial activities, including *warfare*



"The development of full artificial intelligence could spell the end of the human race.” - Stephen Hawking, theoretical physicist, cosmologist, author

“I don’t understand why some people are not concerned” – Bill Gates, co-founder of Microsoft

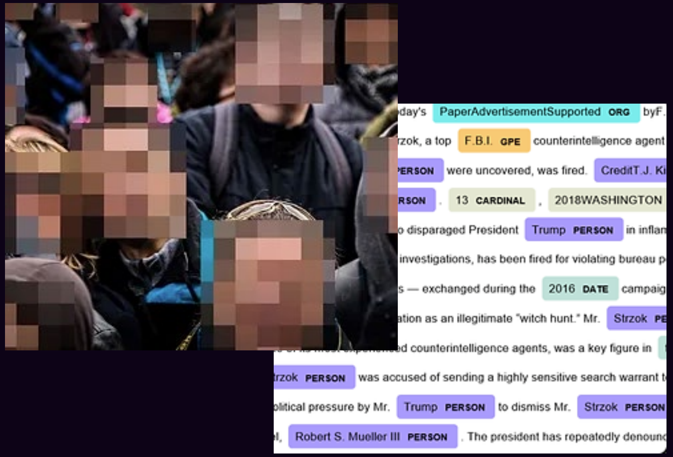
Benefits on Tools based on AI

AI has begun to touch all aspects of cybersecurity

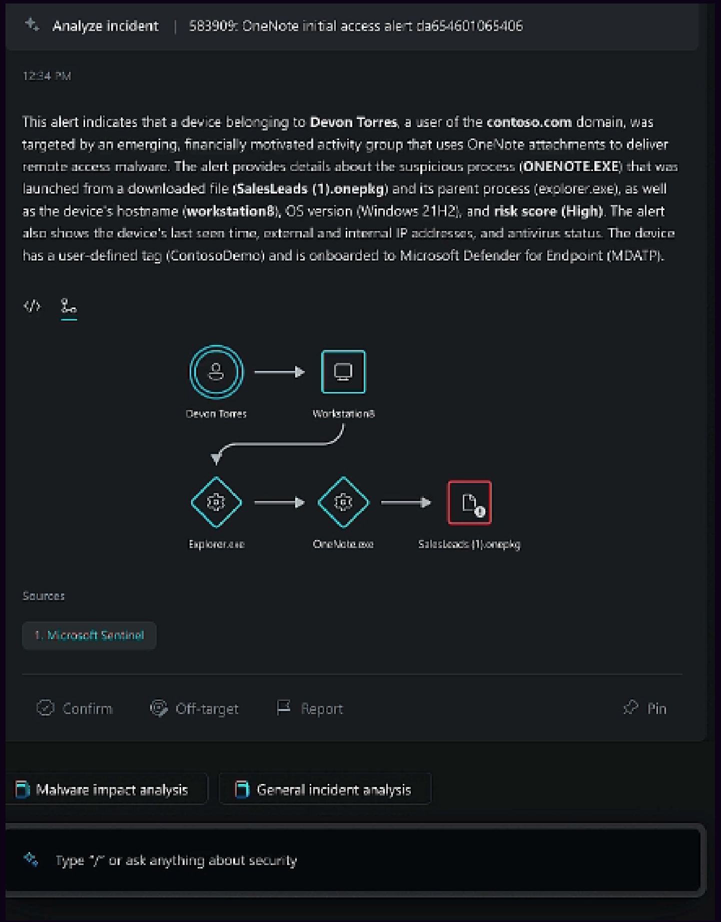
Areas influenced:

- Malware Detection
- Intrusion Detection / Prevention
- Antispam
- Vulnerability Management
- Social engineering
- Data Classification
- Threat Intelligence
- Penetration testing
- Data security

New tools are arising Generative AI & LLM



day's PaperAdvertisementSupported ORG byF.
rzok, a top F.B.I. GPE counterintelligence agent
ERSON were uncovered, was fired. CreditT.J. Ki
RSON . 13 CARDINAL . 2018WASHINGTON
o disparaged President Trump PERSON in inflan
investigations, has been fired for violating bureau p
s — exchanged during the 2016 DATE campaig
ation as an illegitimate "witch hunt." Mr. Strzok PE
d counterintelligence agents, was a key figure in
rzok PERSON was accused of sending a highly sensitive search warrant t
olitical pressure by Mr. Trump PERSON to dismiss Mr. Strzok PERSON
l, Robert S. Mueller III PERSON . The president has repeatedly denounc



Analyze incident | 583909: OneNote initial access alert da654601065406

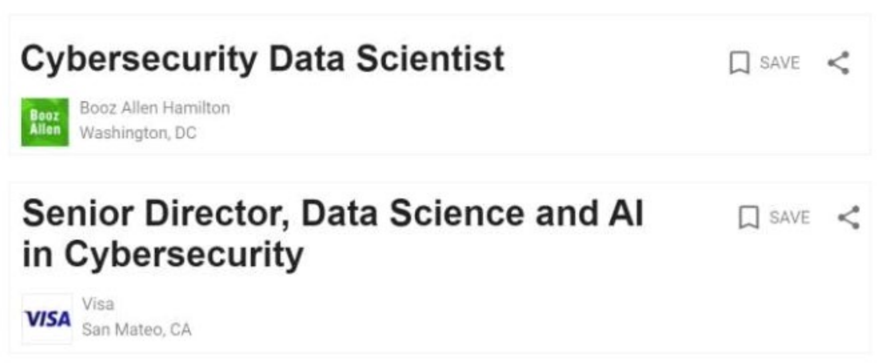
12:34 PM

This alert indicates that a device belonging to **Devon Torres**, a user of the **contoso.com** domain, was targeted by an emerging, financially motivated activity group that uses OneNote attachments to deliver remote access malware. The alert provides details about the suspicious process (**ONENOTE.EXE**) that was launched from a downloaded file (**SalesLeads (1).onepkg**) and its parent process (explorer.exe), as well as the device's hostname (**workstation8**), OS version (Windows 21H2), and **risk score (High)**. The alert also shows the device's last seen time, external and internal IP addresses, and antivirus status. The device has a user-defined tag (ContosoDemo) and is onboarded to Microsoft Defender for Endpoint (MDATP).

Sources

1. Microsoft Sentinel

Confirm
Off-target
Report
Pin
Malware impact analysis
General incident analysis
Type "/" or ask anything about security



Cybersecurity Data Scientist

Booz Allen Hamilton
Washington, DC

Senior Director, Data Science and AI in Cybersecurity

Visa
San Mateo, CA

Plenty of New Cyber Security Jobs

Key Takeaways

AI is pervasive and disruptive

AI has the capacity for good and evil

Effective use requires a paradigm swift to escape the cat/mouse game

- Reactive -> Proactive
- Detection -> Prevention and Automation
- Threat Intelligence -> Behavior Analysis of Human and Machines
- Event based -> Risk based

- Algorithms are getting smarter, but experts are more important
- The way algorithms are used is often dangerous. We need to hire experts
- The new world is here to stay, we need to embrace it

Thanks For Watching

Panagiotis Kalantzis
Cyber Security & Data Privacy Expert,
CISO, vCISO, Cyber Security Strategist &
Board Advisor

in linkedin.com/in/pkalantzis kalantzis.me ✉ pkalantzis@gmail.com