Machine Learning Use Cases in Cybersecurity

S.M. Avdoshin, Department of Software Engineering, National Research University Higher School of Economics

A.V. Lazarenko, N.I. Chichileva, P. A. Naumov, R&D Department, Group-IB

P. G. Klyucharev, Informatics and Control Systems, Bauman Moscow State Technical University

Content

- Machine Learning
- How to use ML in cyberattacks?
- How can we use ML to protect from cyberattacks?
- What are the problems?

Key part of evolution

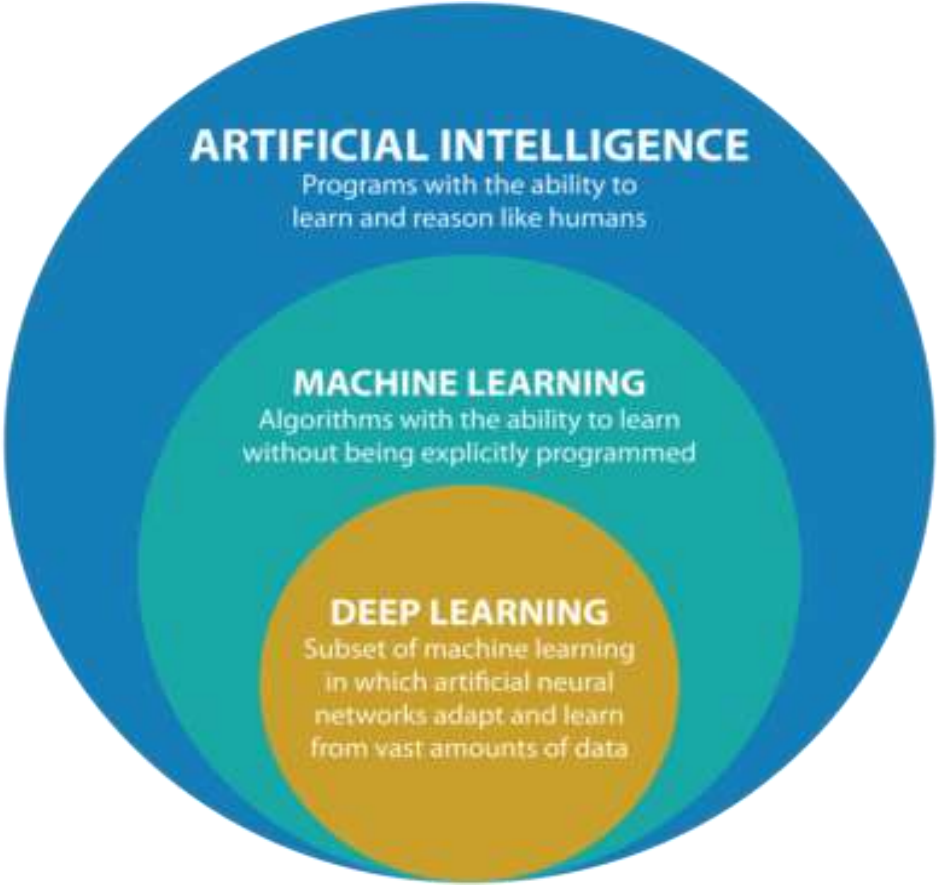
MORE DATA AND COMPUTE

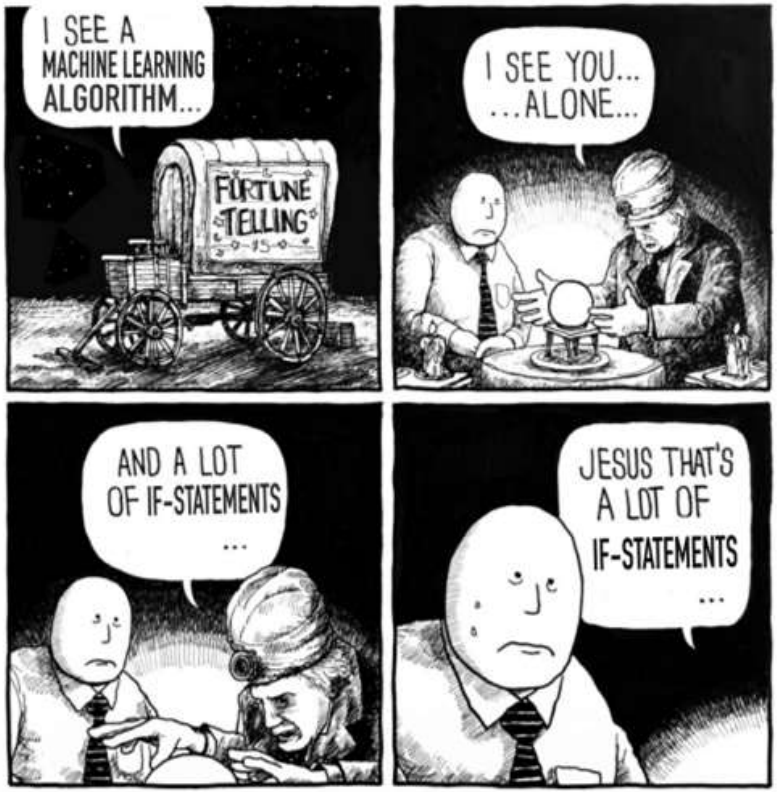
- Explosion in Computing Power
- Exponential Data Volume Growth
- Variety of Data Sources and Formats
- Data Collected at Faster Velocity

MORE OPPORTUNITIES THAN EVER TO USE MACHINE LEARNING THAN EVER BEFORE

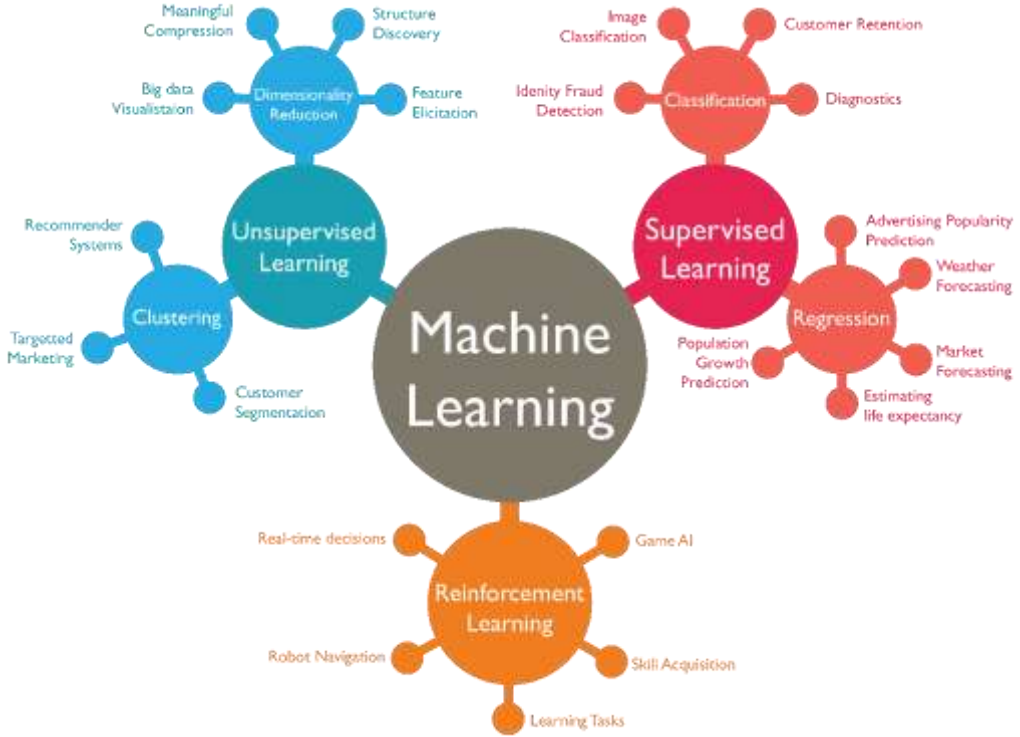
AT A LOWER COST THAN EVER BEFORE

- Lower Cost of Computing
- Affordable Cloud Infrastructure
- Free Open-Source Tools
- Community Code Sharing


ARTIFICIAL INTELLIGENCE
Programs with the ability to learn and reason like humans
MACHINE LEARNING
Algorithms with the ability to learn without being explicitly programmed
DEEP LEARNING
Subset of machine learning in which artificial neural networks adapt and learn from vast amounts of data


I SEE A MACHINE LEARNING ALGORITHM...
FORTUNE TELLING
I SEE YOU... ...ALONE...
AND A LOT OF IF-STATEMENTS ...
JESUS THAT'S A LOT OF IF-STATEMENTS ...

Types of ML


Machine Learning
Unsupervised Learning
Dimensionality Reduction
Meaningful Compression
Structure Discovery
Big data Visualisation
Feature Elicitation
Clustering
Recommender Systems
Targetted Marketing
Customer Segmentation
Supervised Learning
Classification
Image Classification
Customer Retention
Idenity Fraud Detection
Diagnostics
Regression
Advertising Popularity Prediction
Weather Forecasting
Market Forecasting
Estimating life expectancy
Population Growth Prediction
Reinforcement Learning
Real-time decisions
Game AI
Robot Navigation
Skill Acquisition
Learning Tasks

Supervised Machine Learning

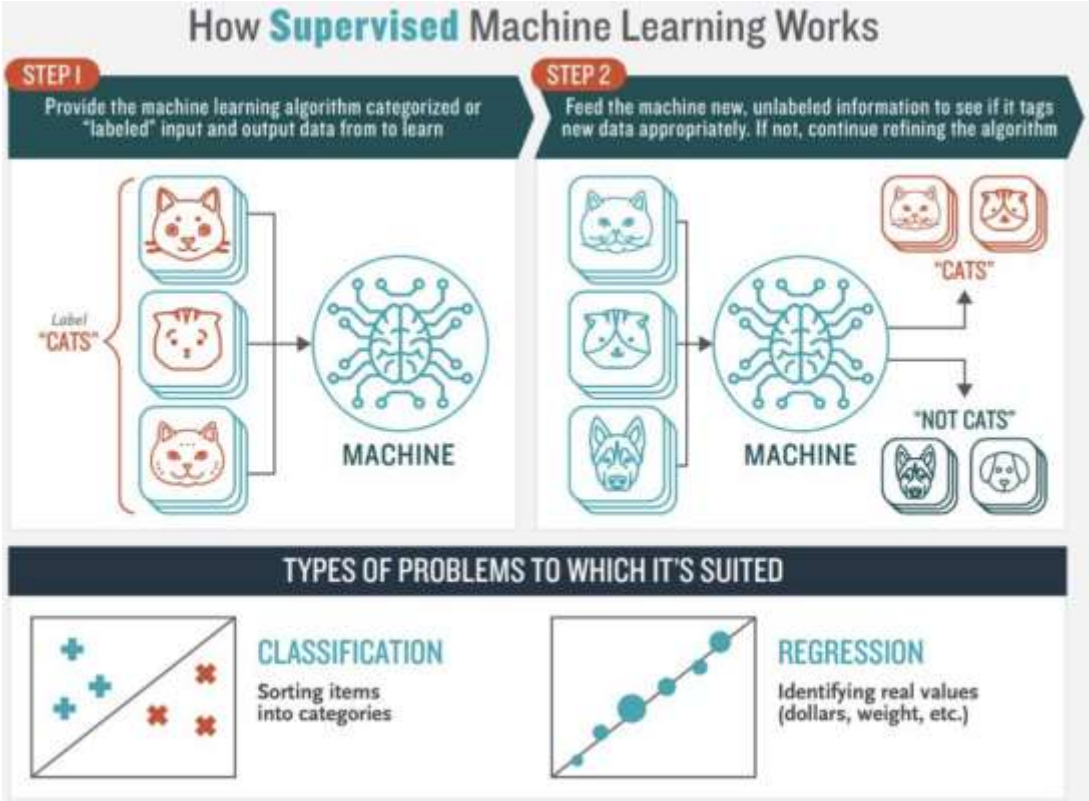


Image Source: boozallen.com

Unsupervised Machine Learning

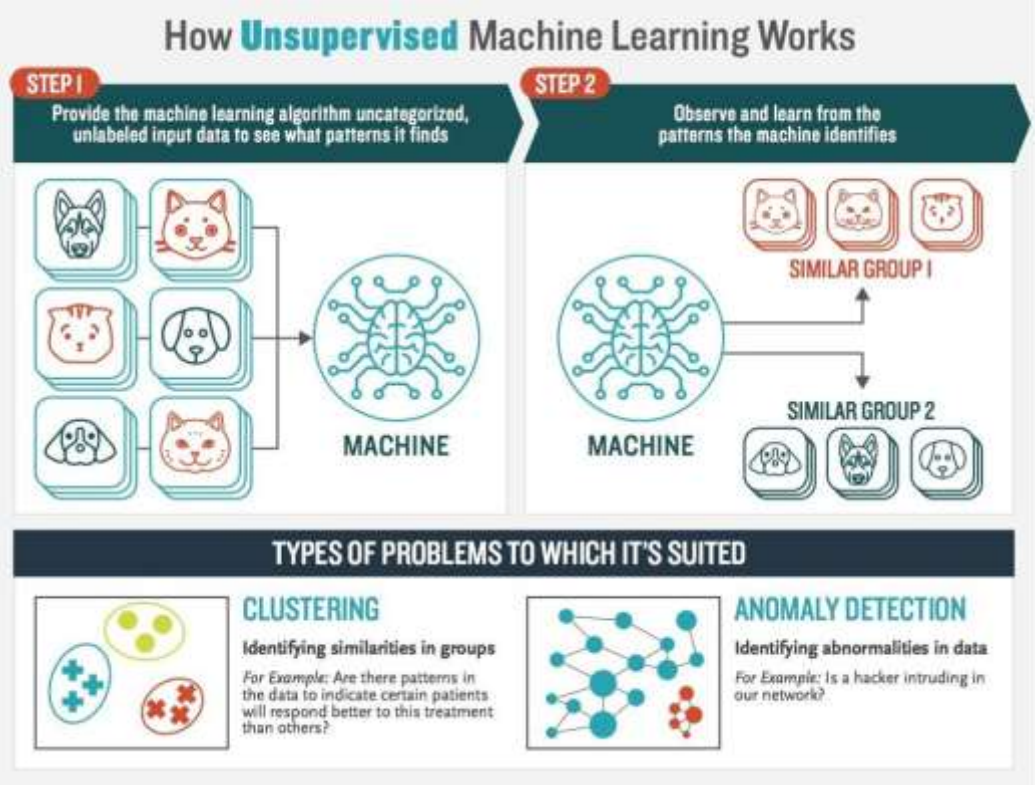
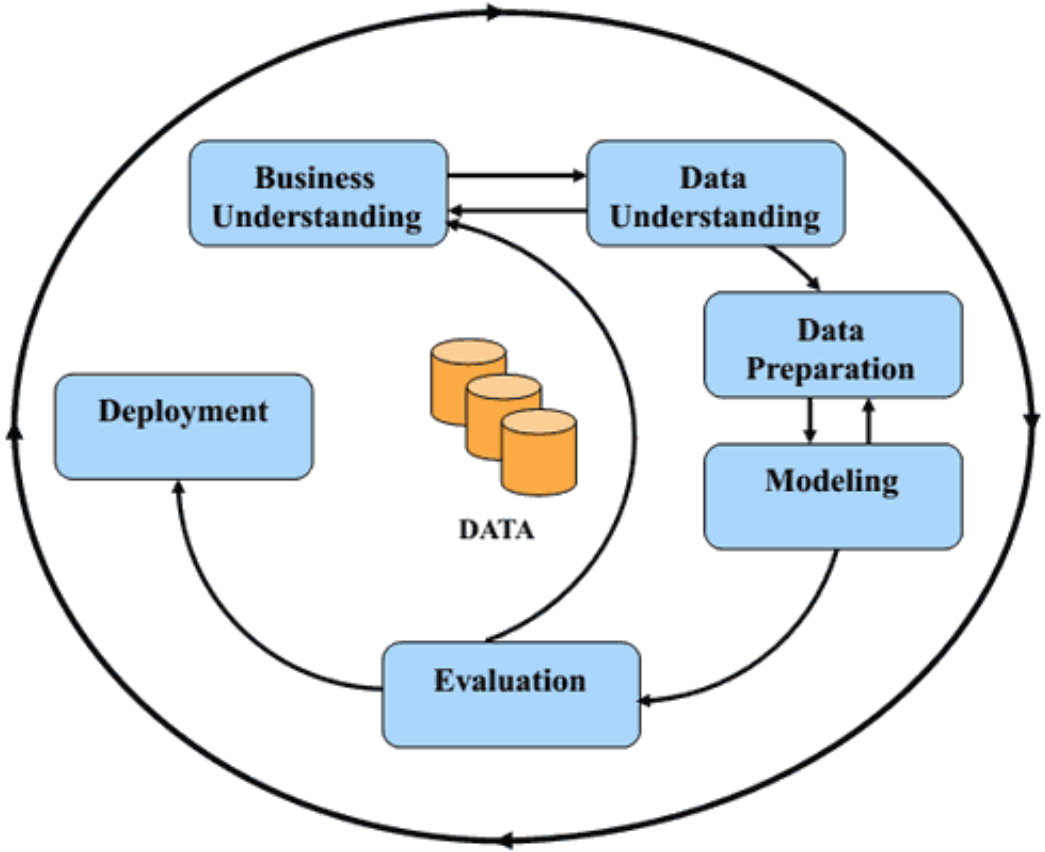


Image Source: boozallen.com

Building and Deploying Machine Learning Models Should Follow a Disciplined Approach



Cross Industry Standard Process for Data Mining

34%

Report their organisation has experienced a damaging cyberattack in the last 12 months

72%

Agree that as long as their protection keeps them safe from cybercriminals, they do not care if it uses AI/ML

73%

Plan to use more AI/ML tools in 2019

84%

Believe cybercriminals are using AI/ML to attack organisations

Who is going to win the battle?

VS

Hackers

Cybersecurity professionals

How to use ML in cyberattacks?

Already implemented...

- Creating fake news, deepfakes
- Phishing mails generator
- Generates malware examples, that are able to bypass black-box ML-based detection models
- Password cracking
- Searching and attacking system vulnerabilities
- Bypass of captcha
- ...And almost any other cyberattacks powered by AI or ML

Cyber Kill Chain Model

How can we use ML to protect from cyberattacks?

Already implemented

- To identify anomalies
- To identify suspicious or unusual behaviour
- Detect and correct known vulnerabilities
- Detect and correct suspicious behaviour
- Detect and correct zero-day attacks
- And almost any other cybersecurity product powered by AI or ML...

Types of solutions which use ML

- Anti-fraud & Identity Management
- Malware classification
- Spam identification
- DNS analytics
- Mobile Security
- Predictive Threat Intelligence
- Behavioural Analysis & Anomaly Detection
- Automated Security Cyber-Risk Management
- App Security
- IoT Security
- Deception Security
- Analyst automation

CYBERSECURITY'S NEXT STEP MARKET MAP:
80+ COMPANIES SECURING THE FUTURE WITH ARTIFICIAL INTELLIGENCE

ANTI FRAUD & IDENTITY MANAGEMENT

AGARI
feedzai
Ravelin
smyte.
ZYUDLYLABS
邦盛科技 Rangsun Technology
GreatHorn
pulseID
skymind
OVU
Castle
GYOMO
rippleshot
simility
veridu
CYBERTONICA
id wall
Shift Technology
sift science
UNFRAUD
DATAVISOR
PRECOGNITIVE
数美 NAVTDATA
SOCURE
trooly

MOBILE SECURITY

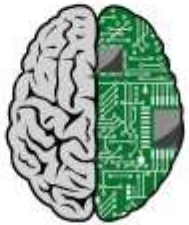
appthority
Mi³ Security
Sentegrity
Skycure
ZIMPERIUM.

PREDICTIVE INTELLIGENCE

CYLANCE
deepinstinct
indeni
INNEFU
IntelliSpyre
SECB
signalsense
ANOMALI
PROTENUS

BEHAVIORAL ANALYTICS / ANOMALY DETECTION

Avata INTELLIGENCE
BehavioSec
DARKTRACE
SPHERICALDEFENCE
8 SECURITY
RUBICA
CyberX
RedLock
sqrrl



AUTOMATED SECURITY

DEMISTO
EdgeWave
JAVELIN
LogicHub

CYBER-RISK MANAGEMENT

cybersaint
CYENCE
Cytora
Haystax
lexumo

What are the problems?

benign network activity is almost **never normal**

adversaries and their tactics are **moving targets**

every false positive costs **time and money**

insights must be both **accurate and actionable**

Cybersecurity solutions must evolve

ADVANCED ATTACKERS AND TECHNIQUES

CYBER CRIME FOR SALE

GROWING COLLATERAL DAMAGE

Thank you for your attention!