Ochráni nás umelá inteligencia pred kyberhrozbami ?

Juraj Nemeček, ITAPA 2021

Tempest

IT makes sense

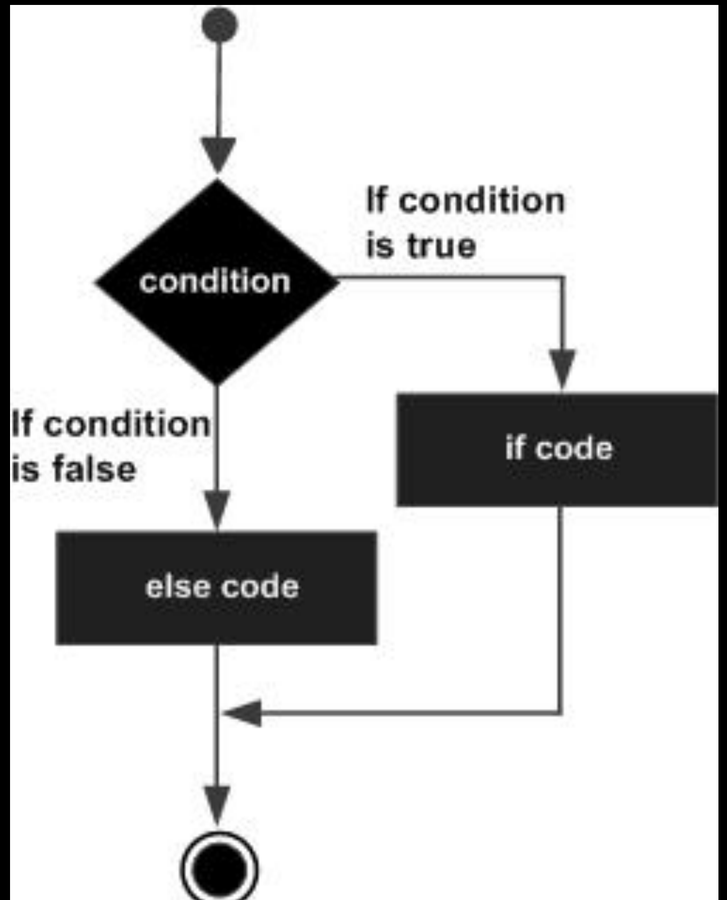
Umelá inteligencia

“Vedecká teória a výskum spojený s budovaním **počítačových systémov** schopných robiť činnosti **vyžadujúce ľudskú inteligenciu**, ako sú rozpoznávanie objektov, rozpoznávanie reči, preklad medzi rôznymi jazykmi alebo vedomá tvorba rozhodnutí.”

Oxford English Dictionary

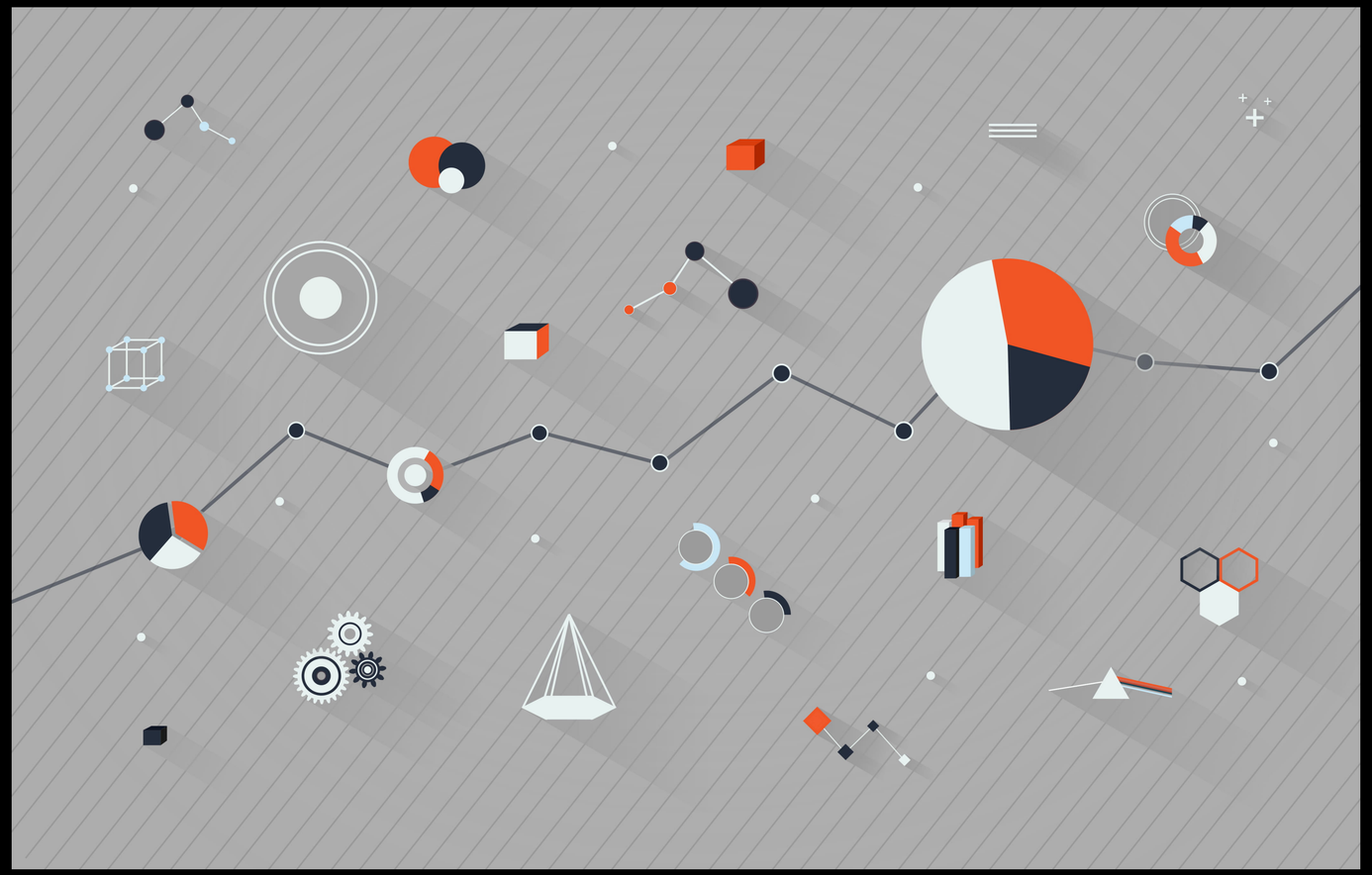
Umelá inteligencia

Programovanie bezpečnosti ?



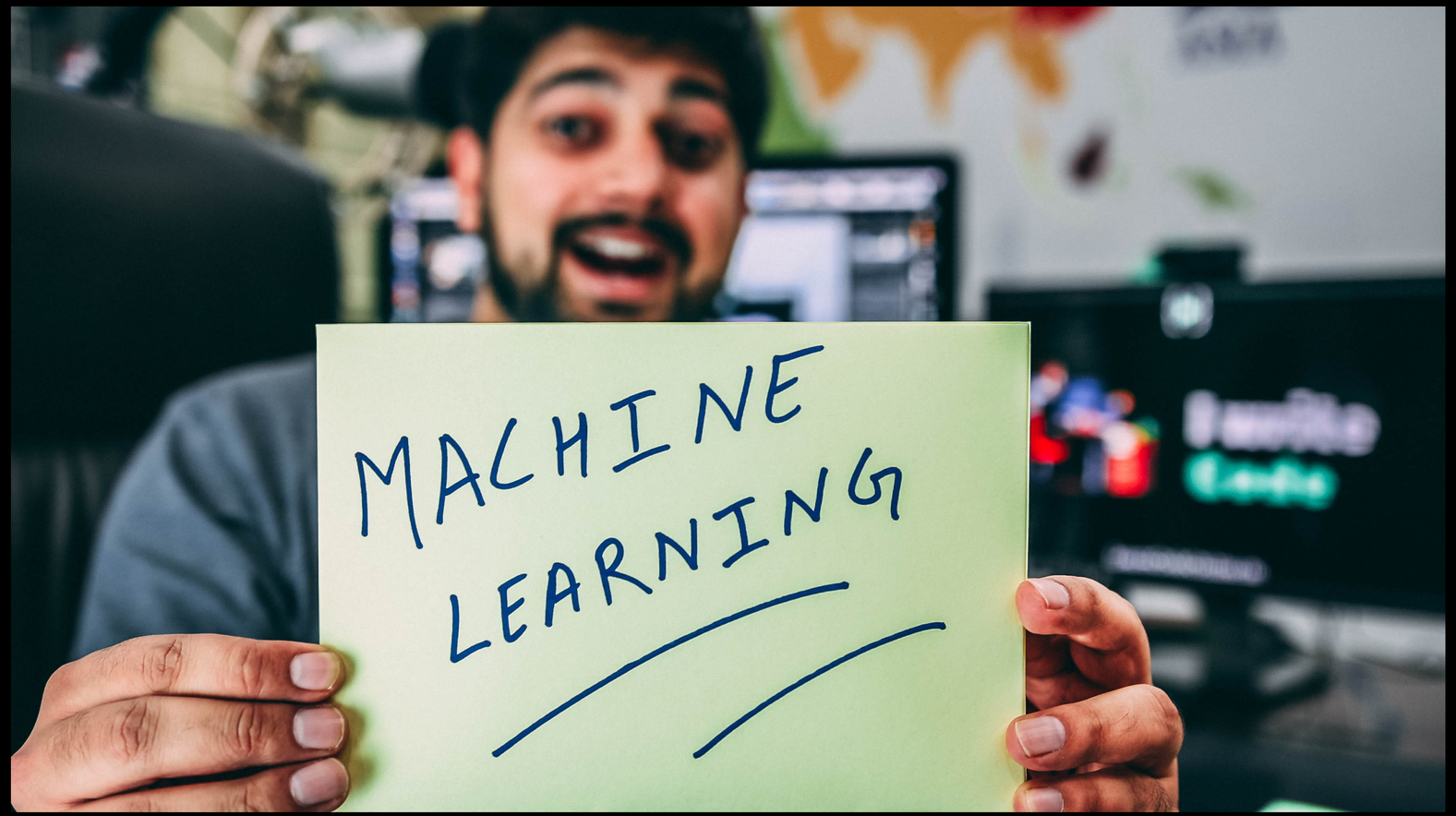
Umelá inteligencia

Príliš veľa dát



Machine learning

Machine learning



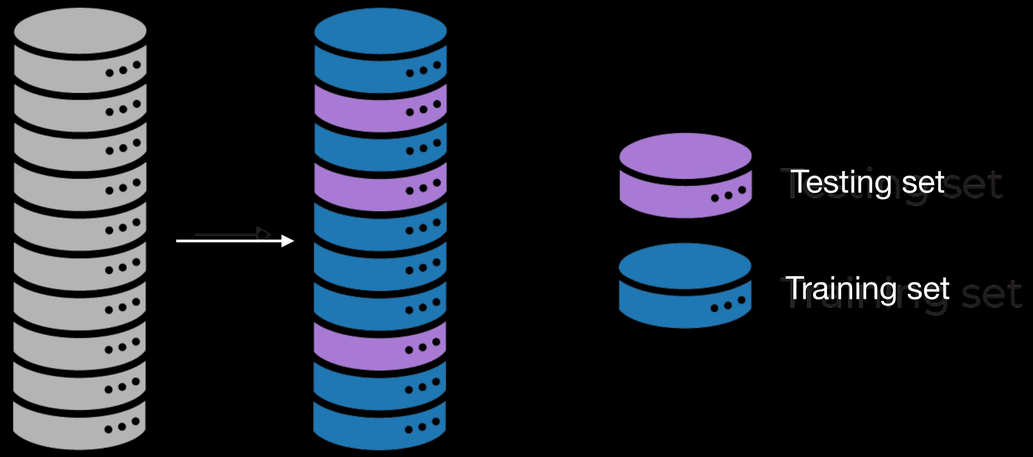
Machine learning

“Vývoj a nasadenie počítačových systémov, ktoré sú schopné adaptácie aj bez explicitných inštrukcií, a to prostredníctvom použitia algoritmov a štatistických modelov na základe ktorých určujú vzťahy medzi vzorcami v analyzovaných dátach.”

Oxford English Dictionary

Machine learning
Dataset

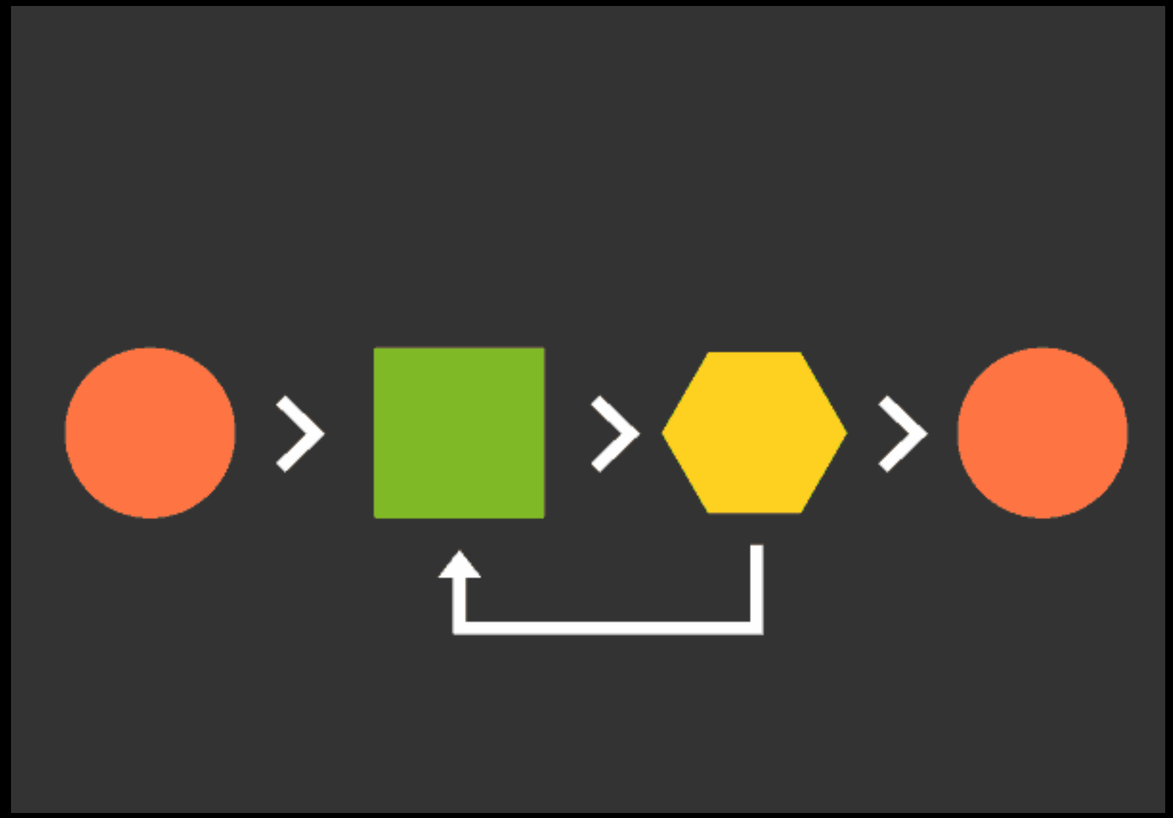
- Trénovací dataset
- Testovací dataset



Machine learning

Alogritmus

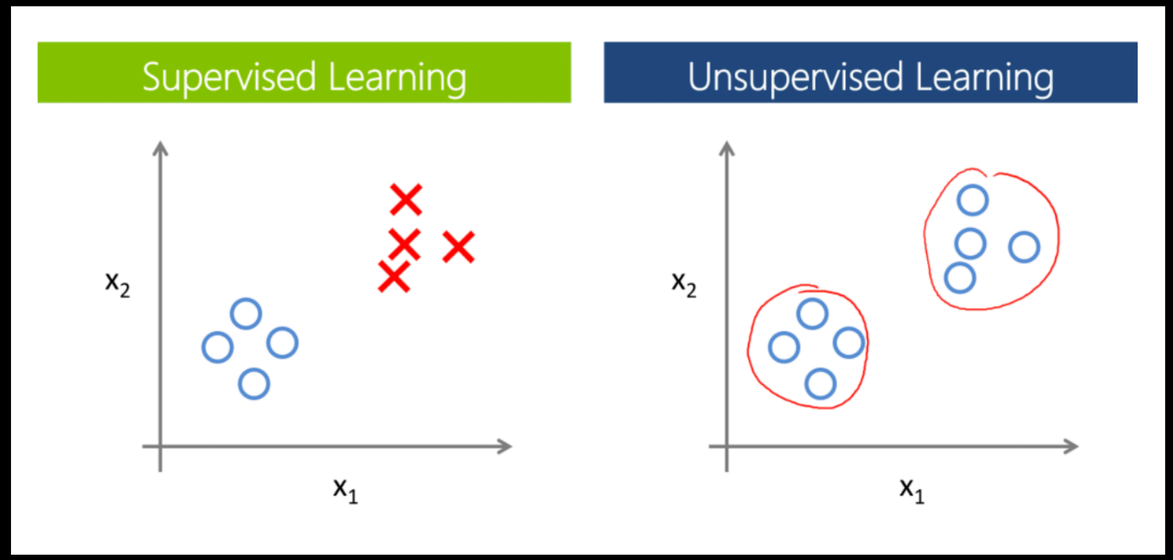
- Data + Algoritmus = Model



Machine learning

Supervised vs unsupervised

- Supervised dáva odporúčania
- Unsupervised hľadá trendy



Machine learning
Problémy

- Správny algoritmus
- Dostupnosť datasetu
- Skreslenie vstupných dát (bias)
- Náchylnosť ML systému na útok
- …

Machine learning

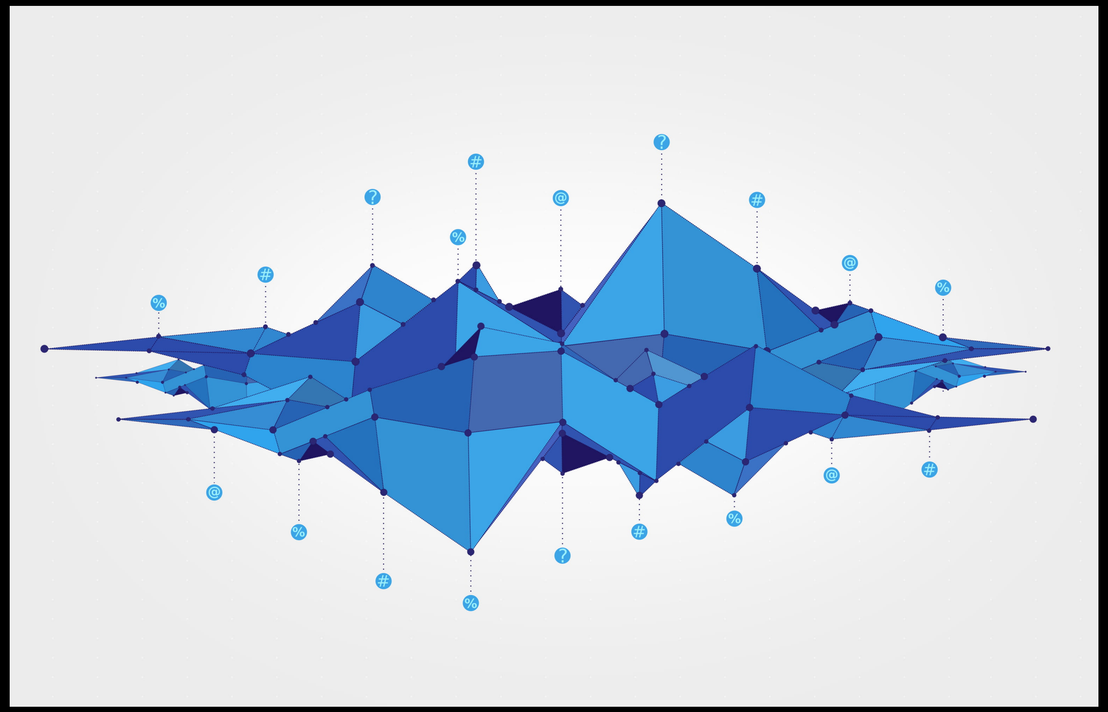
Nasadenie

- AntiSPAM
- Vyhľadávanie zraniteľností v kóde

Machine learning

Nasadenie

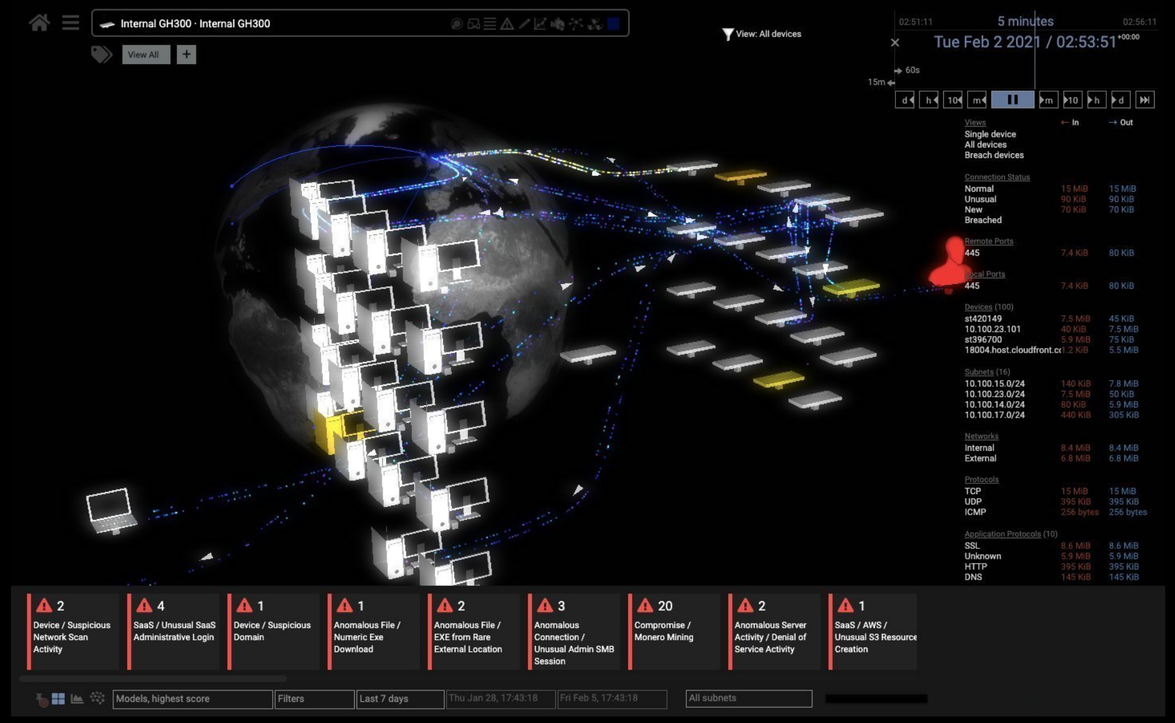
- Data mining záznamov
- Analýza potencionálne škodlivého kódu



Machine learning

Nasadenie

- Behaviorálna analýza sieťovej prevádzky
- Hodnotenie závažnosti incidentov
- Incident response, threat hunting
- Cielené blokovanie útokov



Machine learning

Kam dal'ej

- Autonómna tvorba bezpečnostnej politiky
- Detekcia sociálneho inžinierstva
- Detekcia kyberhrozieb na lokálnych staniciach
- Heterogénne prostredia

Ďakujem za pozornosť

Juraj Nemeček, ITAPA 2021