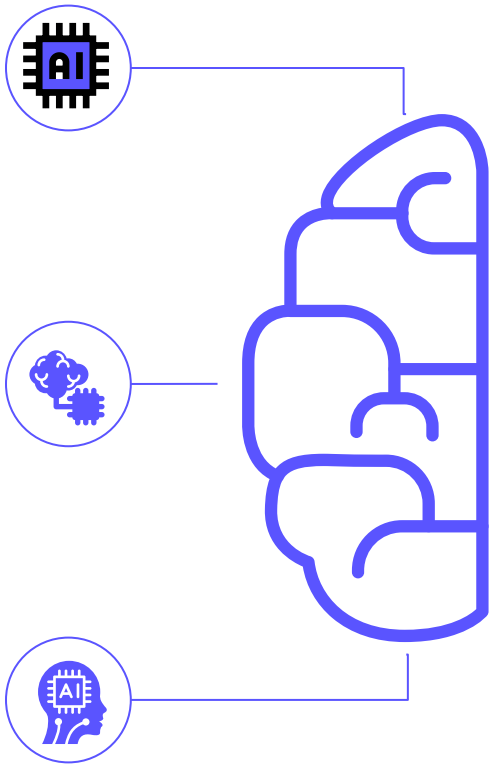
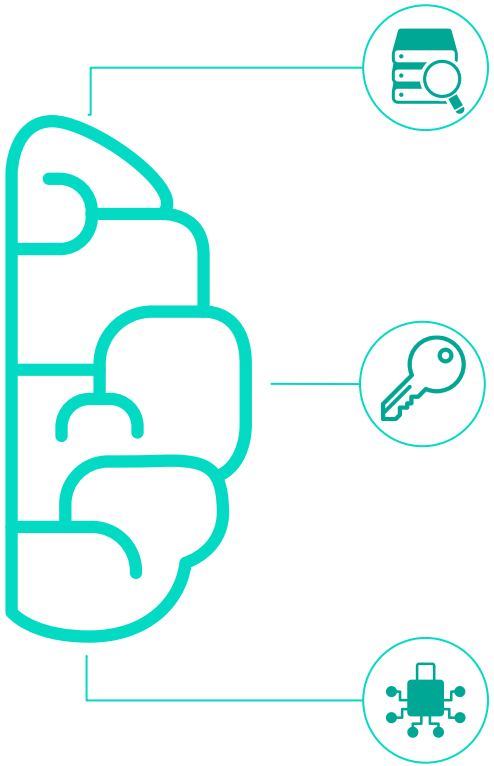


AI and Security

Fluch oder Segen?



ÜBER UNS

swisscom

Gzim Xheladini

Security Solution Architect bei Swisscom Banking Security

IAM, WAF, Confidential Computing, Zero Trust Architecture

ÜBER UNS

Gzim Xheladini

Security Solution Architect bei Swisscom Banking Security

IAM, WAF, Confidential Computing, Zero Trust Architecture

Michael Veser

Security Consultant bei der TEMET AG

PKI, HSM, WAF, SoC, AI

Welche Gedanken haben Sie?

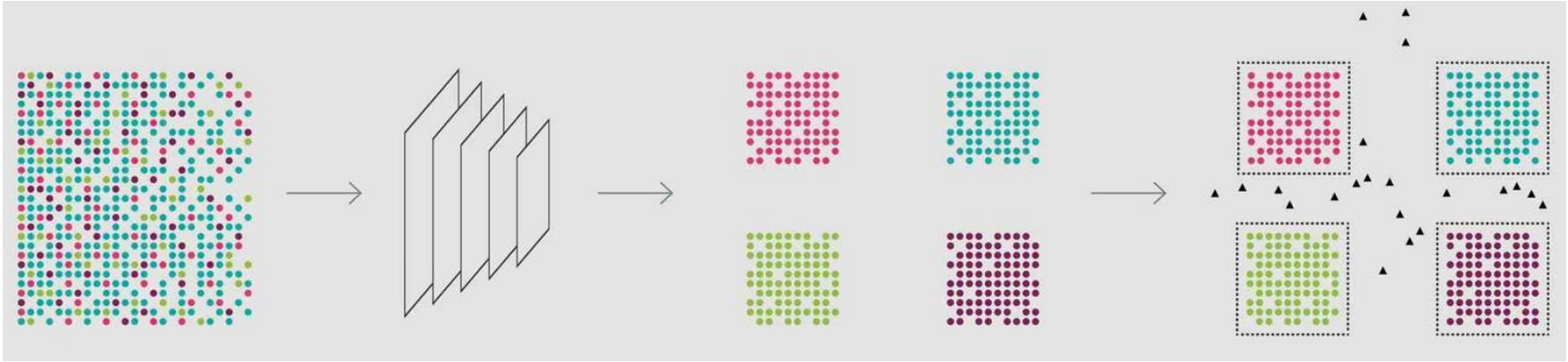
AI

Neural Networks
Big Data
OpenAI
Deep Learning
Natural Language Processing (NLP)
Automation
ChatGPT
Machine Learning
Artificial Intelligence
Autonomous vehicles

IT Security

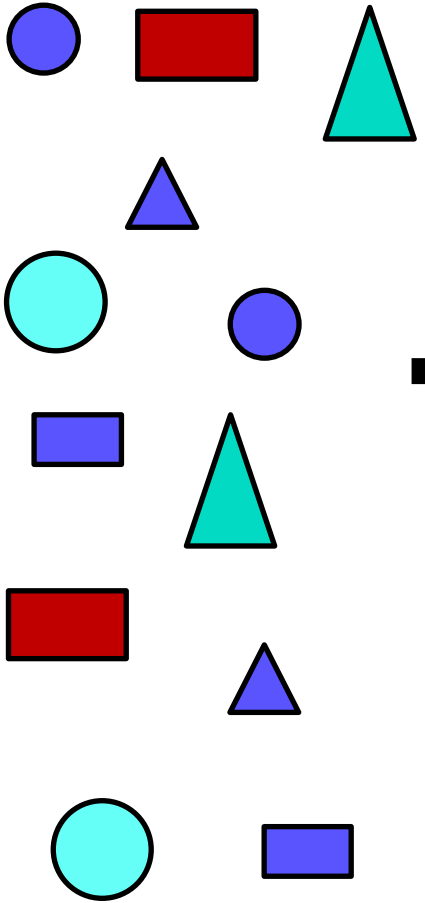
IDS/IPS
Malware
Encryption
Penetration Testing
Authentication
Cybersecurity
Data Privacy
Antivirus
Vulnerability
Firewall

Beispiel Anomaly Detection

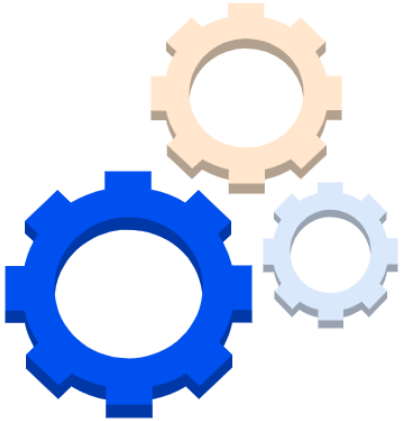


Unsupervised Learning

Input Daten



Maschine

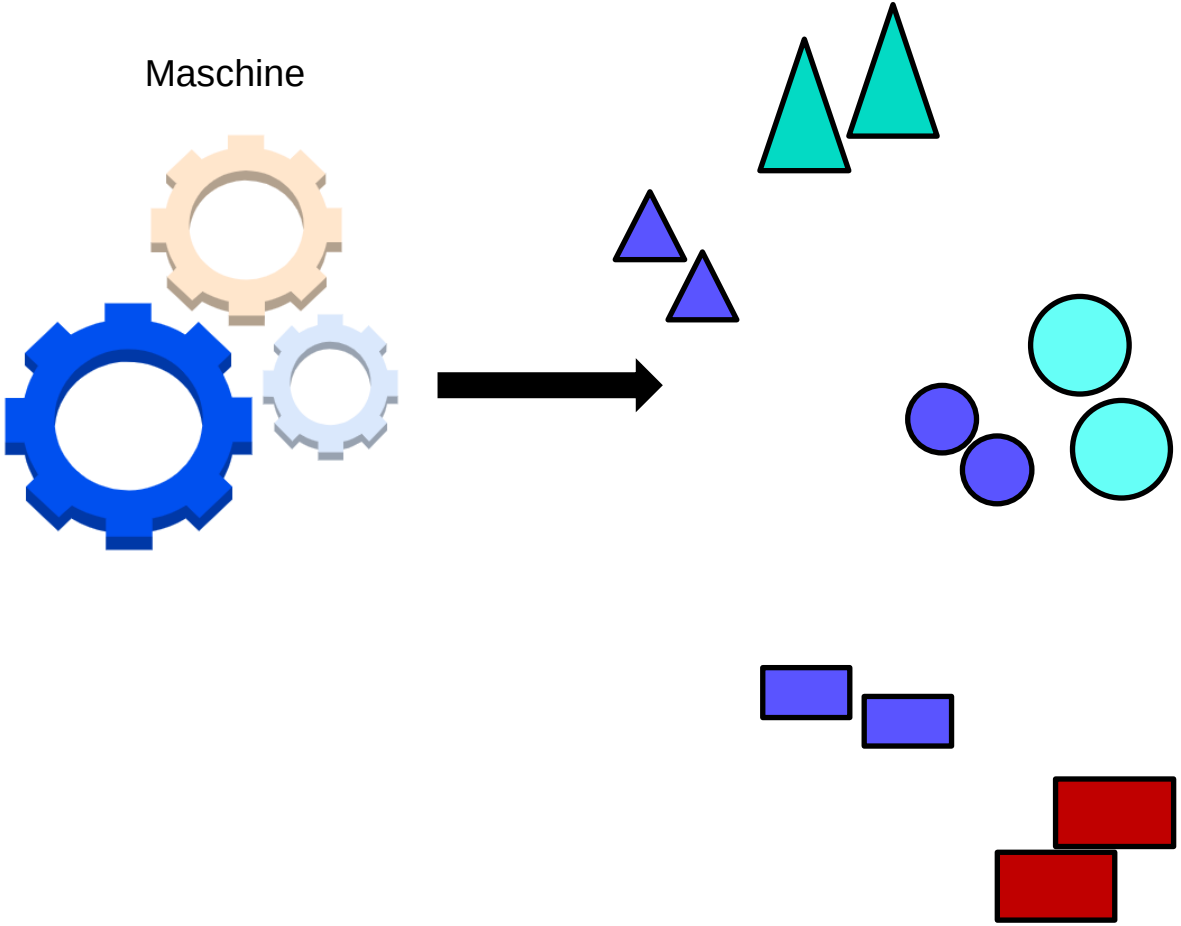


Input Daten

Unsupervised Learning

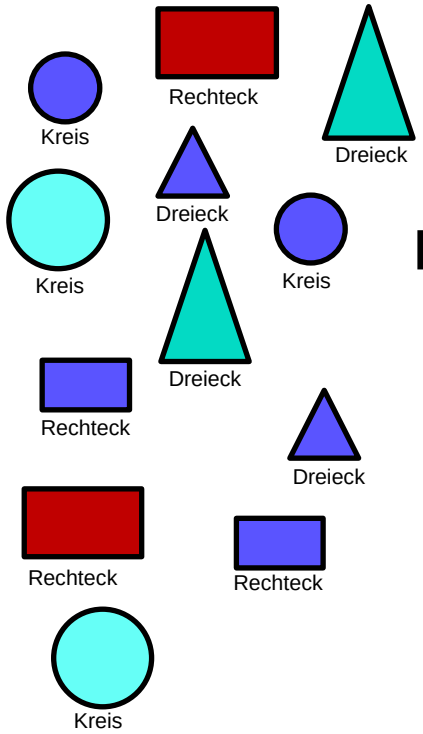
Output Daten

Maschine



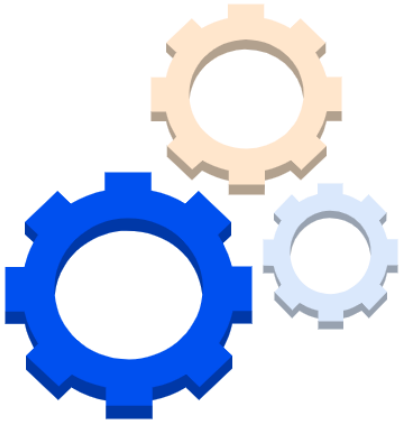
Supervised Learning - Training

Trainingsdaten



Training

Maschine

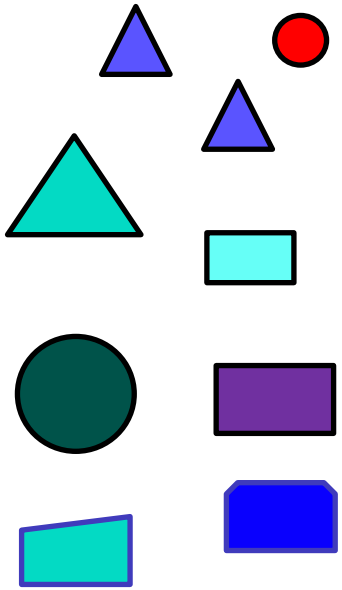


Relevante Labels

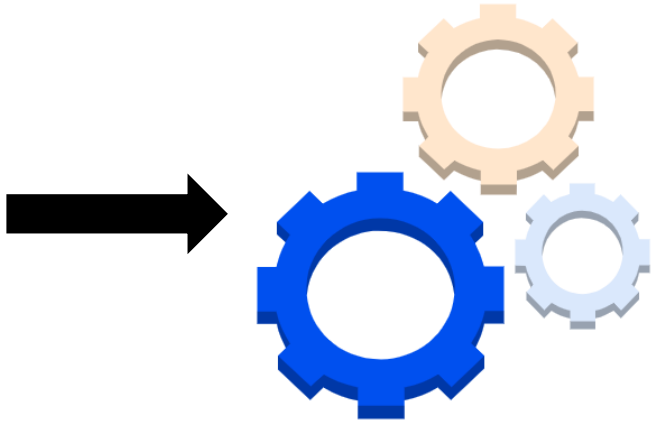
Rechtecke
Dreiecke
Kreise

Supervised Learning - Testing

Testdaten



Maschine



Ergebnis

Rechtecke

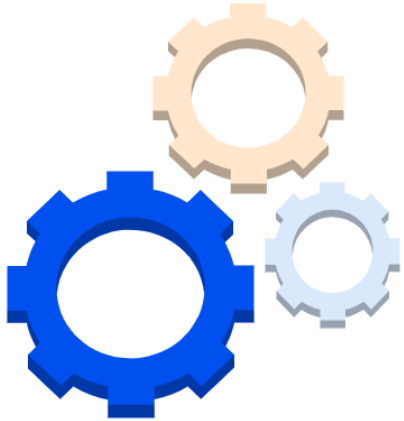
Dreiecke

Kreise

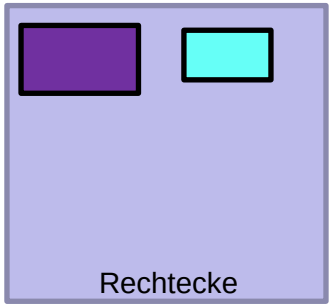
Supervised Learning - Testing

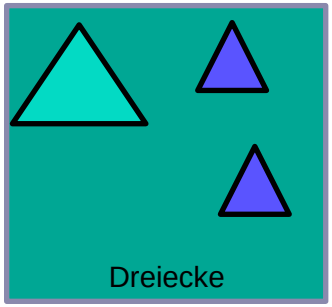
Testdaten

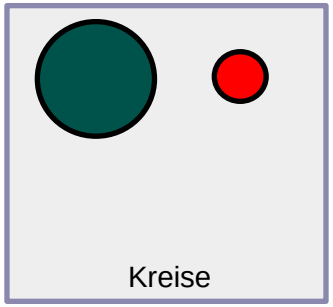
Maschine



Ergebnis







Generative AI

Quelle: https://konradweber.ch/2018/11/08/deep-fake-videos-verifizieren/

Deepfake - oder doch nicht?

Quelle: www.instagram.com/julian_ai_art

Deepfake - oder doch nicht?

Quelle: www.instagram.com/julian_ai_art

Quelle: r/midjourney via Reddit.com

Praxisbeispiel

Missbrauchspotential

Desinformation

Deepfake-Video gaukelt kapitulierenden ukrainischen Präsidenten vor

Fr 18.03.2022 - 12:23 Uhr
von Yannick Chavanne und Rodolphe Koller und Übersetzung von: Pascal Wojnarski, kfi

Russlands Krieg gegen die Ukraine wird auch regelmässig von Desinformationskampagnen begleitet. Nun machte auch ein Deepfake-Video die Runde, das angeblich den kapitulierenden ukrainischen Präsidenten zeigt. Die sozialen Medien gehen rigoros gegen die Verteilung solcher Fehlinformationen vor.

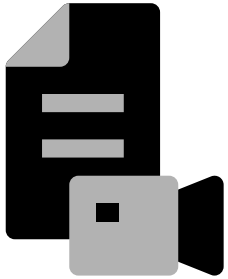
https://www.netzwoche.ch/news/2022-03-18/deepfake-video-gaukelt-kapitulierenden-ukrainischen-praesidenten-vor

Flächendeckende Überwachung mit Gesichtserkennung erreicht in China ein völlig neues Level

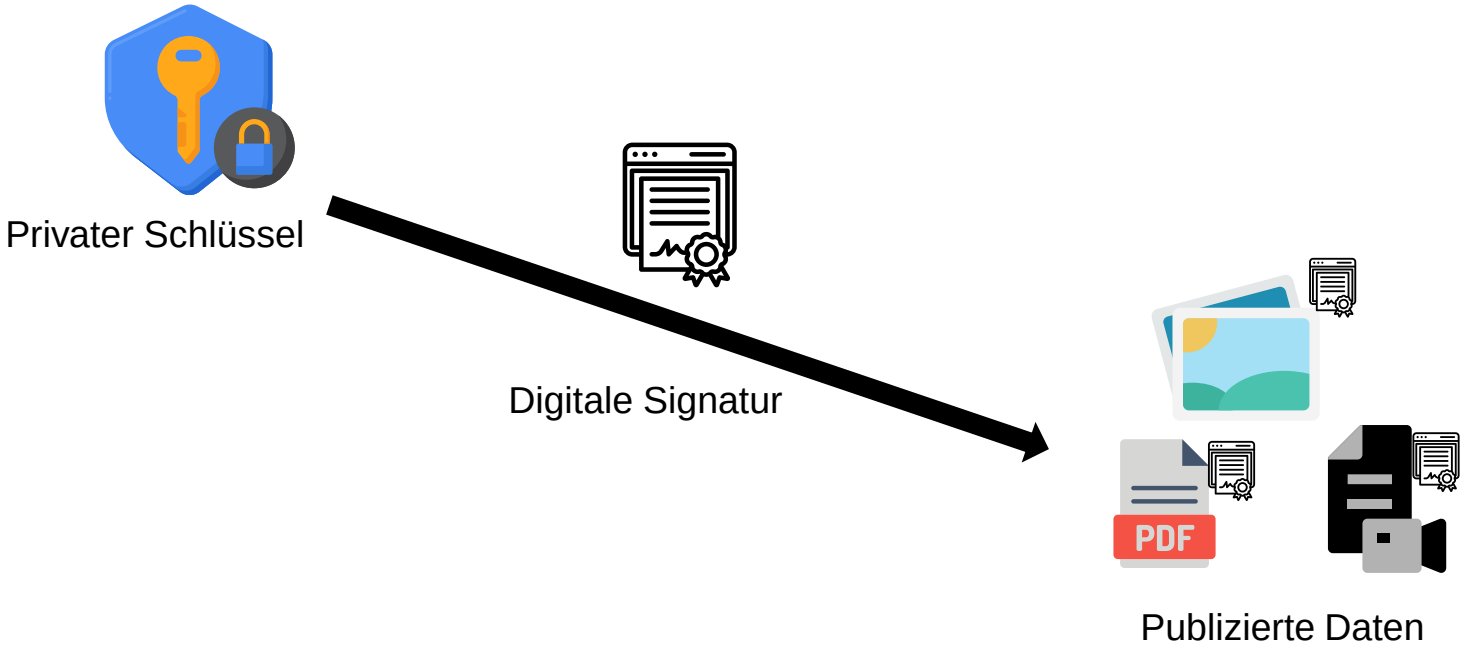
Ein Bericht über ein neues Überwachungssystem in China alarmiert Datenschützerinnen und Menschenrechtsaktivisten. Doch auch im Rest der Welt breitet sich die Überwachung per Gesichtserkennung im öffentlichen Raum aus.

https://www.watson.ch/digital/international/896447927-ueberwachung-mit-gesichtserkennung-erreicht-in-china-ein-neues-level

Generative AI - Problemstellung



Generative AI - Lösungsansatz



Generative AI

Pros

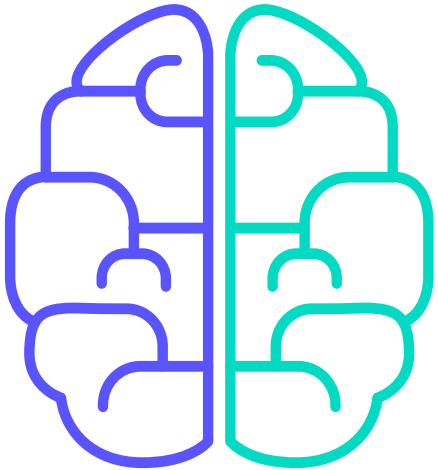
- Tutorials
- Zeitersparnis
- Routinearbeiten

VS

Cons

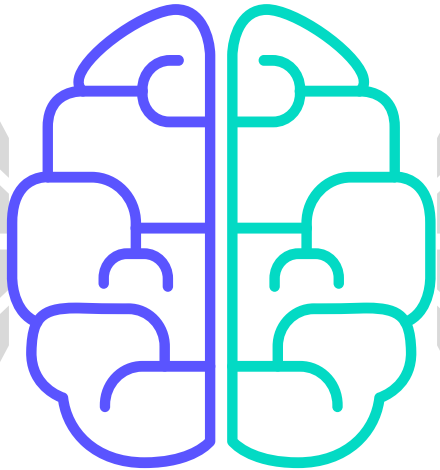
- Rufschädigung
- Kursmanipulation
- Schwer erkennbar

Herausforderungen



Herausforderungen

- Generative AI
- Datenschutzverletzungen
- Missbrauchspotential
- Manipulation



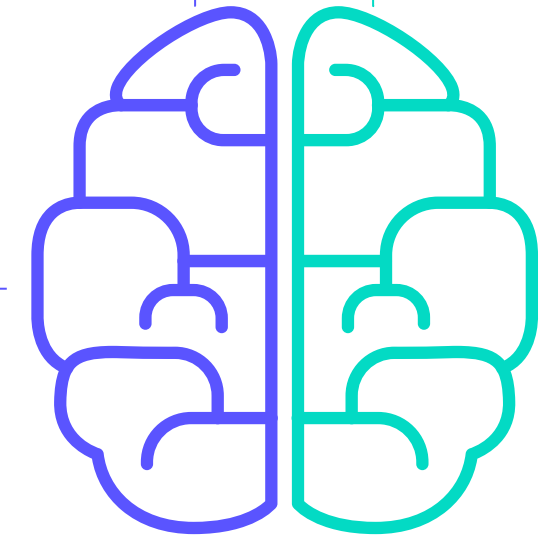
- Datenqualität
- Sinnvolle Algorithmik
- Zugriffskontrolle
- Komplexität

Erkenntnisse

AI generierte Inhalte werden unsere Informationswahrnehmung verändern

Die AI Technik ist aktuell weiter als die eigentlich nötige Security Infrastruktur

AI ist ein Schutzobjekt



IT Security profitiert von AI

AI kann Arbeit erleichtern

Schon heute weit verbreitet

Vielen Dank