



# The next big threat – DATA POISONING

September 2022 | Thomas Plank



**Magenta**®

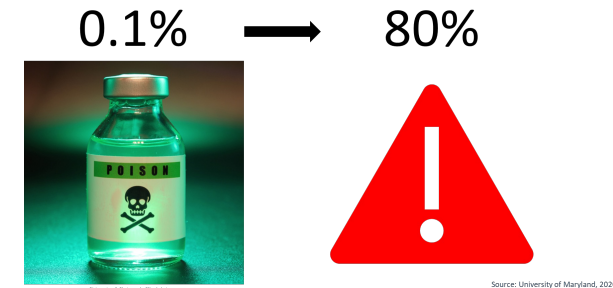


# Problem: Even a little poisoned data puts your business at risk

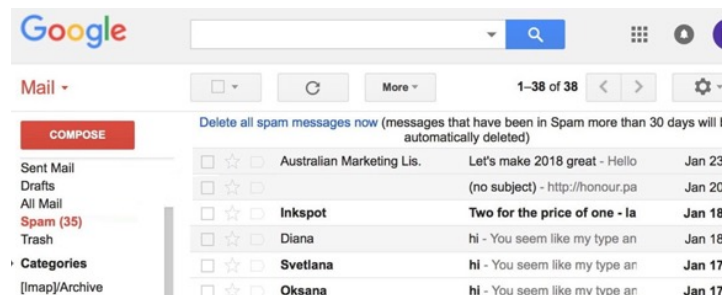
## Manipulating data to sabotage decision-making, data models, or applications



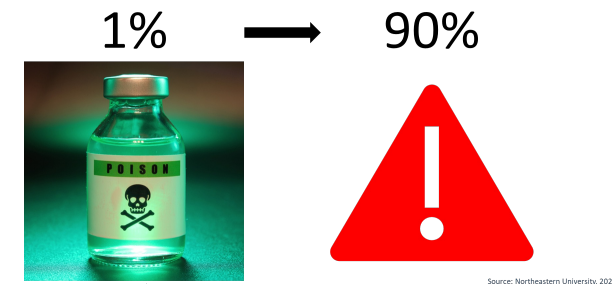
Example: Image recognition model identifying **airplane** or **frog**



Percentage of poisoned data resulting in changed behaviour of decision-making



Example: Spam filter optimized based on **training data & history**



Percentage of poisoned data resulting in changed behaviour of decision-making

# Need to buy: Trustworthy data pipelines eliminate risk

No solution for detection of data poisoning available on the market



2022: **30%** training data poisoning attacks

**3,900% increase** of cyber attacks on critical infrastructure

Through 2022, **30% of all AI cyberattacks will leverage training-data poisoning**, AI model theft, or adversarial samples to attack AI-powered systems.

Gartner, 2020

According to a recent report by Gartner, **attacks on critical infrastructure have increased by 3,900% since 2013**, and they predict that by 2024 a cyber-attack will be so damaging to critical infrastructure that a member of the **G20 will reciprocate with a declared physical attack**.

Gartner, 2021



**Tributech** offers the **only** solution to detect poisoned data **immediately**

# Buyer Personas & Partner Benefits

## Data Poisoning



### Buyer Personas

- CISO
- CIO
- Cyber Security Specialist
- IoT Architect
- IoT Product Owner



### Partner Benefits

- No comparable solution on the market – completely greenfield
- High margins of 10-30% in partner program
- Referral only : 10% for direct intro of end user to Tributech