HOUSTON ANALYTICS

IT ALL STARTED WITH A MISSION

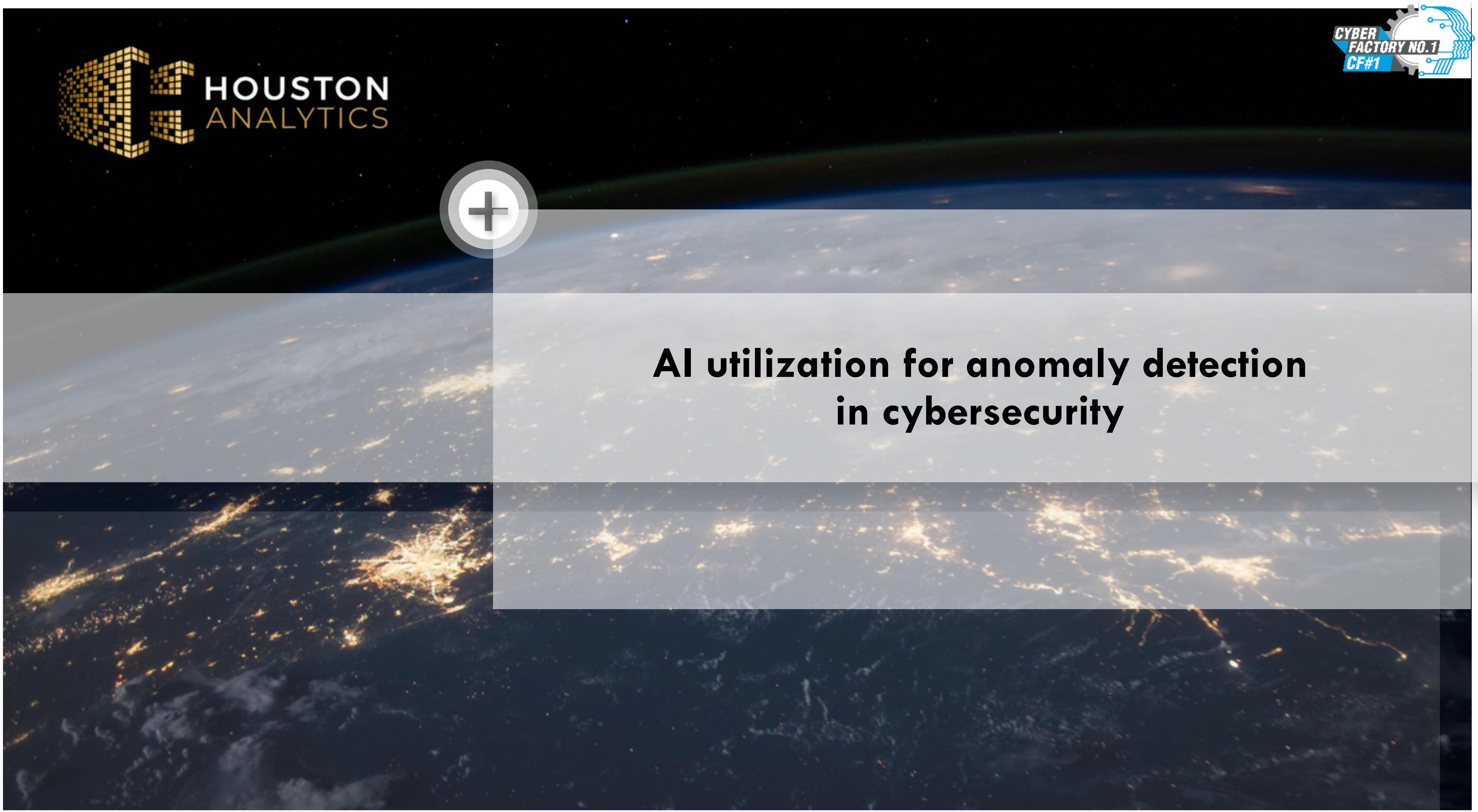
FINLAND | SWEDEN | ESTONIA | UK | GERMANY

AGENDA

Time	Topic
13:00	**Webinar Kick-off. What is CyberFactory#1 about?** Jarno Salonen, VTT
13:10	**Novel Cheese Platform** Lauri Nurminen, High Metal
13:30	**Quality assurance and monitoring of demanding IP networks in lab and live** Risto Kauppi, Rugged Tooling
13:50	**IAM approaches in factory environments** Markku Korkiakoski, Netox
14.10	**AI utilization for anomaly detection in cybersecurity** Antti Syväniemi, Houston Analytics
14:30	Short break, discussion
14.40	**Digital Twin for industrial cybersecurity simulations** Mirko Sailio, VTT
15:00	**Development of Cybersecure Architecture to improve Cyber Resilience – Practical Examples** Jari Partanen, Bittium
15:20	**Webinar conclusion and final words** Jarno Salonen, VTT

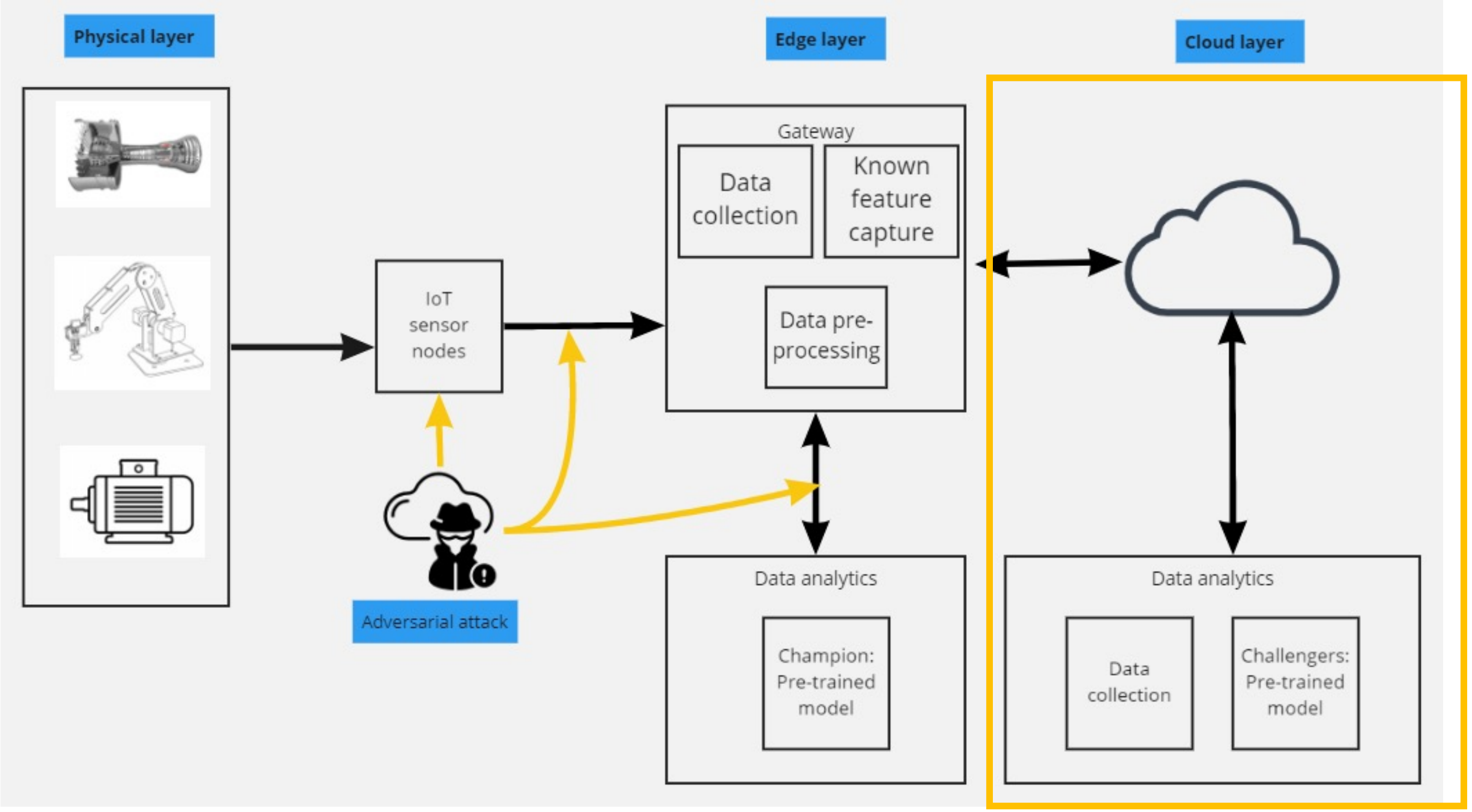
HOUSTON ANALYTICS

CYBER FACTORY NO.1 CF#1



AI utilization for anomaly detection in cybersecurity

CLOUD EDGE EXAMPLE OF THREAD MODELLING: VULNERABLE SPOTS

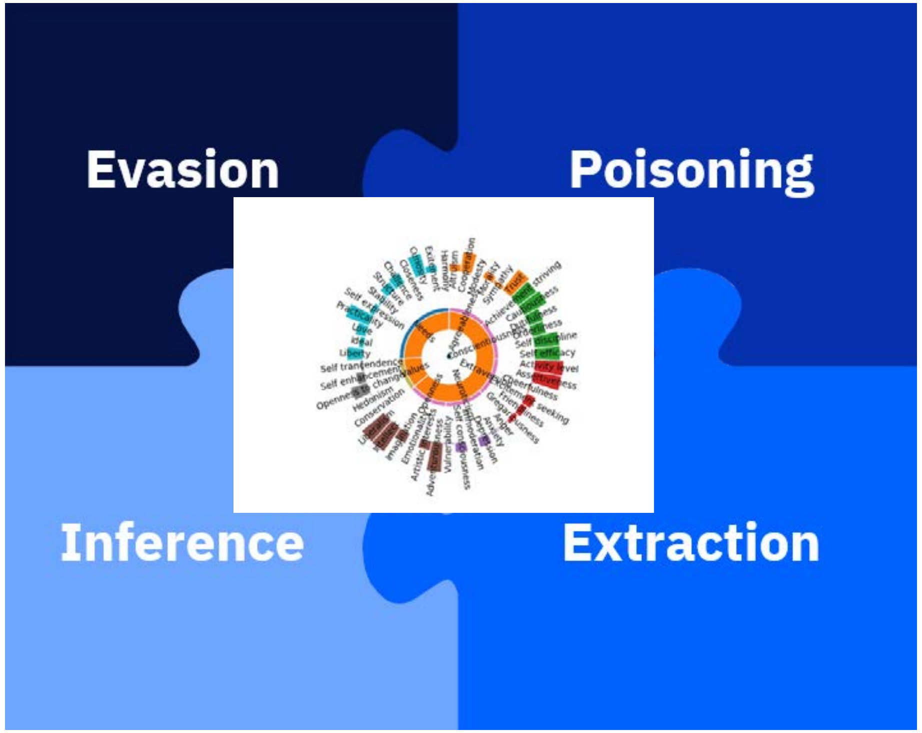


There are multiple vulnerable spots in data collection process where adversarial attack can take place:

- Actual sensors observing initial data
- Data transit from sensors to gateway
- Data transit from gateway to edge layer analytics

ANALYSIS OF OBSERVED INPUT DATA AND ANOMALIES IN BACK END TO FIGURE OUT THEIR INDIVIDUAL CHARACTERISTICS THAT MIGHT REVEAL POTENTIAL ADVERSARIAL ATTACKS

FORMS OF ADVERSARIAL ATTACKS CHALLENGING ROBUSTNESS OF AI



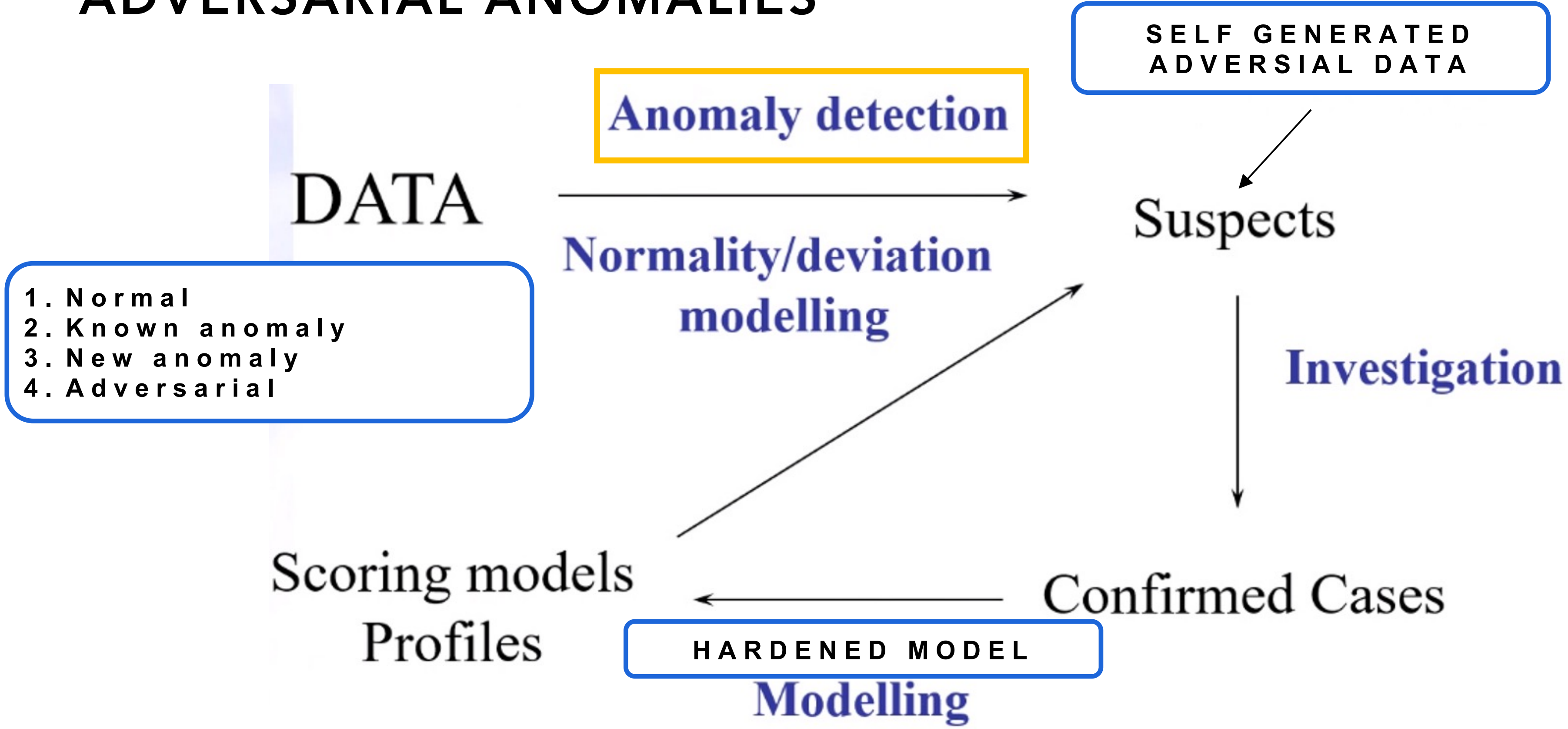
Attack can occur basically in four different ways

- Poisoning
- Interference
- Extraction
- Evasion

All of these attack patterns aim either to collected proprietary information of target's processes or impact into AI based decision making within the factory processes.

THESE ATTACK PATTERNS APPEAR IN DIFFERENT PARTS OF THE ANALYTICS PROCESS

DIFFERENT TYPES OF INPUT DATA - NEW AND ADVERSARIAL ANOMALIES



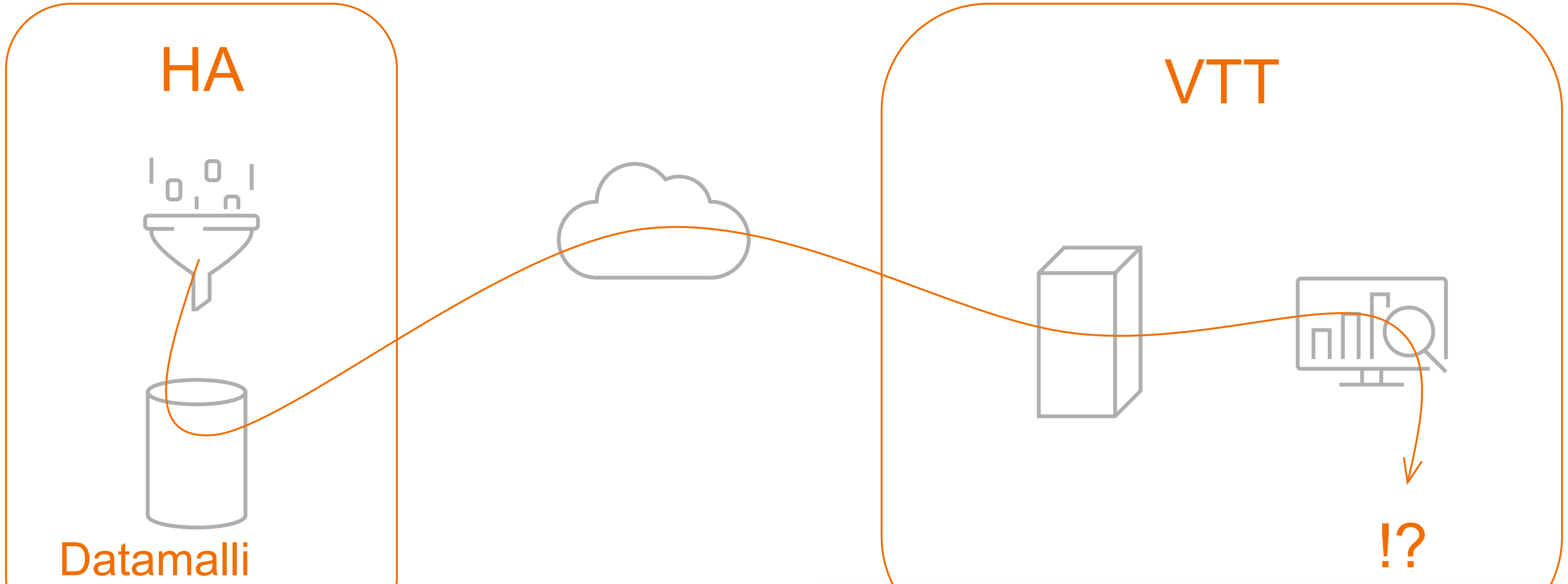
TEST THE MODEL TO FIGURE OUT POTENTIAL ADVERSARIAL ATTACK PATTERNS AND PROHIBIT THEM TO MESS CLASSIFICATION

One approach to prevent misclassification caused by adversarial example attacks:

- Generate adversarial examples
- Uses them to retrain analytical models

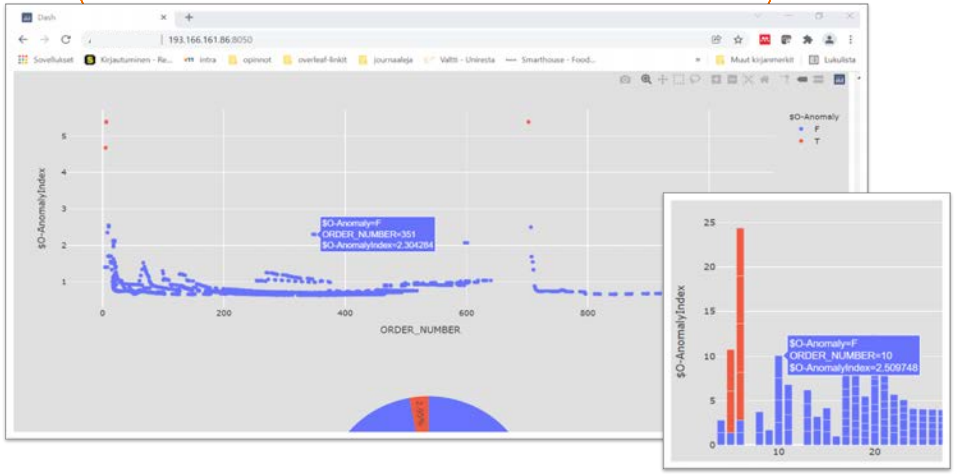
This results in hardened analytical models with a significantly reduced misclassification rate

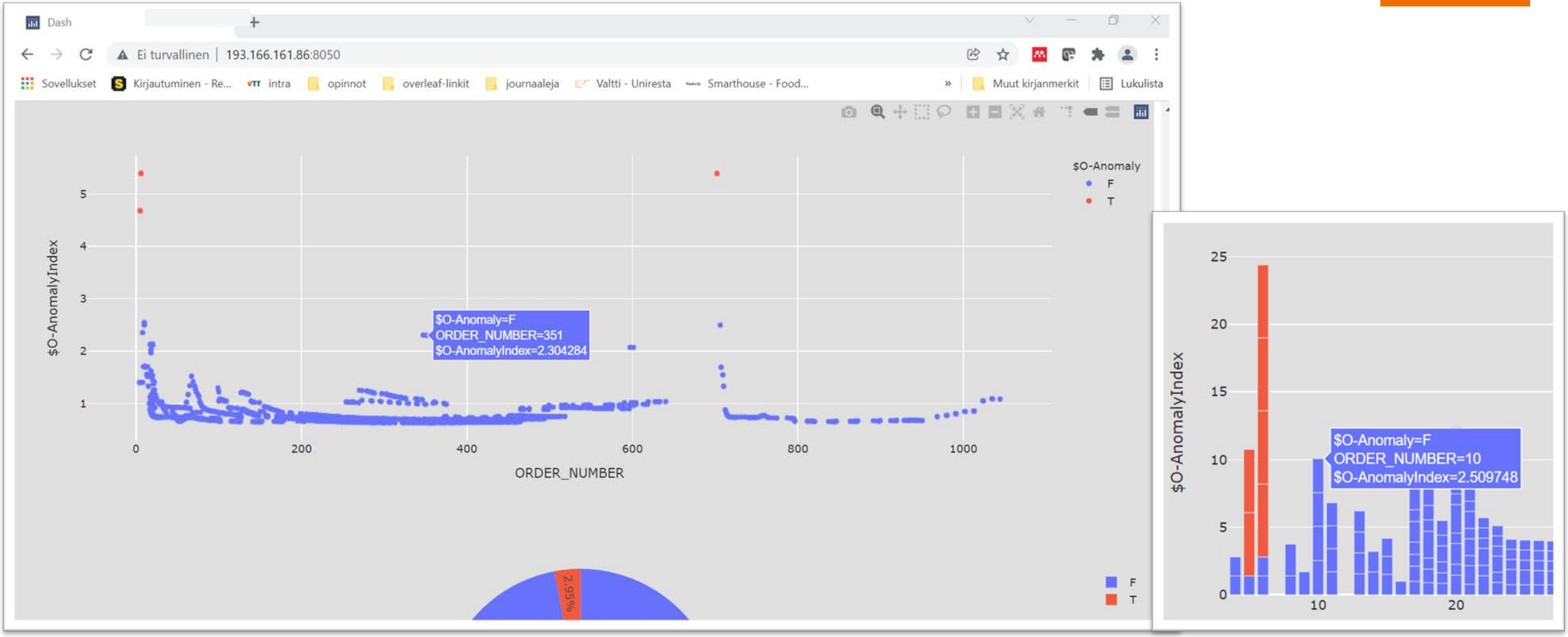
VTT demo



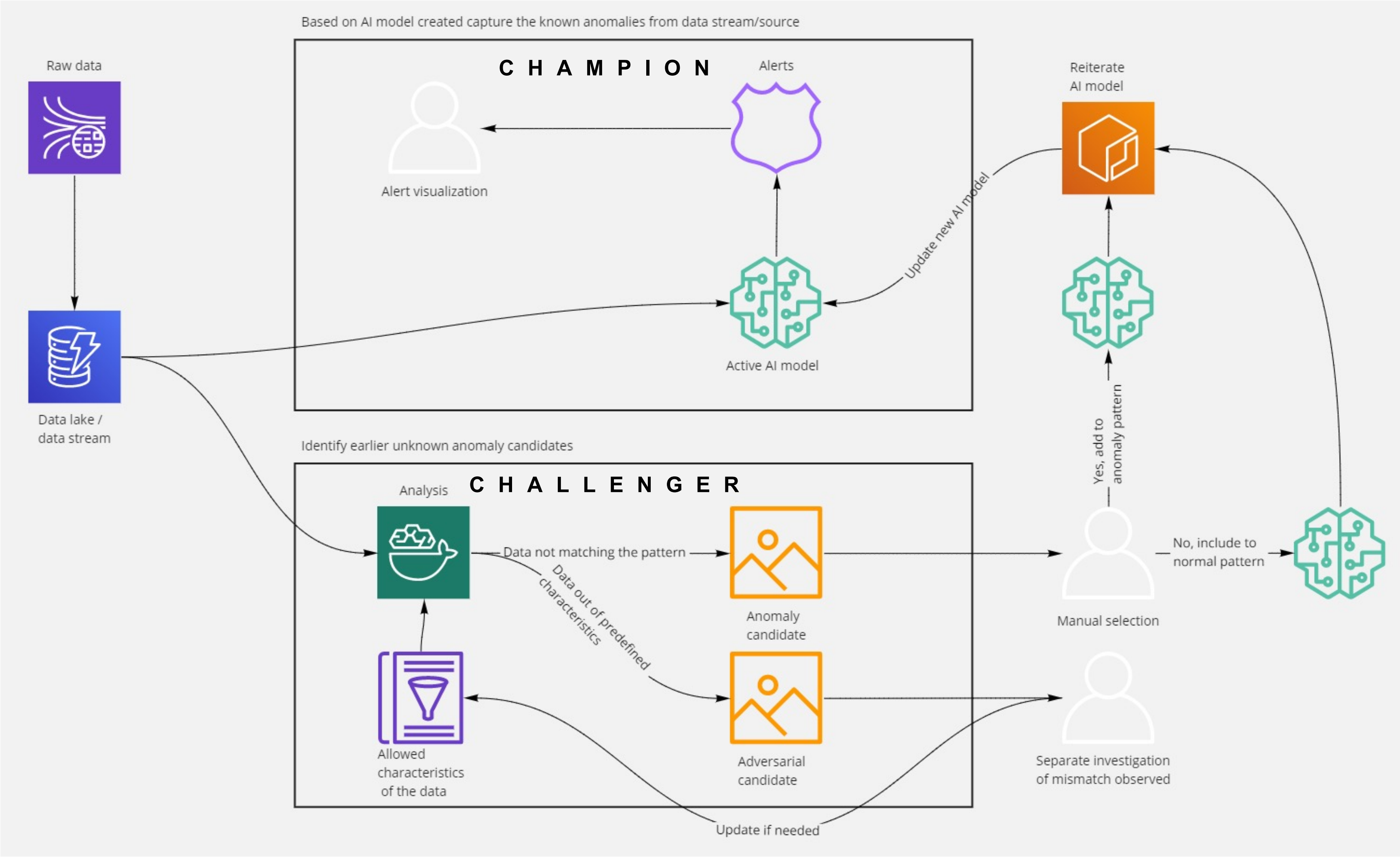
Datamalli
Analytiikkamalli

15/02/2022




Dash
Ei turvallinen | 193.166.161.86:8050
Sovellukset
Kirjautuminen - Re...
intra
opinnot
overleaf-linkit
journaaleja
Valtti - Uniresta
Smarthouse - Food...
Muut kirjanmerkit
Lukulista
$O-AnomalyIndex
5
4
3
2
1
0
200
400
600
800
1000
ORDER_NUMBER
$O-Anomaly=F
ORDER_NUMBER=351
$O-AnomalyIndex=2.304284
$O-Anomaly
F
T
2.95%
F
T
$O-AnomalyIndex
25
20
15
10
5
0
10
20
$O-Anomaly=F
ORDER_NUMBER=10
$O-AnomalyIndex=2.509748

ONE APPROACH: TWO MODELS CONTINUOUSLY DEVELOPING AS NEW DATA BECOMES AVAILABLE WITH MANUAL INTERVENTION CAPABILITY



Based on AI model created capture the known anomalies from data stream/source
CHAMPION
Raw data
Alerts
Alert visualization
Reiterate AI model
Update new AI model
Active AI model
Data lake / data stream
Identify earlier unknown anomaly candidates
Yes, add to anomaly pattern
Analysis
CHALLENGER
Data not matching the pattern
Data out of predefined characteristics
No, include to normal pattern
Anomaly candidate
Manual selection
Allowed characteristics of the data
Adversarial candidate
Separate investigation of mismatch observed
Update if needed

Adversarial part will not be implemented during this project as planned focus is on anomaly detection. It is illustrated here as on optional component to increase robustness of the solution.

NEW MODEL IS VALIDATED WITH DATA, IF IT IS BETTER IT WILL REPLACE THE OLD

HOUSTON ANALYTICS

FINLAND | SWEDEN | ESTONIA | UK | GERMANY

WWW.HOUSTON-ANALYTICS.COM

Antti Syväniemi

CEO
+358 50 387 5971
antti.syvaniemi@houston-analytics.com

HOUSTON
ANALYTICS