Cyber Security Advisory Board meeting - ENTA project
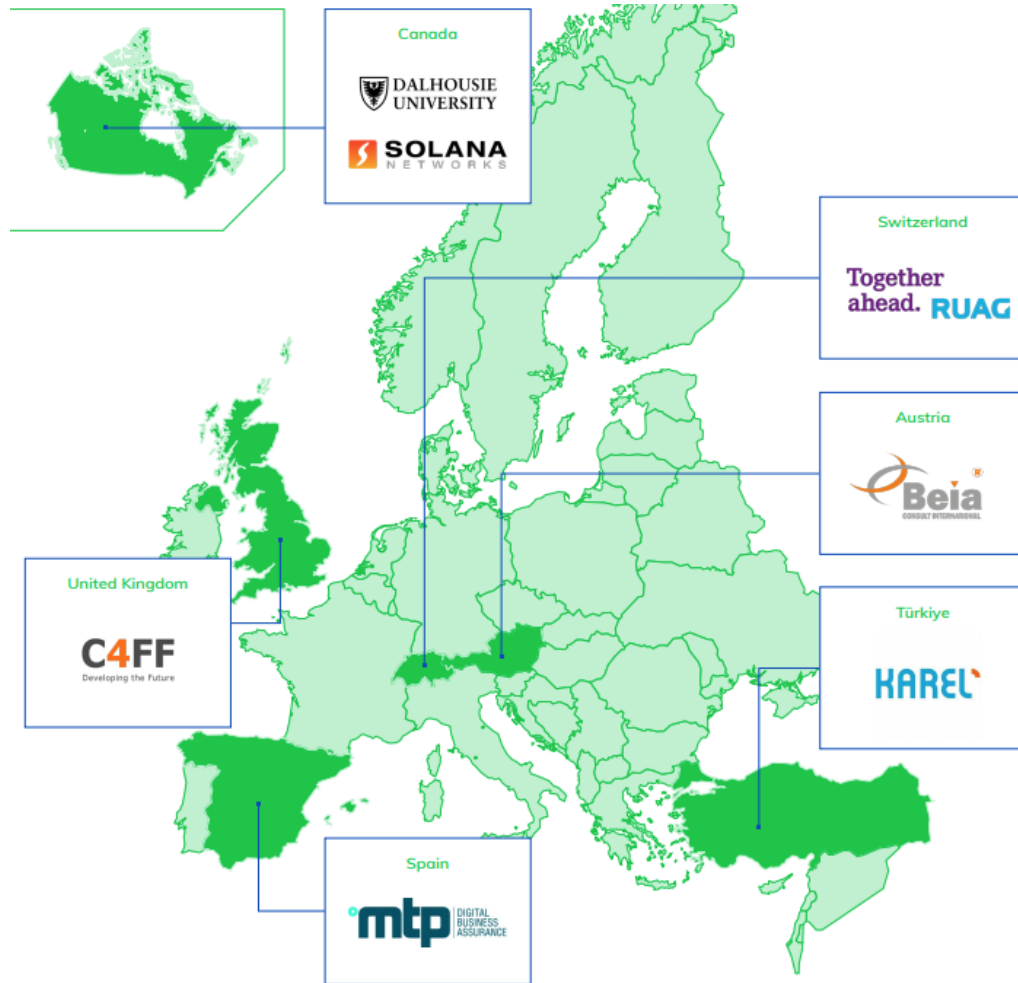
12 December 2023| Online
Luis Redondo

ITEA4

ITEA 4 is the Eureka Cluster on software innovation Σ

Project partners and data

- Start date: October 2021
- End date: March 2025
- Project leader: Solana Networks (Canada)
- Website: https://itea4.org/project/enta.html

Encrypted Network Traffic Analysis for Cyber Security (ENTA) project will provide **visibility** into **encrypted network traffic:**
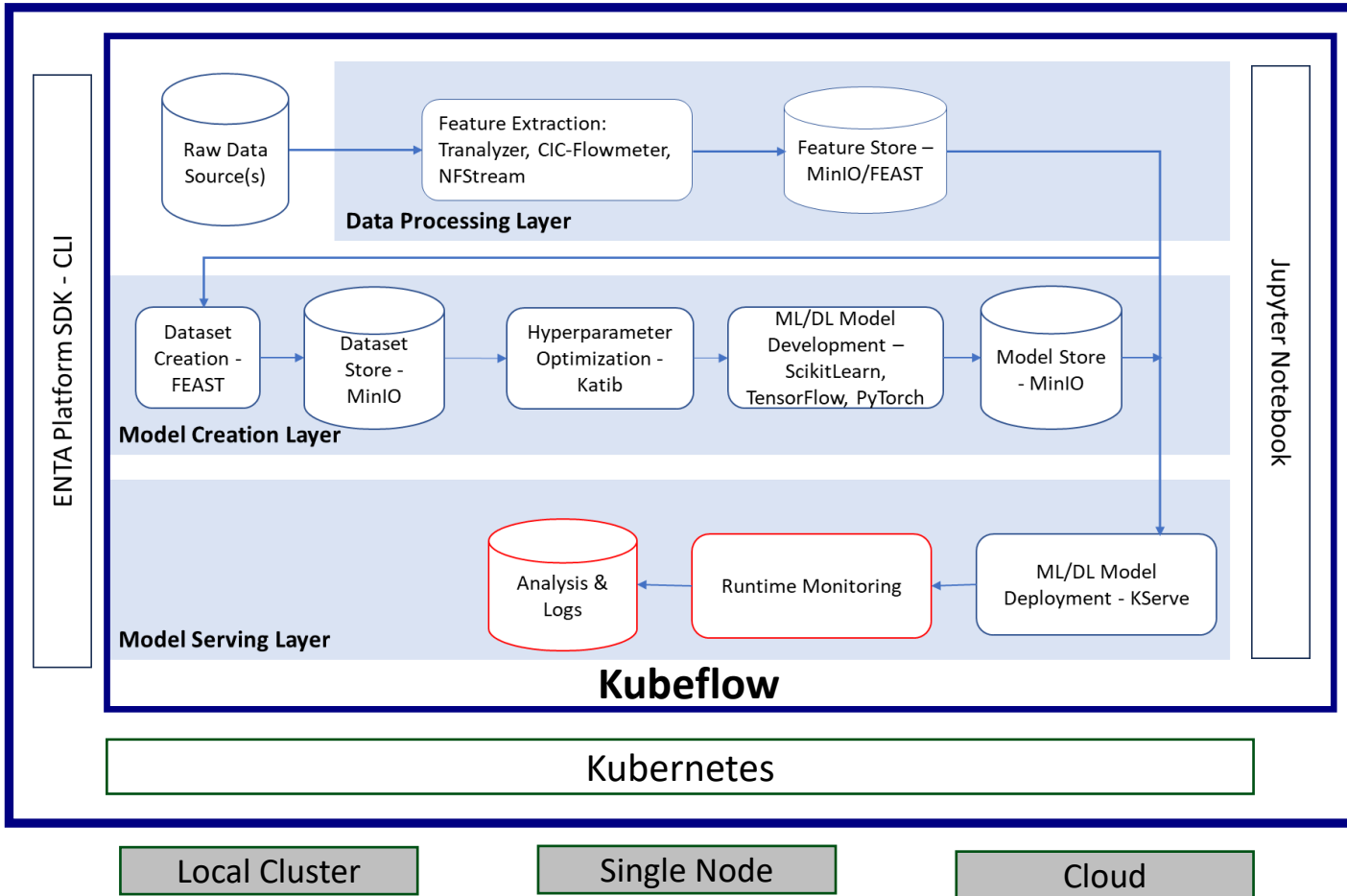- **Classifying encrypted network traffic** (Use Case 1)
- **Protecting IoT networks from cyberattacks** (User Case 2)

Benefits:
- Cybersecurity improved
- Cybercrime costs consequences reduced
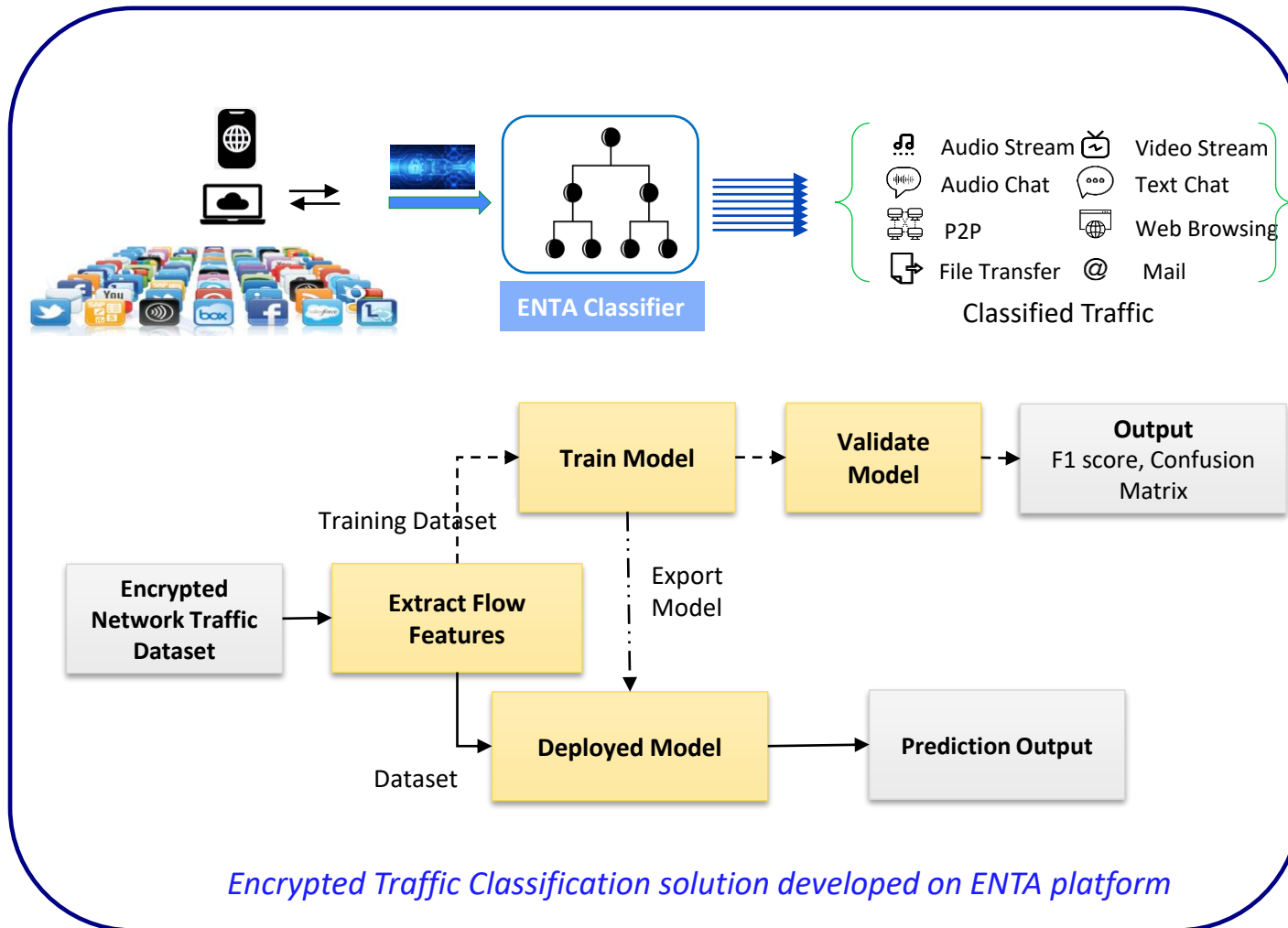- New AI-based cybersecurity business opportunities created**.**

AI Platform to develop network traffic analytics

ENTA Platform

- **Kubeflow** platform is the platform where ENTA platform has been developed
- Supports ML/DL lifecycle for data processing, model creation and deployment with necessary tools to develop ML/DL models
  - Feature extraction – Tranalyzer, NFStream, CIC Flowmeter
  - Object storage – MinIO
  - Dataset creation -- FEAST
  - Model training and optimization - Katib
  - Evaluation
- Supports Tensorflow, PyTorch, XGBoost, Scikit-learn
- Supports Jupyter Notebook
- ENTA SDK enables implementation of use cases
- Off-the-shelf tools can be integrated

Classifying Encrypted Network Traffic

ENTA Classifier

Audio Stream Video Stream
Audio Chat Text Chat
P2P Web Browsing
File Transfer Mail

Classified Traffic

Encrypted Network Traffic Dataset → Extract Flow Features

Training Dataset → Train Model → Validate Model → Output: F1 score, Confusion Matrix

Export Model

Dataset → Deployed Model → Prediction Output

Encrypted Traffic Classification solution developed on ENTA platform

- **Two datasets created**
  - Encrypted OTT applications carrying different traffic types: Video, Audio, File Transfer, Video Chat, Audio Chat and Text
  - Instant Messaging (IM) applications (Telegram, WhatsApp, Teams, Signal, Messenger, Discord) carrying text msgs.
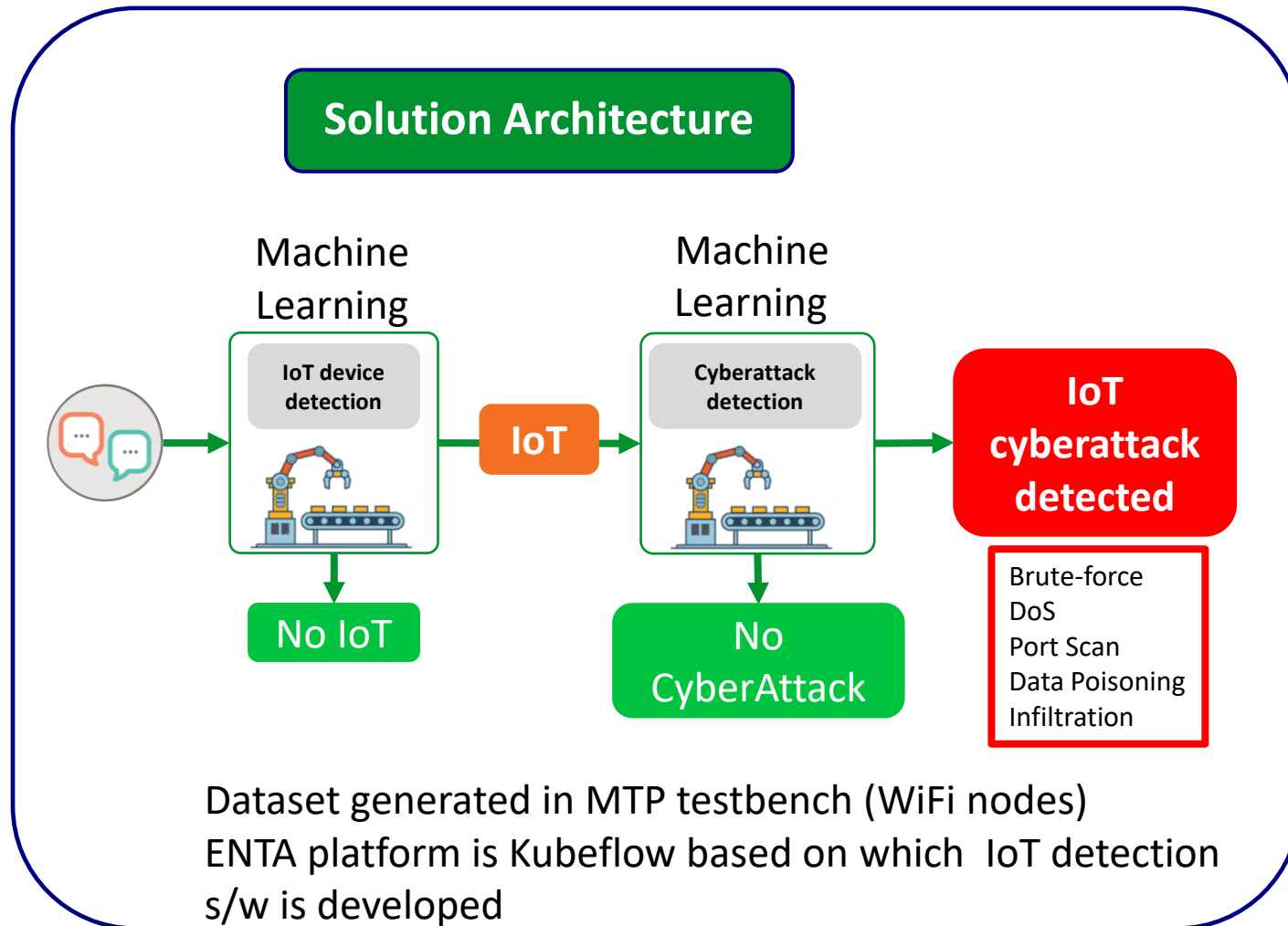- **Classification Results:**
  - OTT traffic types can be identified with F1-score higher than 90% using XGBoost.
  - IM Apps can be classified using Random Forest Classifier -- higher than 95% F1-score.
- **Work in progress:**
  - Models to detect applications with higher accuracy & better discrimination among applications using Deep Learning approach
  - Ability to detect group chats among IM messages

ITEA4 Σ

Protecting IoT networks from cyberattacks

Solution Architecture

Machine Learning

IoT device detection

Machine Learning

Cyberattack detection

IoT

IoT cyberattack detected

No IoT

No CyberAttack

Brute-force
DoS
Port Scan
Data Poisoning
Infiltration

Dataset generated in MTP testbench (WiFi nodes)
ENTA platform is Kubeflow based on which IoT detection s/w is developed

- **Almost 100% cyberattacks detected**
  - Rogue IoT devices
  - Malicious information
- **Real time detection**
- **Applicable in other HW/SW scenarios**
  - PoC in progress for a network of surveillance camera

ITEA4 Σ

Contact details

Biswajit Nandy
Solana Networks – (Canada)
bnandy@solananetworks.com

Luis Redondo
MTP – (Spain)
lredondo@mtp.es

ITEA4
https://itea4.org

ITEA is the Eureka Cluster on software innovation

Σ eureka
https://www.eurekanetwork.org

Thank you