# CitySCAPE
# IDS/IPS engine for CPaaS

Rosella O. Mancilla
Engineering Ingegneria Informatica SpA

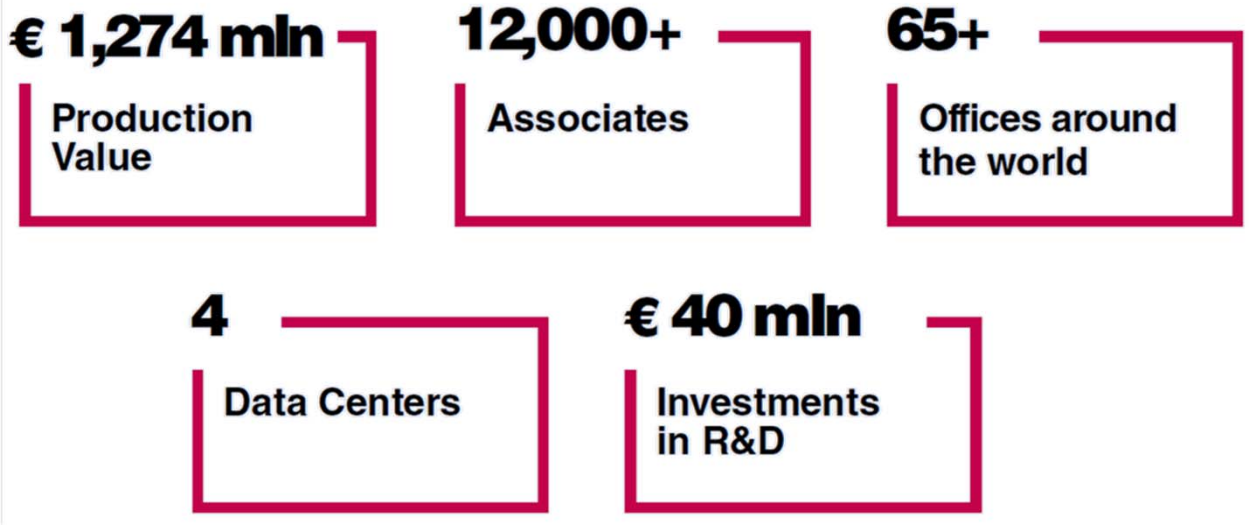
Dec. 15, 2021

# Agenda


- Engineering Ingegneria Informatica
- Anomaly detection
  - The process
- IDS/IPS engine in CPaaS
  - Deployment scenario

# Engineering– Profile

- With around **12,000 professionals** in **65 locations** (in Italy, Belgium, Germany, Norway, Republic of Serbia, Spain, Sweden, Switzerland, Argentina, Brazil and the USA), the Engineering Group **designs, develops and manages innovative solutions** for the business areas where digitalization is having the biggest impact, including Digital Finance, Smart Government & E-Health, Augmented City, Digital Industry, Smart Energy & Utilities, Digital Media & Communication.



# Engineering- Profile


- ENGINEERING implements a highly structured innovation process, in which **Research & Development represents a core pillar**, both as an internal development force of more than **450 researchers** across **5 R&D labs**, and through **partnerships with highly skilled international partners**. This central department of Research & Development has a strong track record in successful participation to European and national projects. With a **significant annual investment in R&D of 40 M€, ENGINEERING plays a leading role in research, by coordinating national and international projects** (with more than 80 on-going projects) and a network of industrial and research partners and universities throughout Europe.

**€ 40 mln**
in annual investments

**70+**
ongoing research projects

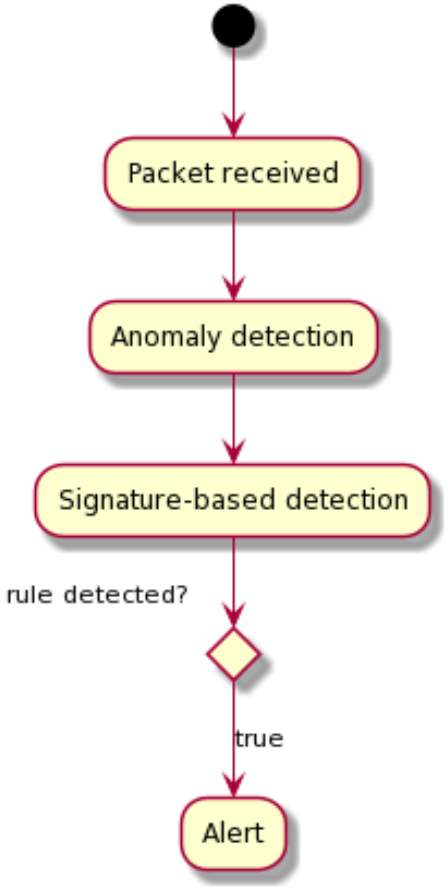
**450+**
researchers and data scientists

**5**
development laboratories

# Engineering- Profile

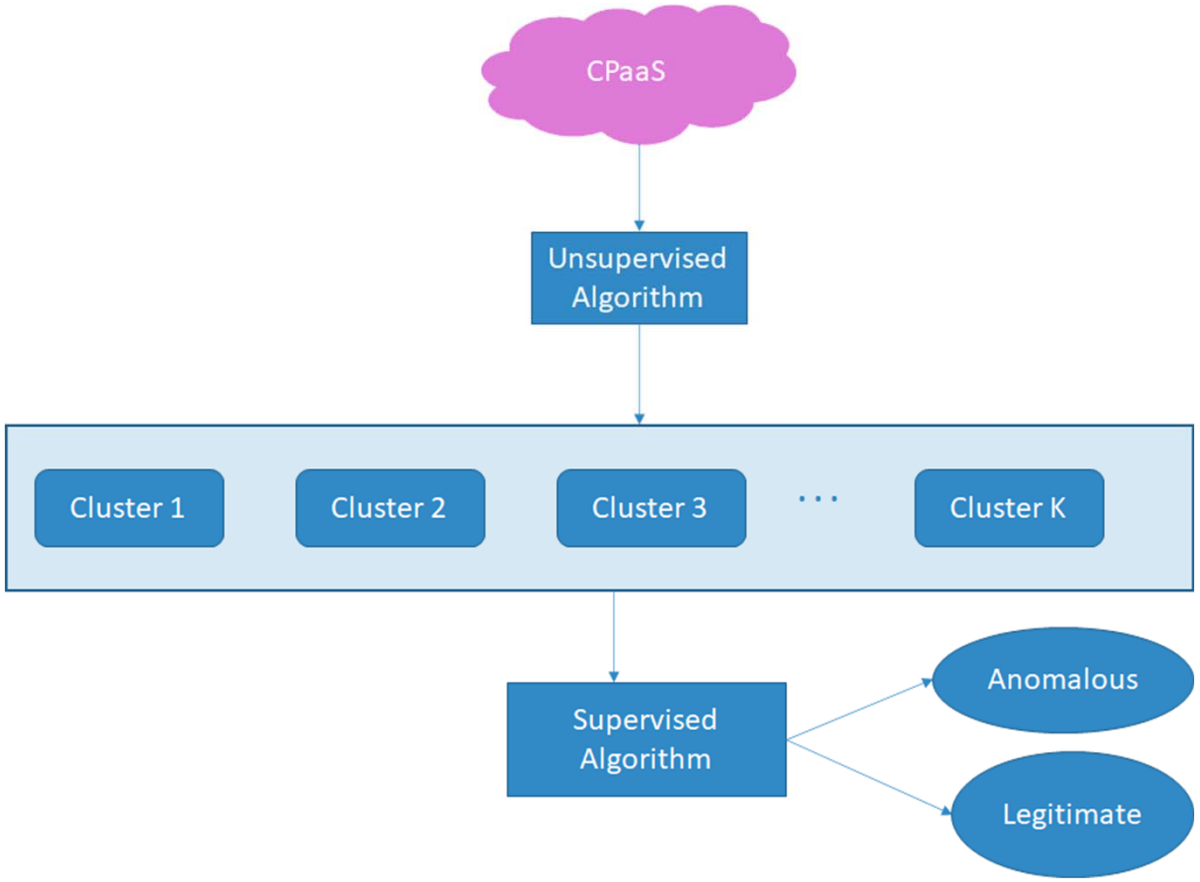
- Rosella O. Mancilla profile:
  - Part of the Research & Development Department of ENG since 2014
  - Part of Cybersecurity team since 2015, involved into:
    - Proposals writing
    - Design, Development, Deployment and integration of assets in national and EU funded projects (such as DOGANA and COMPACT projects)
- ROLE in the Project
  - Leader of T5.4 : design and develop an intrusion detection system for CITYSCAPE - Intrusion detection systems (IDS) and intrusion prevention systems (IPS) constantly watch your network, identifying possible incidents and logging information about them, stopping the incidents, and reporting them to security administrators. In addition, some networks use IDS/IPS for identifying problems with security policies and deterring individuals from violating security policies. IDS/IPS have become a necessary addition to the security infrastructure of most organizations, precisely because they can stop attackers while they are gathering information about your network

# Anomaly detection




- Identify anomalous traffic from legitimate
- Identify malicious traffic
  - Add rule to alert anomalous traffic

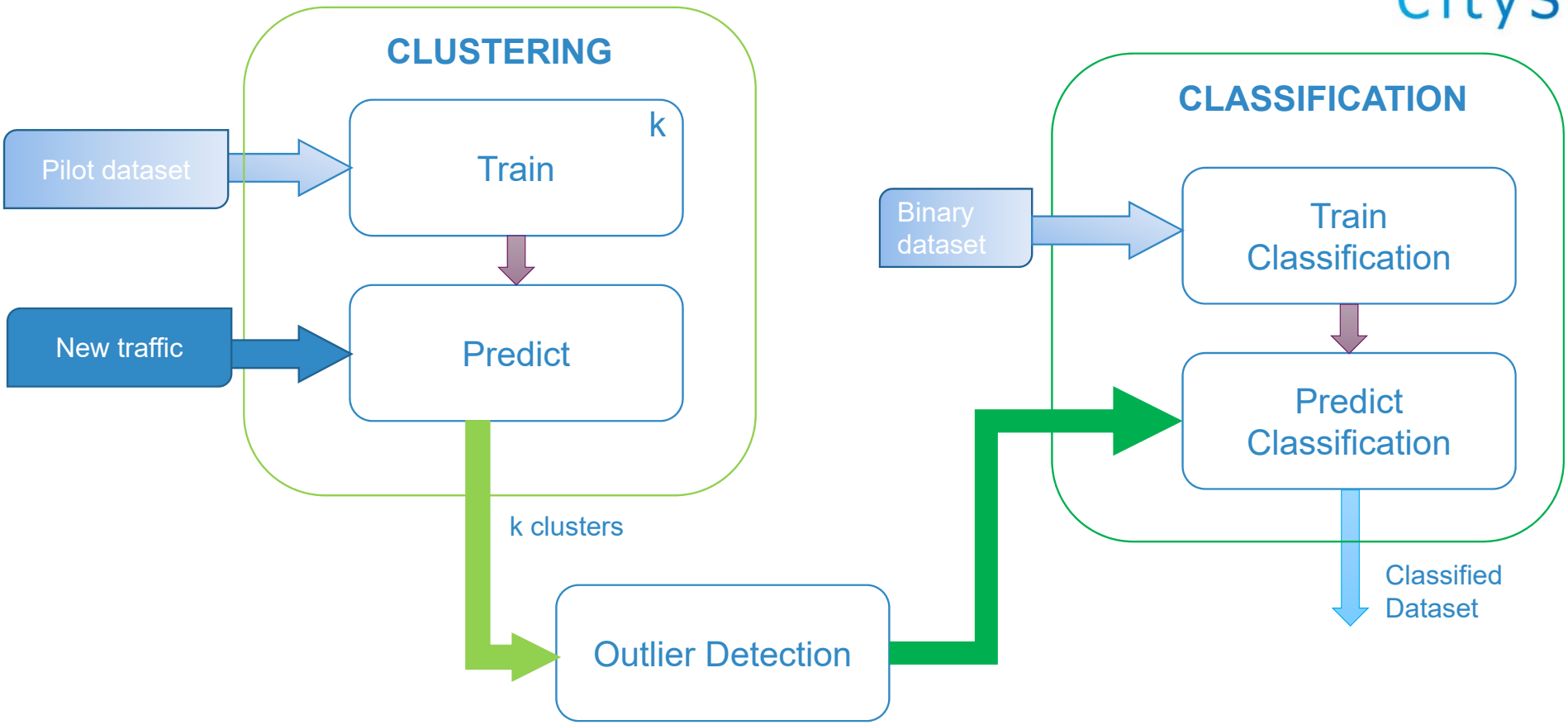
# Anomaly detection: idea



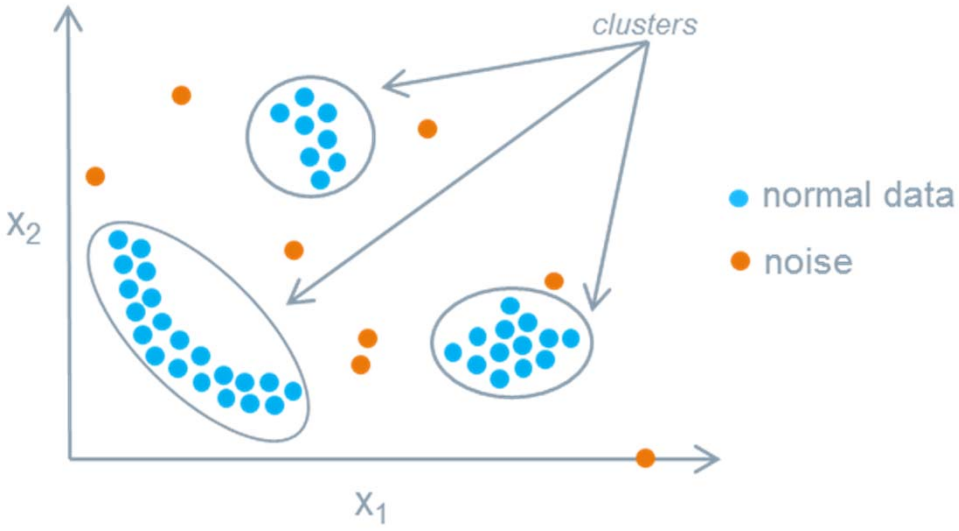

- We do not have a labelled dataset from the Pilot to train the ML algorithms (usually classification)
- anomalous traffic = outlier

❑Datasets
- ✓KDD CUP99
  - HCRL
  - IoT 23
  - Tallin

# Anomaly detection: predict



# Outlier detection



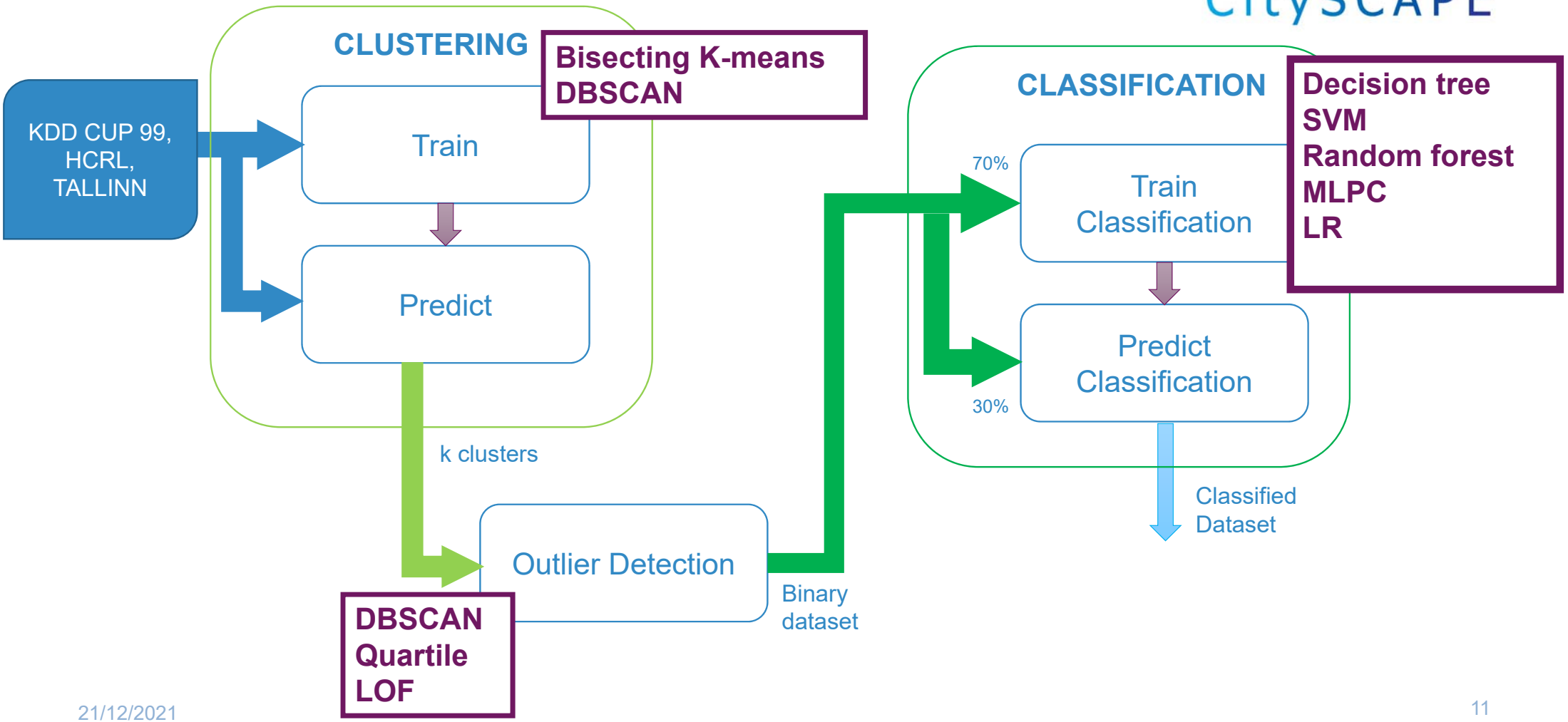

Assumptions

- Distance based techniques
- No normal distribution
- Multivariate dataset (two or more attributes)

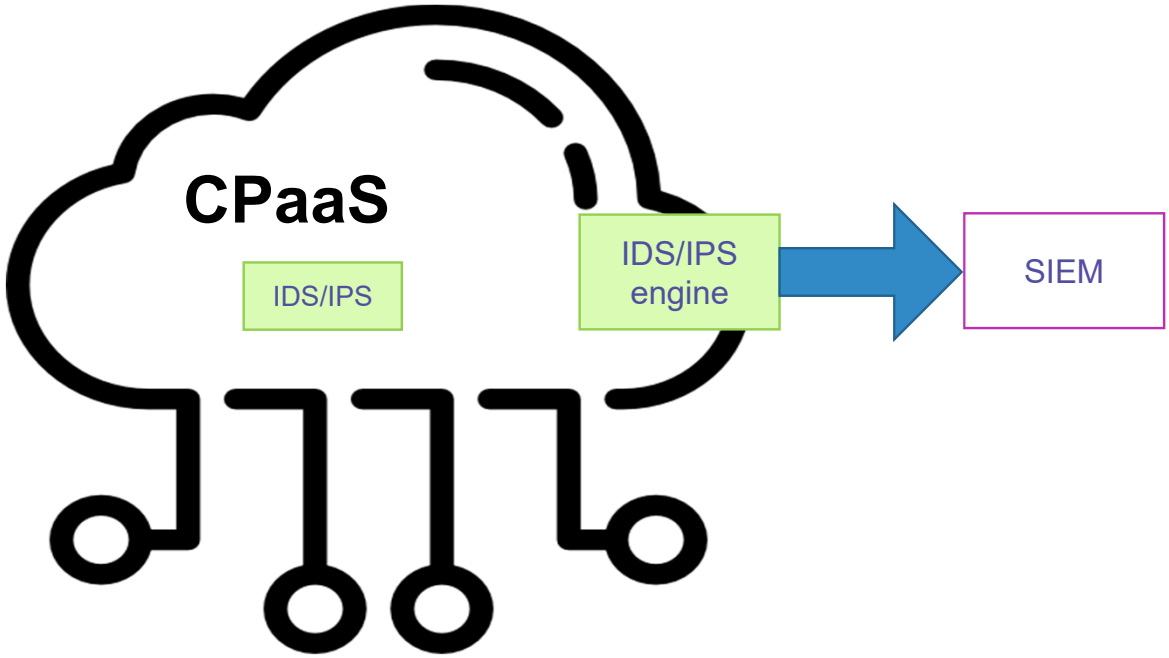
# Classification Accuracy:

| | | | |
|---|---|---|---|
| **CLUSTERING + OULIER DETECTION** | NORMAL | X | ~0 |
| | ANORMAL | ~0 | Y |
| | | NORMAL | ANORMAL |
| | | **CLASSIFICATION** | |

# Anomaly detection: implementation



# IDS/IPS engine Vs CPaaS and SIEM




- Forward events to the public IDS/IPS engine
- Forward events to the SIEM
- Update Anomaly detection model

# Any questions?

# Thank you!

Rosella Omana Mancilla
Engineering Ingegneria Informatica SpA
rosellaomana.mancilla@eng.it

This project has received funding from the EU's Research and Innovation programme Horizon 2020 under grant agreement No 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.