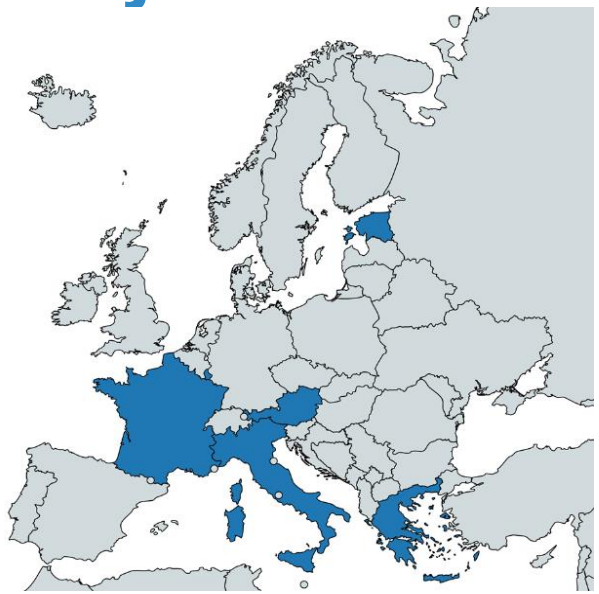
CitySCAPE

Amedeo D’Arcangelo – Kaspersky
Luca Bianconi – Gruppo Sigla
Fabio Podda - AMT

CSET Conference – September 15, 2021

Project at a Glance



- **Call identifier**: H2020-SU-DS-2019
- **Topic**: SU-DS05-2018-2019 - Digital security, privacy, data protection and accountability in critical sectors
- **EC Funding:** 6 293 011,25 €
- **Duration**: 36 months – 1 Sep 2020 → 31 Aug 2023
- **Consortium**: 15 partners
- **Coordinator:** Institute of Communication and Computer Systems (ICSS), Greece – Dr. Angelos Amditis (a.amditis@iccs.gr)
- **Learn more**: www. cityscape-project.eu
- **Join us**: @EUCityscape CitySCAPE Project

Genova Use Case - Some details

Focus on **2 transport scenarios**:

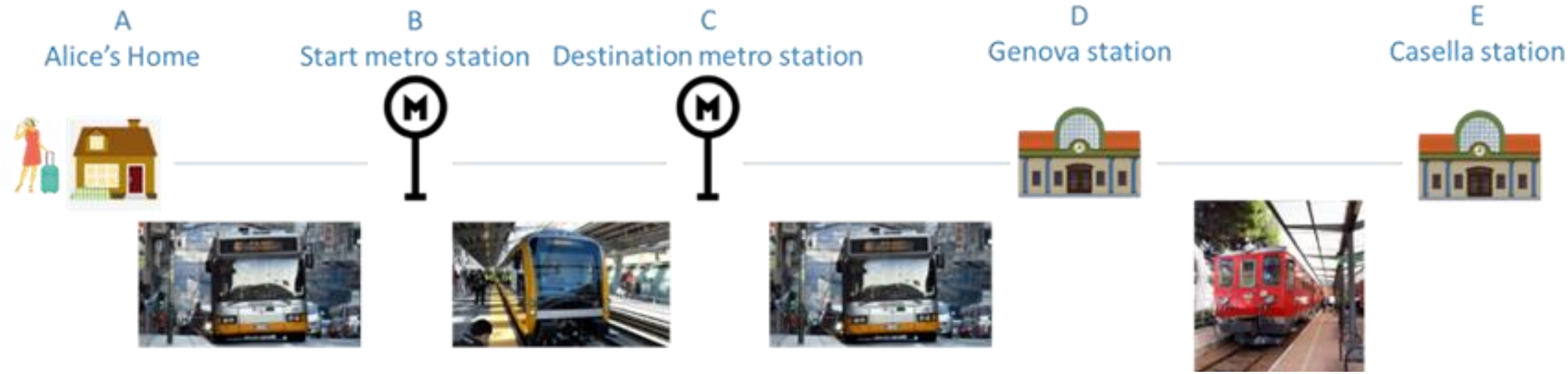
- ✓ **Information to passengers** (*info-mobility*),
- ✓ Electronic and mobile **ticketing**

considering **electronic services** (e.g., website or mobile application) provided to the public transport users

For each scenario several micro-use cases are analyzed addressing very specific situations

- *Info-mobility*
  - ✓ Waiting time at the stop
  - ✓ Service schedule
  - ✓ Waiting time of the next train
  - ✓ Metro Station info-mobility
  - ✓ Notifications to passengers on service update
- *Ticketing*
  - ✓ Ticket from the mobile app
  - ✓ Validating a mobile ticket
  - ✓ Ticketing – City-Pass subscription
  - ✓ Validating a City-Pass subscription ticket
  - ✓ Ticketing Using Urban Train

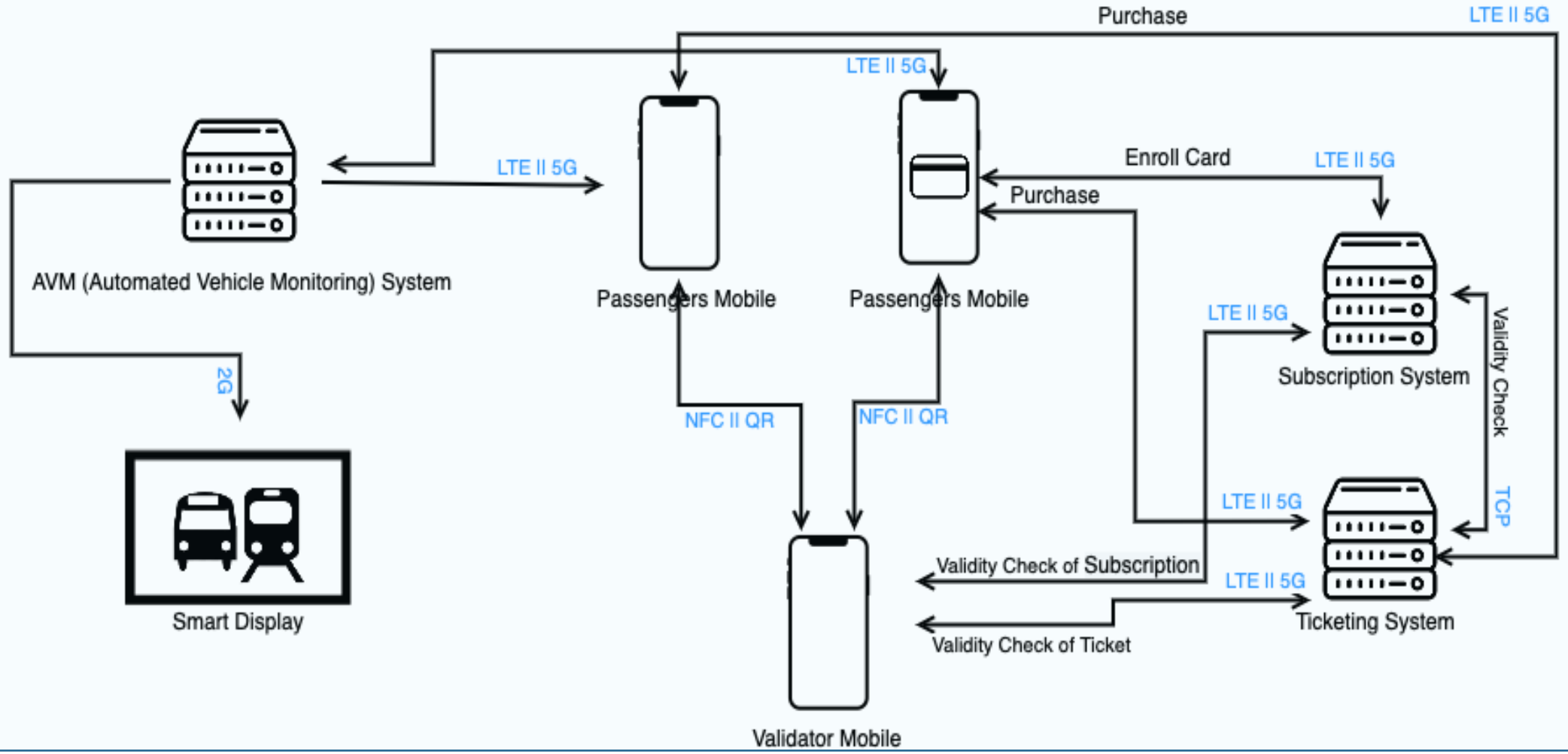
Genova Use Case - Some more details



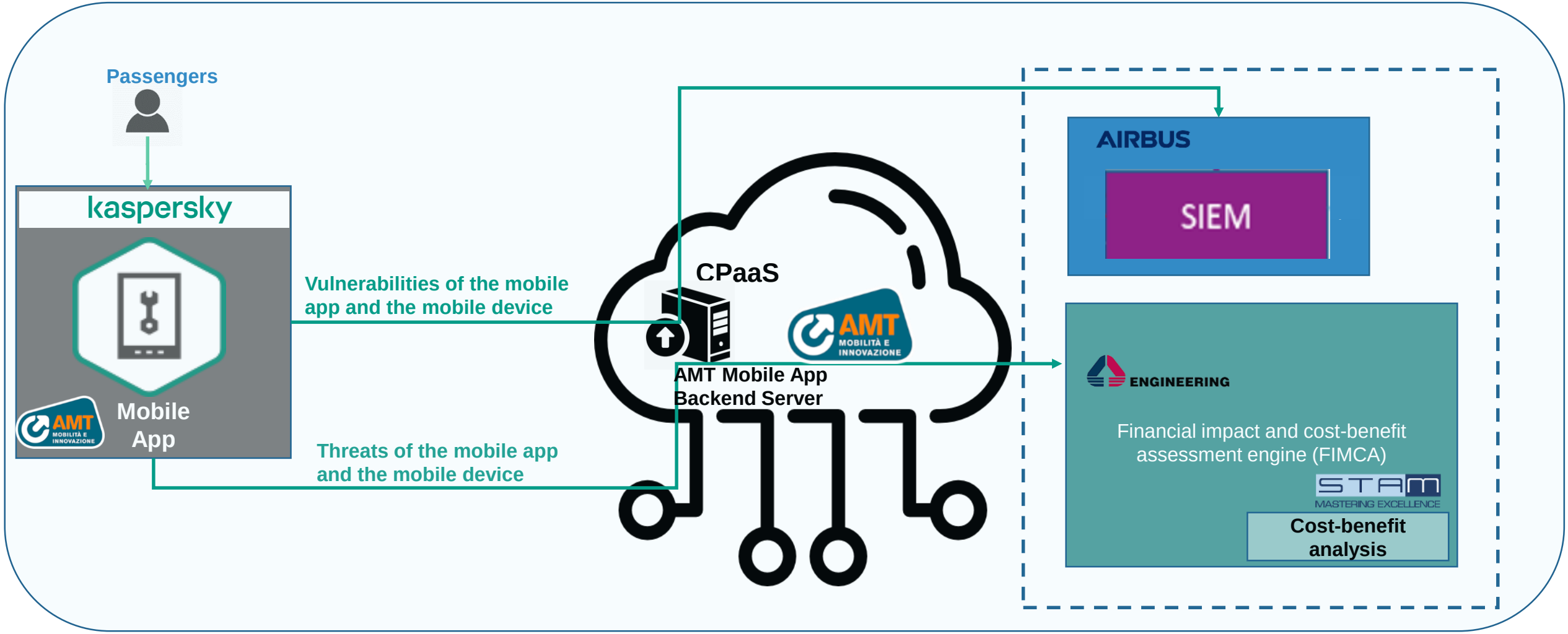
2 macro-scenarios combining all the micro-use cases

1. All the steps for the transport of a passenger **from their home in Genoa to Casella** using public transportation
2. **Re-plan scenario** – during her trip, an event of a "technical problem" disrupts the provided service, so the passenger has to reschedule and re-arrange paths

Use case infrastructure
High-level Architecture



Kaspersky Mobile Security SDK and the AMT Genova Mobile App



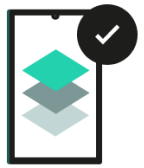
KMS – SDK for iOS & Android
Integrating security measures in the AMT mobile apps

CitySCAPE

Assessing device

Protecting device

Securing connection



Securing data

Protecting apps

Risk Detection

- ✓ Root detector.
- ✓ Insecure settings detector.
- ✓ Unknown apps detector.*
- ✓ Malicious apps detector.*

Device Protection

- ✓ On-Access scanner*.

Web & Network Protection

- ✓ DNS spoofing checker.
- ✓ Certificate Validation.
- ✓ Wi-Fi Safety Analysis.
- ✓ Website reputation analysis.

Data Protection

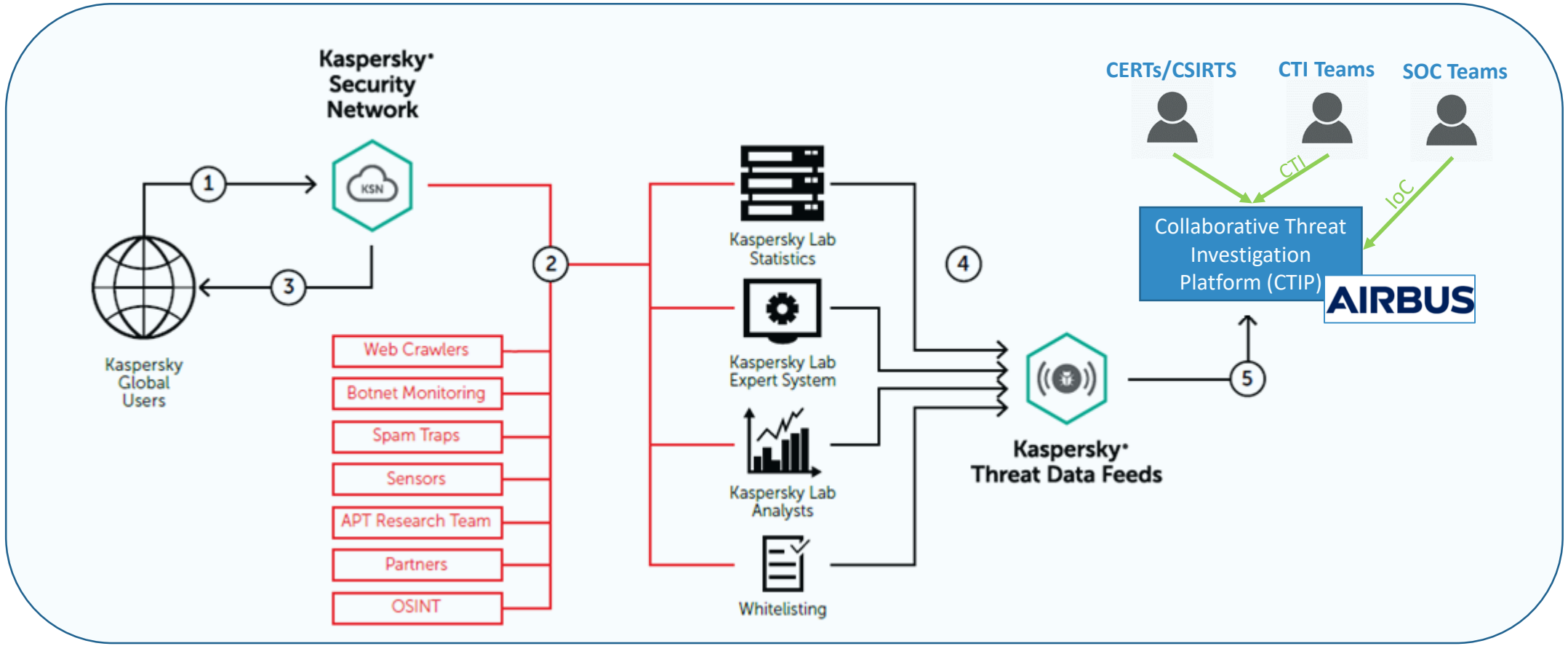
- ✓ Secure Input technology vs Keyloggers.
- ✓ Secure storage for sensitive data.

Self Defense

- ✓ Protection from 3rd party exploitation*.
- ✓ Method implementation replacement detector*.
- ✓ Digital signature verification*.
- ✓ Debugging detection*.

* Feature available only for Android

Kaspersky Threat Data Feeds and the CitySCAPE Collaborative Threat Investigation Platform (CTIP)



Kaspersky CyberSafety Management Games

Target Audience

- ✓ Onsite edition:
  - ✓ AMT administrative area employees.
  - ✓ AMT operational area employees.
- ✓ On-line edition:
  - ✓ More than 50 regular passengers (Genoa + Tallinn).

CitySCAPE

kaspersky

Training for Genova Use Case

CitySCAPE

kaspersky

Training employees to:

- ✓ **Prevent success of attackers** because one click is all it takes to overcome hardware and software defenses
- ✓ **Shape an organization into one where employees are part of the defense strategies**
- ✓ **Protect business** (brand image and services)

Expectations

- ✓ **Prevent attacks to critical IT infrastructures and assets via an integrated risk assessment**
- ✓ **Defend organization against novel cyber attacks by recognize them on time**
- ✓ **Improve the cybersecurity awareness of the company employees**
- ✓ **Prevent fraud on ticketing by using innovative solutions both on the IT infrastructure and on the mobile phone**

Any questions?

Thank you!

Amedeo D’Arcangelo

Luca Bianconi

Fabio Podda

amedeo.darcangelo@kaspersky.com
luca.bianconi@grupposigla.it
fabio.podda@amt.genova.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.