CitySCAPE

The European project CitySCAPE on cyber-security for multi-modal transport systems

Francesca Giampaolo – Engineering

Amedeo D'Arcangelo – Kaspersky

Luca Bianconi – Gruppo Sigla

EuroCyberSec 2021 Workshop – 25-26 October 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

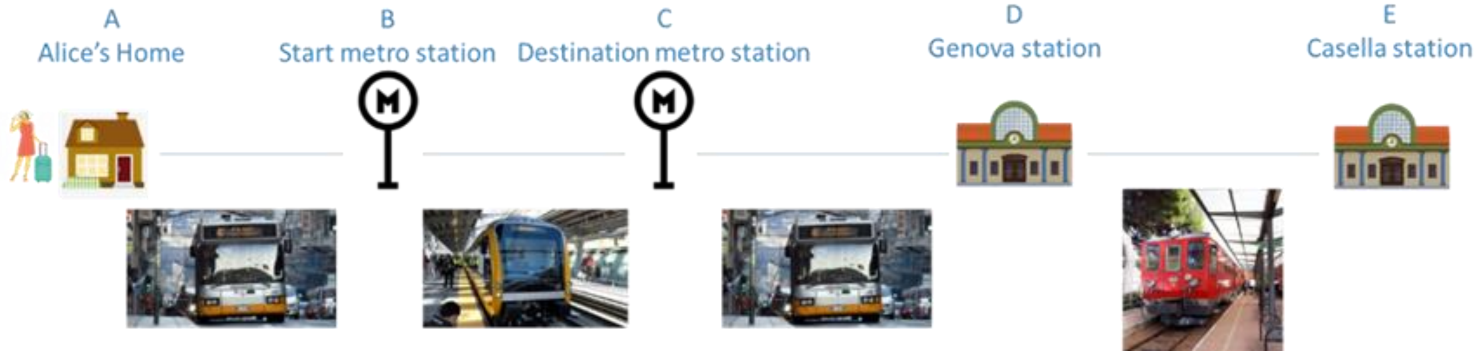
Focus on **2 transport scenarios**:

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

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

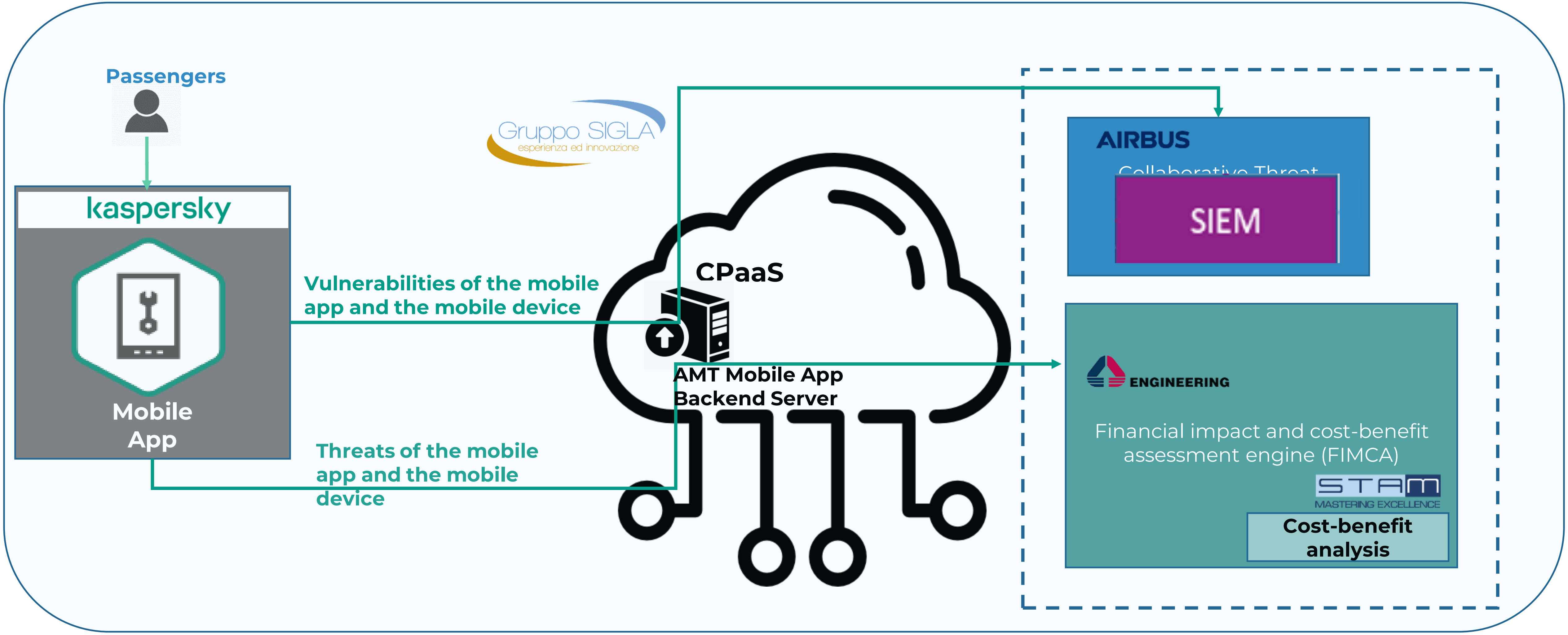
For each scenario several micro-use cases are analyzed addressing very specific situations

- ○ ***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



Kaspersky Mobile Security SDK and Genova Mobile App

CitySCAPE



Passengers

kaspersky

Mobile App

Vulnerabilities of the mobile app and the mobile device

Threats of the mobile app and the mobile device

Gruppo SIGLA
esperienza ed innovazione

CPaaS

AMT Mobile App Backend Server

AIRBUS

Collaborative Threat

SIEM

ENGINEERING

Financial impact and cost-benefit assessment engine (FIMCA)

STAM
MASTERING EXCELLENCE

Cost-benefit analysis

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

CitySCAPE

Assessing device

Risk Detection

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

Protecting device

Device Protection

- ✓ On-Access scanner*.

Securing connection

Web & Network Protection

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

Securing data

Data Protection

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

Protecting apps

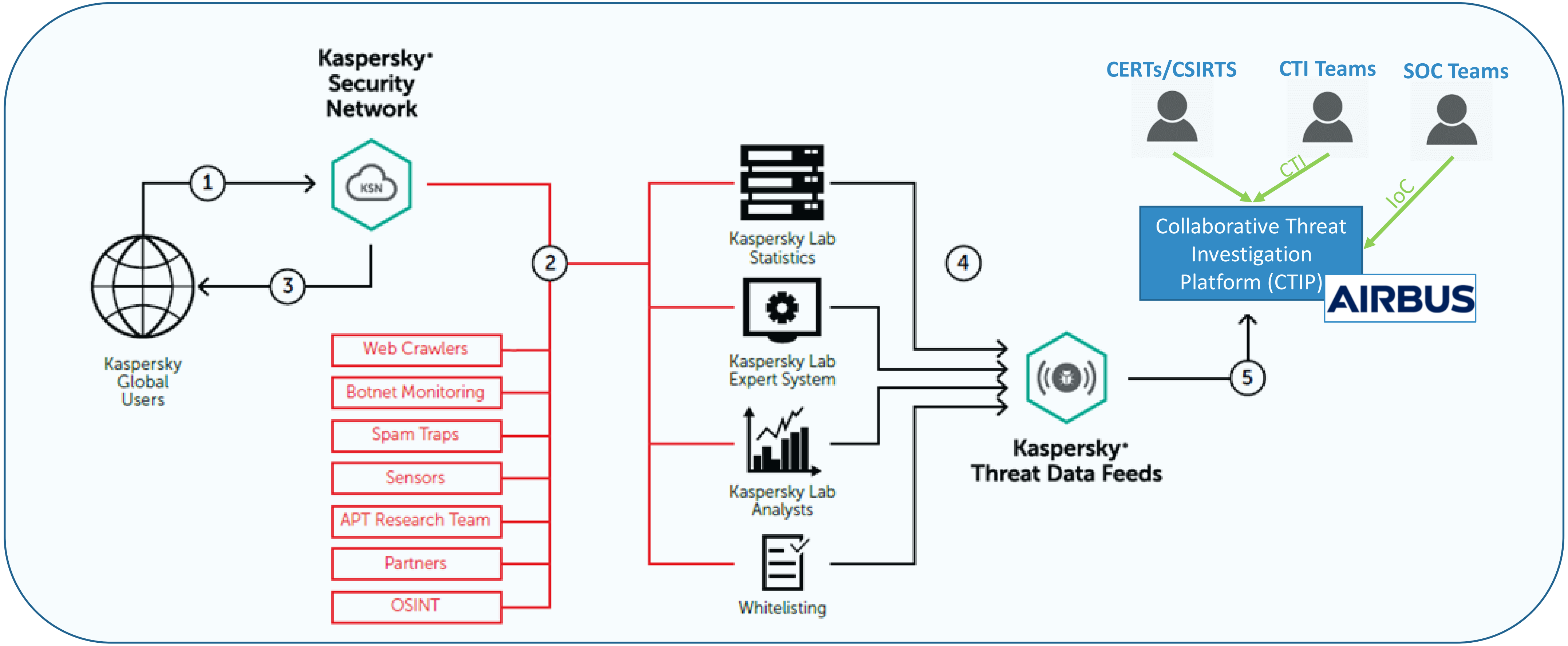
Self Defense

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

* Feature available only for Android

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

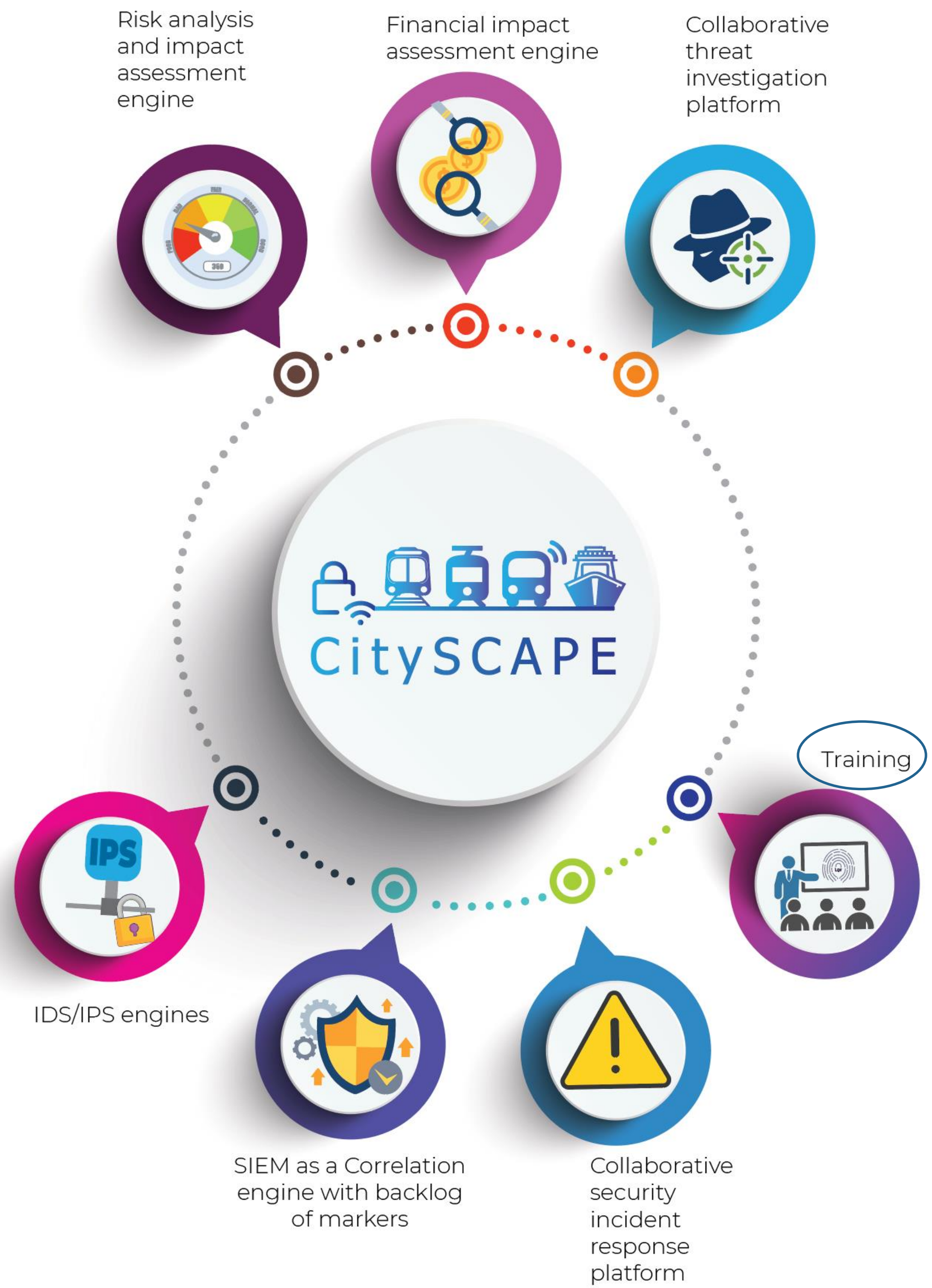
CitySCAPE



Kaspersky CyberSafety Managemer Games

Target Audience

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



Risk analysis and impact assessment engine

Financial impact assessment engine

Collaborative threat investigation platform

CitySCAPE

Training

Collaborative security incident response platform

SIEM as a Correlation engine with backlog of markers

IDS/IPS engines

CitySCAPE

kaspersky

FIMCA component

- The first step is to **identify critical assets** (*tangible* and *intangible*) to evaluate and determine the scope of the assessment. This will allow to prioritize which assets to assess.
  For the evaluation of the intangible assets the system will suggest how to proceed to **define the cost** associated to the asset.

- The **Montecarlo Simulation** will support the **calculation of the medium cost** that will occur in case of an attack that compromise one or more assets.

- We have now determined the **value of the asset** in case of compromission.

  Now we have to **calculate how much we could spend to protect it**.

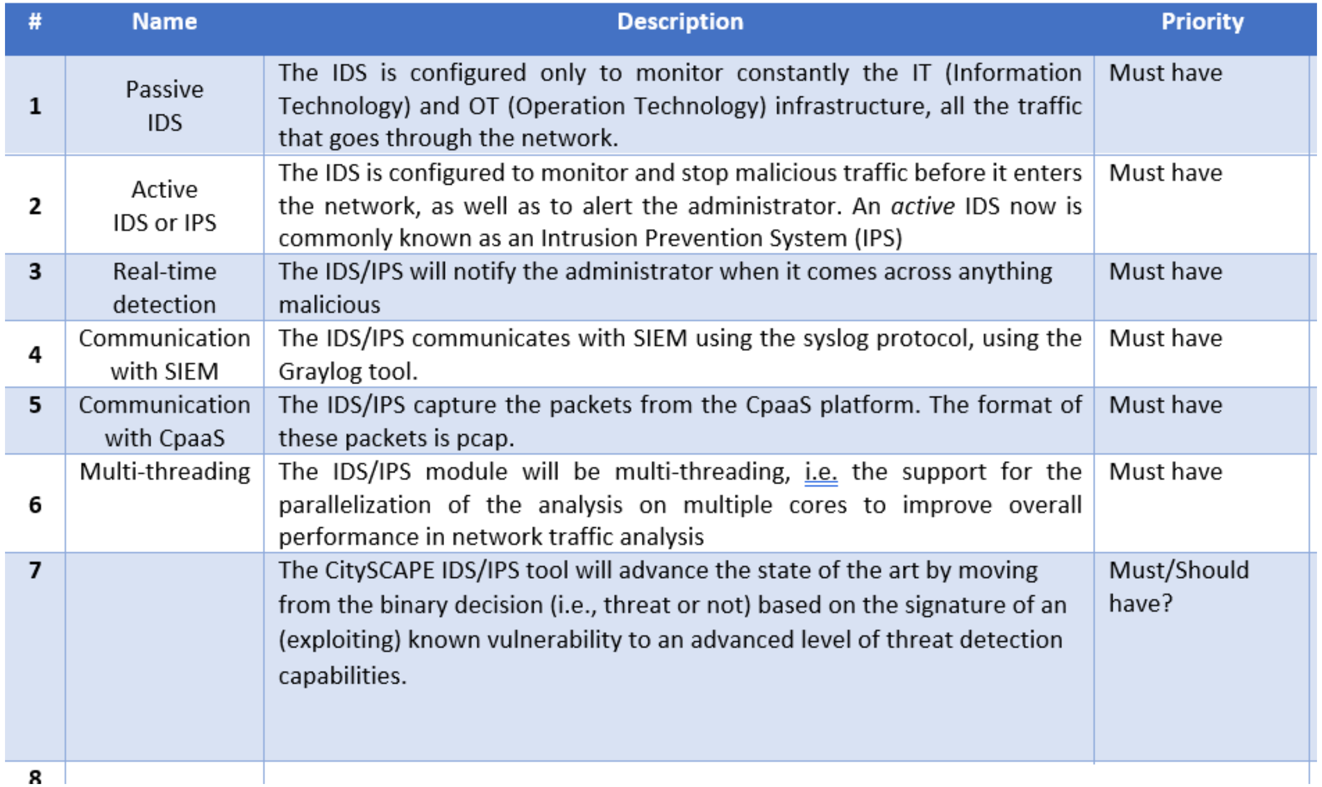
  We will refer to the CIS Controls to set up a **list of countermeasure** related to a specific asset and to a specific phase of NIST. The quantitative evaluation of the **return on investment** in safety is calculated by how much loss you have avoided thanks to your investment.

$$ROSI = \frac{ALE - mALE - Cost\ of\ the\ solution}{Cost\ of\ the\ solution}$$

IDS/IPS component

- The objective is to develop the **IDS/IPS module** that will support cybersecurity experts in the **analysis of all the events and anomalies on the network**, detect any potential incident, evaluate the situation and put in place the **most appropriate** (risk-based) **reaction**.

  The IDS/IPS module will be able to **monitor constantly** the **IT** (Information Technology) and **OT** (Operational Technology) **infrastructures**



#	Name	Description	Priority
1	Passive IDS	The IDS is configured only to monitor constantly the IT (Information Technology) and OT (Operation Technology) infrastructure, all the traffic that goes through the network.	Must have
2	Active IDS or IPS	The IDS is configured to monitor and stop malicious traffic before it enters the network, as well as to alert the administrator. An *active* IDS now is commonly known as an Intrusion Prevention System (IPS)	Must have
3	Real-time detection	The IDS/IPS will notify the administrator when it comes across anything malicious	Must have
4	Communication with SIEM	The IDS/IPS communicates with SIEM using the syslog protocol, using the Graylog tool.	Must have
5	Communication with CpaaS	The IDS/IPS capture the packets from the CpaaS platform. The format of these packets is pcap.	Must have
6	Multi-threading	The IDS/IPS module will be multi-threading, i.e. the support for the parallelization of the analysis on multiple cores to improve overall performance in network traffic analysis	Must have
7		The CitySCAPE IDS/IPS tool will advance the state of the art by moving from the binary decision (i.e., threat or not) based on the signature of an (exploiting) known vulnerability to an advanced level of threat detection capabilities.	Must/Should have?
8			

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

Other work in progress

CitySCAPE

Name	Project Description
Truth Seekers Chain	designs methodology to tackle spread of fake news and tampered contents
Dogana ADVANCED SOCIAL ENGINEERING AND VULNERABILITY ASSESSMENT FRAMEWORK	framework that delivers "aDvanced sOcial enGineering And vulNerability Assessment“
COMPACT CYBERSECURITY FOR PUBLIC ADMINISTRATIONS	effective tools and services for removing security bottlenecks for Public Administrations
Hermeneut	methodology based on cost-benefit analysis to assess the vulnerability of their tangible and intangible assets

Name	Project Description
Cyber Security for Europe	testing and demonstrating potential governance structures for Network of Competence Centres
PrOTectMe	creates a targeted start-up offering B2B cyber-risk management services to Medium Enterprises
GEIGER	help SMEs and entrepreneurs to become aware of and reducing risks related to data protection, privacy, and cybersecurity
TRAPEZE	develop technologies to empower citizens to actively contribute to the cyber resilience of the common European data space

Any questions?

Thank you!

Francesca Giampaolo
Amedeo D'Arcangelo
Luca Bianconi

✉ francesca.giampaolo@eng.it
amedeo.darcangelo@kaspersky.com
luca.bianconi@grupposigla.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.