

1st CitySCAPE Pilot Demonstration

Main Goals Achieved:

- to improve confidence of efficient handling of day-one and specific attacks
- to minimize security risks introduced by (less security-aware) external service providers and the risks to personal privacy related to fraud prevention and new ticketing services
- to improve the fraud prediction caused by recent EU FinTech market opening directives and technological advancements

Pilot Facts:

- ▶ Tallinn, Estonia
- ▶ Duration: 2 months
- ▶ AV Shuttle network
- ▶ Five scenarios realized in real conditions
- ▶ Eight training sessions for CERT's, CSIRT's and non IT professionals

Risk analysis and impact assessment engine

Financial impact assessment engine

Collaborative threat investigation platform



IDS/IPS engines

Training

SIEM as a Correlation engine with backlog of markers

Collaborative security incident response platform



 @EUCityscape

 CitySCAPE Project

www.cityscape-project.eu

2nd CitySCAPE Pilot Demonstration

Main Goals Achieved:

- to validate all the CitySCAPE tools developed throughout the project among a precise set of scenarios that involved the two major topics of the pilot: information to passengers and digital ticketing
- to involve AMT mobile application, together with all the info mobility and ticketing infrastructure in the testing scenarios

Pilot Facts:

- ▶ Genova, Italy
- ▶ Duration: 4 months
- ▶ Public transport network
- ▶ Five scenarios realized in real conditions
- ▶ Main focus: Information to passengers & digital ticketing
- ▶ Training sessions for CERTs and CSIRTs
- ▶ Public demonstration sessions with: universities, schools, citizens & passengers, institutions & stakeholders, end-users



About CitySCAPE Project

CitySCAPE is a project funded by the EU's Horizon 2020 research and innovation program, which comprises 15 partners Europe, united in their vision to cover the cybersecurity needs of the multimodal transportation.

The traditional security controls and security assurance arguments are becoming increasingly inefficient in supporting the emerging needs and applications of the interconnecting transport systems, allowing threats and security incidents to disturb all dimensions of transportation

The CitySCAPE software toolkit will:

- ✓ Detect suspicious traffic-data values and identify persistent threats
- ✓ Evaluate an attack's impact in both technical and financial terms
- ✓ Combine external knowledge and internally observed activities to enhance the predictability of zero-day attacks
- ✓ Instantiate a networked overlay to circulate informative notifications to CERT/CSIRT authorities and support their interplay.

Project Facts

- **Duration:**
36 months
(September 2020-August 2023)
- **Call identifier:**
H2020-SU-DS-2019
- **Topic:**
SU-DS05-2018-2019
Digital security, privacy, data protection and accountability in critical sectors
- **Pilots:** Tallinn, Estonia / Genova, Italy
- **Project Coordinator:**
Dr Angelos Amditis,
Institute of Communication and Computer Systems (ICCS)
a.amditis@iccs.gr



"This work is a part of the CitySCAPE project. This project has received funding from the European Union's Horizon 2020 research and innovation programme 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."

Get Connected

 @EUCityscape

 CitySCAPE Project

www.cityscape-project.eu

Consortium



www.cityscape-project.eu



 @EUCityscape  CitySCAPE Project