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.

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

1st CitySCAPE Pilot Demonstration

- 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

2nd CitySCAPE Pilot Demonstration

- 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

Risk analysis and impact assessment engine

Collaborative threat investigation platform

Training

Financial impact assessment engine

IDS/IPS engines

SIEM as a correlation engine with backlog of markers

Collaborative security incident response platform

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.