

What is CitySCAPE About?

The Challenge

The traditional security controls and security assurance arguments are becoming increasingly inefficient in supporting the emerging needs and applications of the multimodal transport systems, allowing threats and security incidents to disturb all dimensions of transportation. Therefore, the enormous potential of the multimodal ecosystem, namely a more efficient transportation, which lies on the extent to which it globally remains cyber-secure, is becoming vulnerable.

The CitySCAPE Solution

CitySCAPE introduces innovative risk analysis techniques and orchestrates a number of software solutions to realize an interoperable toolkit that seamlessly integrates to any multimodal transport system.

More specifically, 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.

CitySCAPE At a Glance

Consortium



AIRBUS



kaspersky



Project Facts

Duration: 36 months
(September 2020-
August 2023)

EU funding: 4 998 057.88€

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



Get Connected

@EUCityscape CitySCAPE Project

www.cityscape-project.eu

Objectives

- **Enhance** cybersecurity technologies in the multimodal passenger transportation ecosystem at city-level addressing users and data privacy concerns.
- **Introduce** risk analysis tools to identify threats and their propagation mechanism focusing on transport/digital infrastructure but also relevant in other NIS Directive critical sectors and assess the impact of a potential attack.
- **Improve** the proactive approach of handling cybersecurity challenges and actively contribute to the predictability of threats in (regional) multimodal transport systems
- **Enhance** end-user engagement towards the definition and provision of multimodal passenger transport requirements about digital security, privacy and personal data protection.
- **Further** strengthen the role of CERTs/CSIRTs by providing them with direct/real-time informative notifications about observed cybersecurity incidents and facilitate the collaborative investigation of incidents in line with the NIS Directive.
- **Significantly** contribute to multimodal transport standards and gain experimental evidence on the feasibility of security labelling in city-level multimodal transport.
- **Showcase** and validate the CitySCAPE solution efficiency in large scale pilot demonstrators involving all relevant entities and digital infrastructure of transport providers, under use cases of interest
- **Analyse** and outreach the multimodal transport security market to maximize the CitySCAPE footprint and exploitation.



Expected Impact

- **CitySCAPE** will offer the concrete technical basis for a unique opportunity of an efficient collaborative threat investigation among a broad set of CERTs/CSIRTs by introducing a platform capable of sharing information coming from different sources and therefore achieve the maximization of the CSIRT network added value.
- **CitySCAPE** toolkit capabilities will allow an accurate identification of so-far under-explored/hidden privacy risks serving the in-depth application of privacy-by-default principle and GDPR regulation in all city-level transportation stakeholders.
- **CitySCAPE** will introduce and validate an agile concept of a standalone interoperable solution to manage current cybersecurity/privacy risks across complex interconnected infrastructures.
- **CitySCAPE** will estimate the attack impact on both technology and financial terms that will drive a cost-benefit analysis on potential further investments to cybersecurity and privacy countermeasures.
- The **CitySCAPE** solution will address related security issues of mobile devices, increasing passengers' safety in city-level transport.
- The **CitySCAPE** toolkit will identify and track the potential path of a cyber-attack across the whole multimodal transport chain showcasing how an attack may unexpectedly affect modules that are not directly connected to its entry point.
- The **CitySCAPE** capability of collaborative threat investigation will immediately strengthen the CERTs/CSIRTs link to the transportation stakeholders.
- **CitySCAPE** will promote best practices in cybersecurity management solutions to the multimodal transport community and through training of security experts will seek to communicate their value and thus, increase their acceptance.
- **CitySCAPE** standardization will fill the gap in security labelling showcasing the solid basis of a mature EU market and rendering the compliance to standards a clear path for commercial growth.