CYBERSECURITY

City-level cyber-secure multimodal transport ecosystem
Cyber safe transport within the European Union

What is the project?

CitySCAPE

- Digitalisation has led to the transport sector becoming increasingly interconnected. Most of the time, transport services are centralised. However, these interconnections increases the vulnerability to cyber-attacks. **CitySCAPE will improve cyber security within multimodal transport**. The project will produce a modular software toolkit with the following purposes:
  1. **To enforce prediction of zero-day attacks**
  2. **To detect suspicious traffic and data flows**
  3. **To evaluate the technical and financial impact of a cyber-attack**
  4. **To train relevant authorities and improve the circulation of information among them**

- The CitySCAPE solution will eventualy be validated in regional-level pilots in Tallinn (Estonia) and Genoa (Italy) by **transport operators and cyber security organisations,** who will also be trained in using the project tools.

Risk analysis and impact assessment engine

Training

Financial impact assessment engine

IDS/IPS engines

SIEM as a correlation engine with backlog markers

Collaborative security incident response and threat investigation platforms

AIRBUS

Our role in the project

Thanks to our expertise in cyber security, we will have different roles within the project:

- Be **responsible for the integration of the CitySCAPE stack**
- Develop a **collaborative threat investigation platform**
- Develop a **collaborative incident response platform**
- Implement a **correlation engine** with a backlog of markers to raise more meaningful alerts

In order to offer a **collaborative and easy-to-use approach** to threat investigation and real-time cyber security incidents information sharing, our **CSIRT cyber defence services** are actively involved.

About our incident response team

To ensure that the cyber threats are contained and eradicated in a quick and efficient manner, we have built our own **experienced Computer Security Incident Response Team (CSIRT)**.

Our CSIRT team applies a meticulous methodology to detect and contain the attack, before removing it from the affected system. It consists of **dignosing the incident, eradicating the problem, reconstructing with concrete solutions and investigating further**. This will help you to quickly recover from a cyber incident.

CSIRT 24/7
Rapid Response Team

+33 (0) 9 72 30 13 99

HORIZON 2020: ec.europa.eu/programmes/horizon2020
CitySCAPE: www.cityscape-project.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883321. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.

Programme co-funded by the
EUROPEAN UNION

AIRBUS

FRANCE
Metapole 1, boulevard Jean Moulin
CS 40001 / 78996 Elancourt Cedex
France

GERMANY
Willy-Messerschmitt-Str. 1
82024 Taufkirchen
Germany

UNITED KINGDOM
Quadrant House / Celtic Springs
Coedkernew / South Wales
NP10 8FZ / United Kingdom

contact.cybersecurity@airbus.com
www.airbus-cyber-security.com