How TRUNSPORT Works

The platform consists of five interconnected components. The first is the Generative AI Mapper, which provides an intuitive interface for users to design their infrastructure and interact directly with the AI powered chatbot.

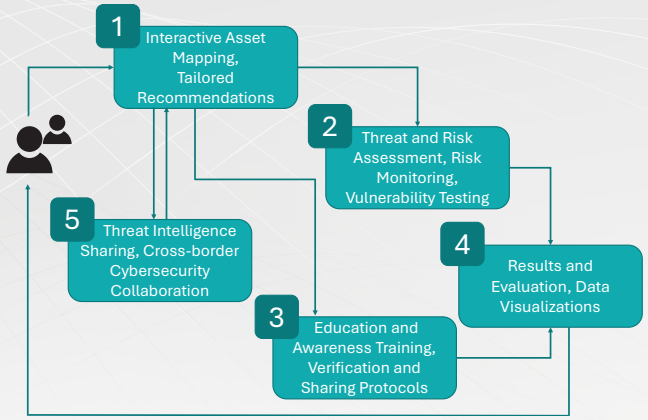
The second component is the analysis and threat detection layer, responsible for identifying risks and assessing vulnerabilities.

The third component delivers training modules to increase awareness of social engineering attacks and offers guidance on information sharing policies and verification procedures.

The fourth component is a comprehensive dashboard that consolidates results and presents reports, visualizations, and charts to help users monitor their cybersecurity posture over time.

Finally, the fifth component supports collaboration among transport and critical infrastructure stakeholders, enabling threat intelligence exchange and cross border cyber-resilience exercises.

Cyber Support Hub



TRUNSPORT

Mapping Security for **Smarter Transport**

Follow us on LinkedIn
TRUNSPORT

Check our YouTube Channel
@TRUNSPORT-x8z

Check our website
www.trunsport.eu

Funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Preparedness and mutual assistance support services for **TRU**stworthy cyber-resilient operations in tra**NSPORT** and related industrial sectors

Start Date
01/01/2026

End Date
31/12/2028

TRUNSPORT Motivation

TRUNSPORT is an EU-funded initiative dedicated to strengthening cybersecurity resilience across the transport sector and related critical infrastructures. As digitalisation accelerates, transport systems face growing cyber threats that can disrupt operations and compromise safety. TRUNSPORT addresses these challenges through its Cyber Security Hub, a one-stop platform offering advanced services for preparedness, protection, and mutual assistance.

What makes it innovative?

It enables users to map their infrastructure through an intuitive drag and drop interface, selecting system components from a visual, cartoon style library to easily build a representation of their operational environment. This approach helps users quickly identify connections, dependencies, and critical pathways within their systems. In addition, an interactive AI driven chatbot provides real time guidance. Users can ask questions about potential vulnerabilities, receive recommendations on high risk areas, and get advice on protective measures or response actions during a cyber incident.

Project's Objectives

1
Assess cybersecurity per NIS2; identify vulnerabilities and gaps.

2
Map transport operations, critical infrastructure, and key interdependencies.

3
Enhance vulnerability assessments via penetration testing across all systems.

4
Provide standardized cyber ranges for testing and cross-border exercises.

5
Strengthen industrial cybersecurity and improve incident response.

6
Deliver AI-driven threat and risk assessments using real-time data.

7
Enable continuous risk monitoring of attack surfaces and vulnerabilities.

8
Deliver the Cyber Support Hub as a unified cybersecurity platform.

9
Engage stakeholders through Open Calls across sectors and borders.

10
Collaborate with EU cybersecurity alliances for shared knowledge and resilience.

Consortium

CERTH/HIT
Hellenic Institute of Transport

eBOSRD
Engineered for Excellence
Driven by Passion For Innovation

ENIEEY
ICCS

6esfa

InCites
CONSULTING

deepblue

SEA Milan Airports

EVIDEN