Partners

CYSMET

UBITECH
ubiquitous solutions

GRUPPO
Maggioli

ΟΡΓΑΝΙΣΜΟΣ ΛΙΜΕΝΟΣ ΒΟΛΟΥ Α.Ε.

Integrated, Dynamic & Collaborative Risk Management System for Maritime Transport & Supply Chains

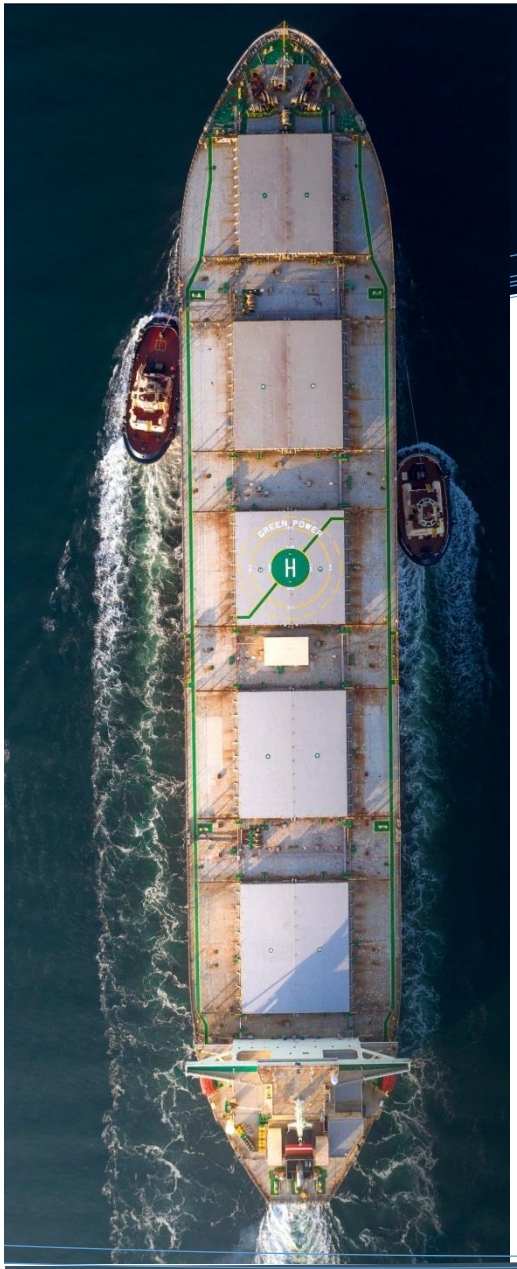
Global Supply Chains are becoming more complex and integrated. The organizations operating within the Supply Chains are heavily dependent on ICT and they are exchanging large amounts of data. There is a pressing need for methodologies and tools for the efficient evaluation and management of security threats and vulnerabilities throughout the interconnected infrastructures of the stakeholders of the Supply Chain services. **CYSMET** introduces a novel Maritime Supply Chain Risk Assessment methodology, tailored to small ports requirements with numerous interedependencies between the stakeholders, to alleviate the limitations of existing methodologies in handling cyber-security risks and threats and their impact. Here is how:

- Modelling of asset and service dependencies between comprising stakeholders of Maritime Supply Chains.
- Dynamic integration and management of open threat & vulnerability information.
- Dynamic and collaborative Risk assessment and management methodology.
- Platform validation and evaluation through real scenarios.
- Contribution to standards for security management processes in Supply Chain Services.

CYSMET

Thessalias 8 & Etolias 10
15231 Chalandri
Athens, Greece
Tel: +30 216 5000 500
Fax: +30 216 5000 599
Email: info@ubitech.eu

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Διαρθρωτικό και Επενδυτικά Ταμεία
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΑΝΑΠΤΥΞΗΣ ΚΑΙ ΕΠΕΝΔΥΣΕΩΝ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΠΡΟΓΡΑΜΜΑΤΩΝ ΕΤΠΑ & ΤΕ
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ ΚΑΙΝΟΤΟΜΙΑ
ΕΣΠΑ 2014-2020
ενισχύω - εργασία - αλληλεγγύη
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης



Integrated, Dynamic & Collaborative Risk Management System for Maritime Transport & Supply Chains

CYSMET

CYSMET

CYSMET Services

COLLABORATIVE RISK ASSESSMENT SERVICE

The service focuses on assessing the likelihood of various risks and the overall resilience and reliability of Supply Chain Services. The service provides the appropriate tools and methodology steps to examine and assess multidimensional risks spanning across the entire supply chain as well as their cascading effects.

RISK MANAGEMENT SERVICE

This service supports organizations in more effectively covering the weaknesses and dealing with the threats that have been identified in the Supply Chain Services, enabling further security event management by detailing all impactful threats that can be later used by security administrators for selection and deployment of mitigation measures.

ATTACK SIMULATION SERVICE

The service aims to design, execute and analyze simulation experiments related to the generation of all possible threat scenarios and the calculation of the cascading effects that an event may have on the operation of the Maritime Supply Chains. It enables organizations to model and simulate a set of attacks on their infrastructures, assessing their applicability and effectiveness, and model the cascading effects and the attack paths even between assets of different stakeholders.

OPEN THREAT INTELLIGENCE AND INFORMATION EXCHANGE SERVICE

The service allows the integration of data, related to known attacks, threats, AND vulnerabilities of information systems from open information sources (e.g., NIST National Vulnerability Database - NVD, Common Vulnerabilities and Exposures - CVE).

DATA INJECTION ATTACKS

SQL injection attack simulation and illegal access to the database of a ferry ticket company resulting to leak of personal and corporate data, and the disruption of the chain of transportation.

CYBER-PHYSICAL THREATS

Attack scenarios concerning the distribution of fuel using tankers. The considered scenario scould cause a number of very serious consequences (loss of life, marine pollution).

ATTACK ON HULL STRESS MONITORING SYSTEM (HSMS)

The scenario focuses on cyber-attacks involving the breaching of the ship's network via the Satcom system or via the Internet, or even via phishing and gaining unauthorized access and control of the HSMS system.

ATTACK ON CONTAINER STOWAGE PLANNING SYSTEM

Man-in-the-middle and spoofing attacks on the messaging protocols of the stowage planning systems of container ships, affecting the stowage plan and the balance of the ship itself.

Ευρωπαϊκή Ένωση
Ευρωπαϊκά Διαρθρωτικά και Επενδυτικά Ταμεία

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΑΝΑΠΤΥΞΗΣ ΚΑΙ ΕΠΕΝΔΥΣΕΩΝ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΠΡΟΓΡΑΜΜΑΤΩΝ ΕΤΠΑ & ΤΣ
ΕΥΔ ΠΡΟΓΡΑΜΜΑΤΟΣ «ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ»

ΕΠΑνΕΚ 2014–2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ
ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ
ΚΑΙΝΟΤΟΜΙΑ

ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

https://cysmet.ubitech.eu

CYSMET Project

CYSMET