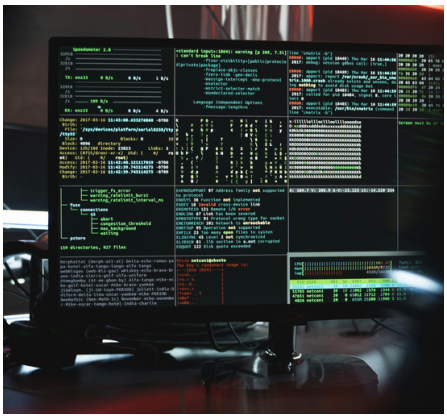
NEWSLETTER

ISOLA

CYBERSECURITY PILOT:

Major Achievement in Second Year

Building on its promising first year, the ISOLA project continued to evolve, transforming conceptual designs into practical technological solutions. The focus was sharpened on refining critical elements such as advanced surveillance and data analytics, which are pivotal for detecting and mitigating maritime security threats. Despite the challenges posed by the ongoing pandemic, the project consortium fortified its collaboration, leaning on digital platforms to ensure a seamless workflow. This period was also significant for the initiation of prototype development, marking a crucial step in evaluating the system's applicability in real-world settings and refining its features.



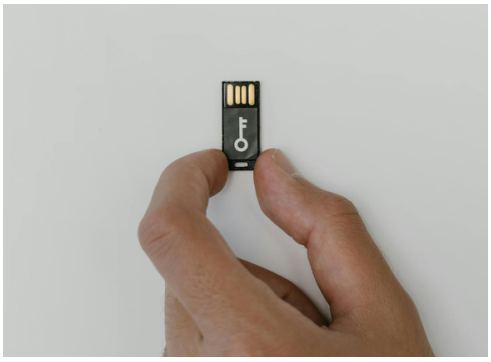
A notable milestone was achieved in the context of Pilot Use Case 5 (PUC5), where DVATS's network-based Passive Vulnerability Detection system was put to the test on a docked maritime vessel operating on a scaled-down network. This pilot, successfully completed in November 2021, was designed to rigorously assess network security on a ship. Impressively, DVATS not only identified all three intentionally deployed vulnerable services but also uncovered an additional five vulnerable services within the vessel's network, underscoring the efficacy and depth of the ISOLA project's technological advancements.

As ISOLA progresses towards its conclusion, the successful completion of PUC5 exemplifies the project's core strengths—robust international collaboration and cutting-edge technological innovation. These qualities have been instrumental in navigating the complex challenges inherent in enhancing global maritime security, setting ISOLA on a definitive path to making a significant and lasting impact.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883302. This publication reflects only the author's views and the European Union is not liable for any use that may be made of the information contained therein.

CYBERSECURITY

Important Security Aspect in Shipping



In June 2017, the global shipping giant A.P. Moller-Maersk was hit by the NotPetya ransomware, disrupting its operations worldwide and causing estimated losses of up to $300 million. This incident, one of the most significant cyber-attacks in maritime history, highlighted the vulnerability of the sector to digital threats.

The malware, targeting Microsoft Windows vulnerabilities, paralyzed Maersk's port and logistics operations across 120 countries, underscoring the interconnected nature of global supply chains and the potential for widespread impact from such attacks.
The Maersk cyber-attack served as a wake-up call for the maritime industry, emphasising the urgent need for enhanced cybersecurity measures. Following the attack, there has been a concerted effort to bolster maritime cyber defences, including adhering to the International Maritime Organization's cybersecurity guidelines and fostering a culture of cyber awareness among maritime personnel.
The incident underscores the importance of continuous vigilance and adaptation in cybersecurity strategies within the maritime sector. As digitalization in maritime operations advances, the industry must ensure that cybersecurity resilience keeps pace to safeguard global maritime trade against future cyber threats.

Cybersecurity Solution in ISOLA

The ISOLA project enhances maritime cybersecurity by focusing on vulnerability assessments in maritime vessels' ICT systems. As these vessels rely heavily on complex systems, identifying and measuring vulnerabilities is crucial to counteract cyber risks.

The cybersecurity component within the ISOLA system created by Cyberlens utilises the Dynamic Vulnerability Assessment and Testing Service (DVATS) for this task, employing both passive and active scanning methods. Passive scanning analyses network data non-intrusively, identifying potential vulnerabilities without disrupting system operations. Active scanning collects real-time data, checking for known vulnerabilities and assessing their impact using the Dynamic Vulnerability Scoring System (DVSS).

Upon identifying vulnerabilities, DVATS issues alerts, enabling quick actions to mitigate risks, such as isolating affected systems. This proactive approach ensures maritime vessels are safeguarded against cyber threats, maintaining the integrity of their operations and infrastructure.

ISOLA TOOL SPOTLIGHT:

Enhancing Maritime Cybersecurity

Cyberlens joined the ISOLA H2020 EU-funded project with the aim of extending its expertise in cybersecurity for passenger ships. One of its key contributions is the enhancement of Cyberlens' Dynamic Vulnerability Assessment and Testing Service (DVATS), tailored to meet the specific challenges of maritime cybersecurity.

Within ISOLA, DVATS plays a crucial role in detecting, identifying, and measuring vulnerabilities within the ICT systems and infrastructures of passenger ships. It dynamically assesses maritime vessels' ICT systems and presents relevant security information on the ISOLA dashboard, enabling security analysts to make informed decisions on the security posture of their system.
Key features of DVATS include:

- **Passive & Active Vulnerability Analysis:** DVATS incorporates both passive and active scanning capabilities. Passive vulnerability analysis is based on non-intrusive network data and meta-data analysis, while active vulnerability scanning includes real-time collection of host-based indicators for assessment against known vulnerabilities (CVEs) and exploits.

- **Integration with Threat Intelligence:** DVATS integrates with the National Vulnerability Database (NVD) and leverages threat intelligence to prioritize vulnerabilities for remediation.

DVATS stands out for its unique combination of passive and active vulnerability detection, minimizing impact on vessel services while effectively identifying system-wide vulnerabilities. This is particularly crucial for critical legacy systems like engine control systems, where any interference is unacceptable. Furthermore, DVATS offers self-hosted and managed cloud-based deployment, catering to diverse maritime security needs. The cloud-based option is ideal for resource-constrained environments, while the self-hosted deployment suits scenarios with restrictive data policies or limited connectivity.

By offering advanced capabilities and flexible deployment options, ISOLA-enhanced DVATS service represents a significant advancement in maritime cybersecurity, bolstering the resilience of passenger ships against evolving cyber threats.