Who benefits?

Critical Infrastructure Operators
Enhance resilience against cyber threats in complex, interconnected environments.

Logistics and Transport Stakeholders
Secure digital systems across land, sea, and last-mile delivery operations.

Cybersecurity Experts and Developers
Adopt advanced detection, response, and threat modelling techniques.

Technology Providers and Integrators
Incorporate MEDIATE tools and frameworks into scalable, market-ready solutions.

Partners

Get in touch

www.mediate-horizon.eu

info@mediate-horizon.eu

x.com/mediate_horizon

/company/mediate-horizon

@MEDIATE_HORIZON_EUROPE

/communities/mediate

MEDIATE

Key facts

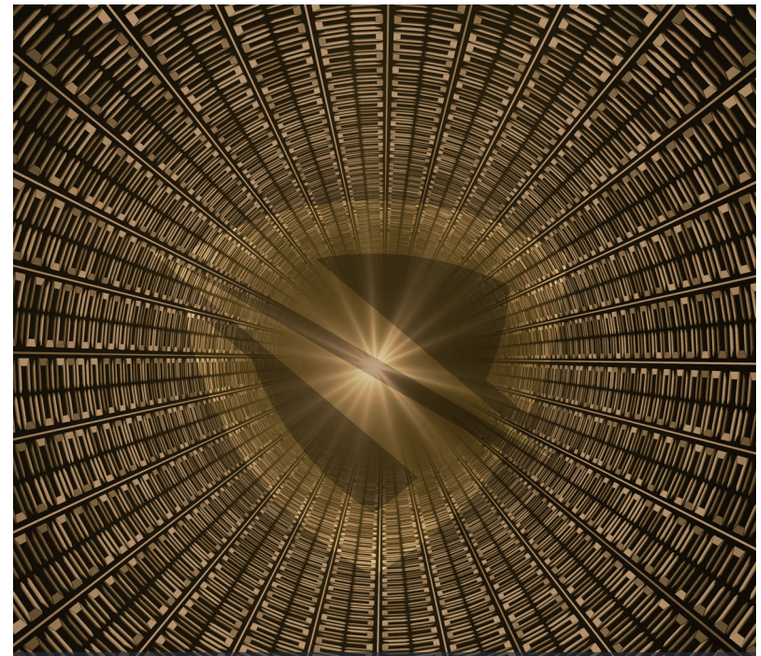
Call: HORIZON-CL3-2023-CS-01
Type of Action: HORIZON-IA
GA Number: 101168465
Start Date: 01 Nov 2024
Duration: 36 months
Project Budget: €4,925,505

Funded by the European Union

This project has received funding from the European Union's Horizon Europe innovation programme under Grant Agreement No 101168465.

MEDIATE

Multi-facEteD ImplementAtion of a mixed sofTwarE/hardware-based zero trust framework for the computing continuum



Overview

The **MEDIATE** framework that will support cybersecurity resilience through reconfiguration, vulnerabilities mitigation through cyber threat analysis, secure integration at the IoT level through software and hardware-based security sensors and trust and security for massive ecosystems through the use of federated learning-based orchestration. Moreover, it will feature AI-based tools for cyber threat intelligence that assist a decision support system and privacy policies for data and identity protection.

Project Objectives

1. Develop a novel dynamic cybersecurity framework for zero trust systems operating in complex computing continuum environments.
2. Establish a Scalable and Intelligent Cybersecurity Command System
3. Create an intelligent AI-based Decision Support System (DSS) Mechanism for Vulnerability Adaptation and Asset/Entity Clearance Scheme
4. Implement efficient AI-based Cyber Threat Intelligence for Risk Analysis
5. Provide dynamic control on access to data and functionalities to implement minimum privilege paradigm and continuous action verification for a zero-trust environment
6. Enforce security on reconfigurable hardware edge/cloud sentinel platforms
7. Deploy, validate and evaluate in critical infrastructures in the context of advanced fourth-party logistics (4PL) operations across supply chain environments
8. Define a business plan for the post-project exploitation of the MEDIATE framework

Use Cases

Use-Case 1

Sea freight operations and management

UC1 aims to apply the MEDIATE Methodology and support platform to assess and enhance the dependability of container ship digital systems (SDS) and Port Community Systems (PCS). DANAOS will use two scenarios involving advanced SDS and Digital Twins to boost efficiency and support decarbonisation. Focus areas include cybersecurity, data-driven decision-making, and AI with federated learning, both at vessel-port and fleet-port levels. Collaboration with external partners like Fundación Valenciaport will help define requirements and support development. Danaos seeks significant dependability improvements as detailed in the following sections.

Use-Case 2

Smart Warehousing

Milsped's warehouse features the AutoStore system to optimise space, boost efficiency, and minimise manual errors. The setup includes 23 robots, 5 ports, and 25,000 bins, with potential expansion to 50,000 bins, 44 robots, and 10 ports. Serving mainly the fashion sector, it supports cross-docking, inventory control, store replenishment, and e-commerce fulfilment, with an annual throughput of 6 million pieces. This use case focuses on securing the Inbound and Outbound processes of the automated warehouse.

Use-Case 3

Last-mile delivery

Led by ISI and ALKE, UC3 focuses on last-mile delivery using a mobile hub built on an autonomous electric vehicle equipped with app-openable lockers. These mobile access hubs support sustainable city logistics by dynamically using urban space. The vehicle follows predefined routes with scheduled stops, allowing users to collect packages during assigned time slots. MEDIATE will address cybersecurity threats, such as attacks on the locking system, using multimodal fusion and distributed learning to enhance resilience and protect against data poisoning.