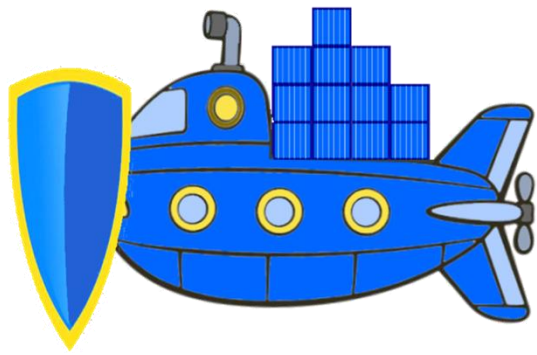




CyberNEMO

End-to-end Cybersecurity to NEMO Meta-OS

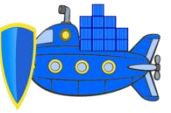
Introduction to CyberNEMO

Andreas Papadakis, Ilias Seitanidis, Theodore Zahariadis

SYNELIXIS



This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101168182



Project Identity

Title: End-to-end Cybersecurity to NEMO Meta-OS

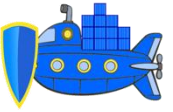
Topic: HORIZON-CL3-2023-CS-01-01
Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)

Funding Instrument: IA (innovation Action)

Project Coordinator: Synelixis S.A. (<https://www.synelixis.com>)
Technical Manager: Telefónica Innovación Digital (<https://www.telefonica.com>)

Duration: 36 months – Starting Date: 1st October 2024

CyberNEMO Consortium

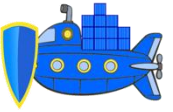


Consortium: 24 Partners, 11 countries

Complementary roles: Industry, SMEs, Telecom operators, End users, Research, OS Ecosystem

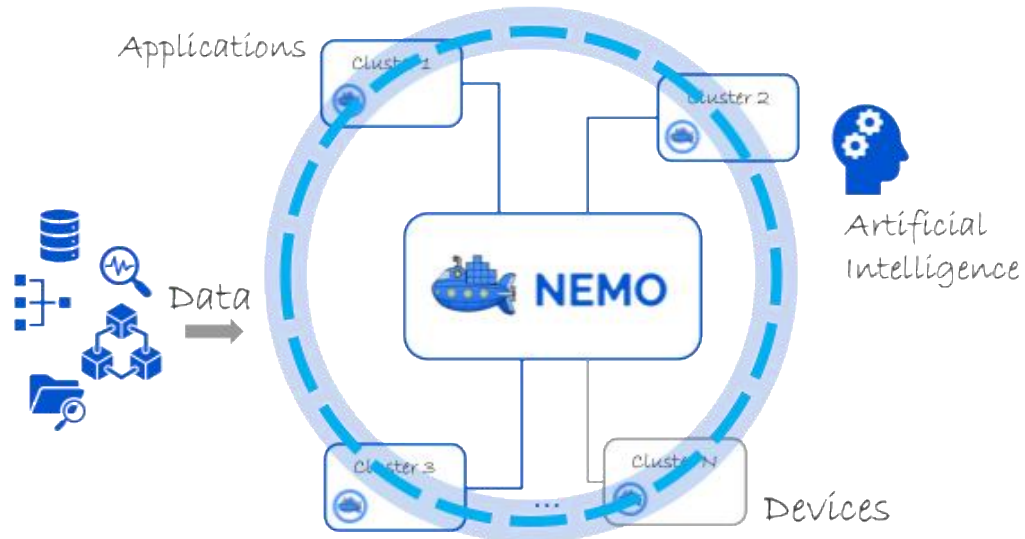
6 pilots: OneLab , 4 x Pilots/LLs, 1 Federated pilot

Rationale and Starting Point



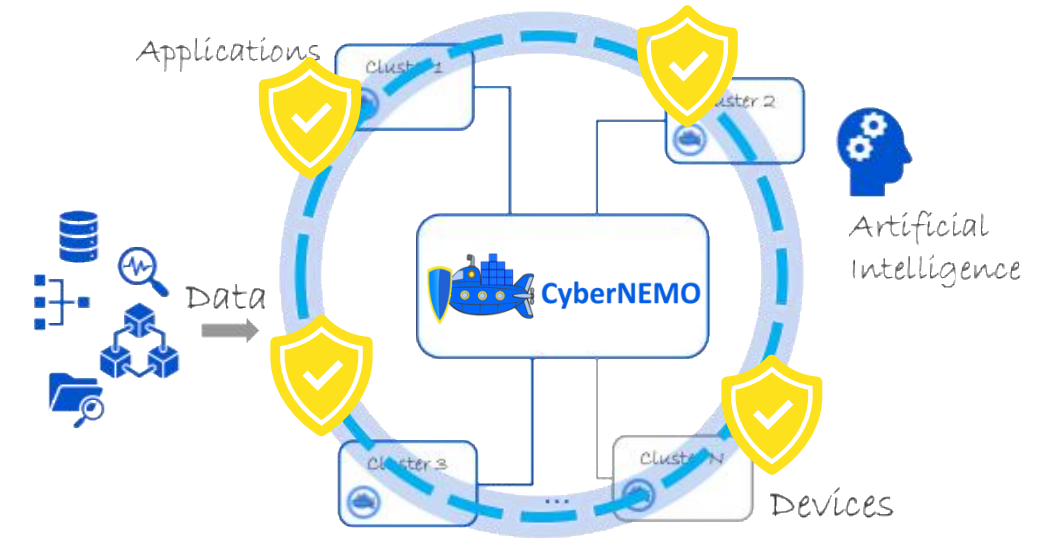
NEMO: Next Generation Meta Operating System

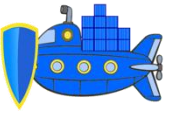
- Unified management of distributed computing resources
- Paradigm adopted by critical infrastructures



CyberNEMO

- Apply Zero-trust principles and provide end-to-end cybersecurity solutions
- To support awareness, preparedness, detection, decision, risk mitigation and resilience.





Technical challenge: Computing Continuum

CyberNEMO targets a dynamic and distributed environment composed of:

- IoT devices and cyber-physical assets
- Edge and cloud infrastructures
- Kubernetes-based services and workloads
- Data spaces and multi-domain interactions

Key Cybersecurity Challenges

Complexity and
Heterogeneity

Decentralized
Governance

Dynamic
Topology

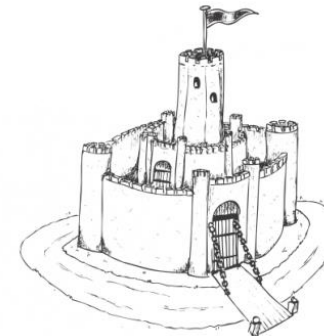
Increased attack
Surface

Data
Sovereignty

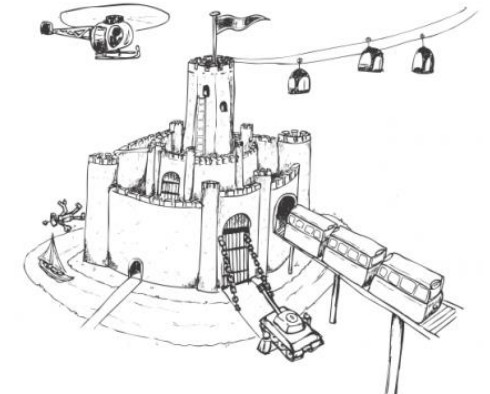
Evolving Regulatory
Framework

Traditional perimeter-based security is not enough for dynamic, federated and cloud-native environments.

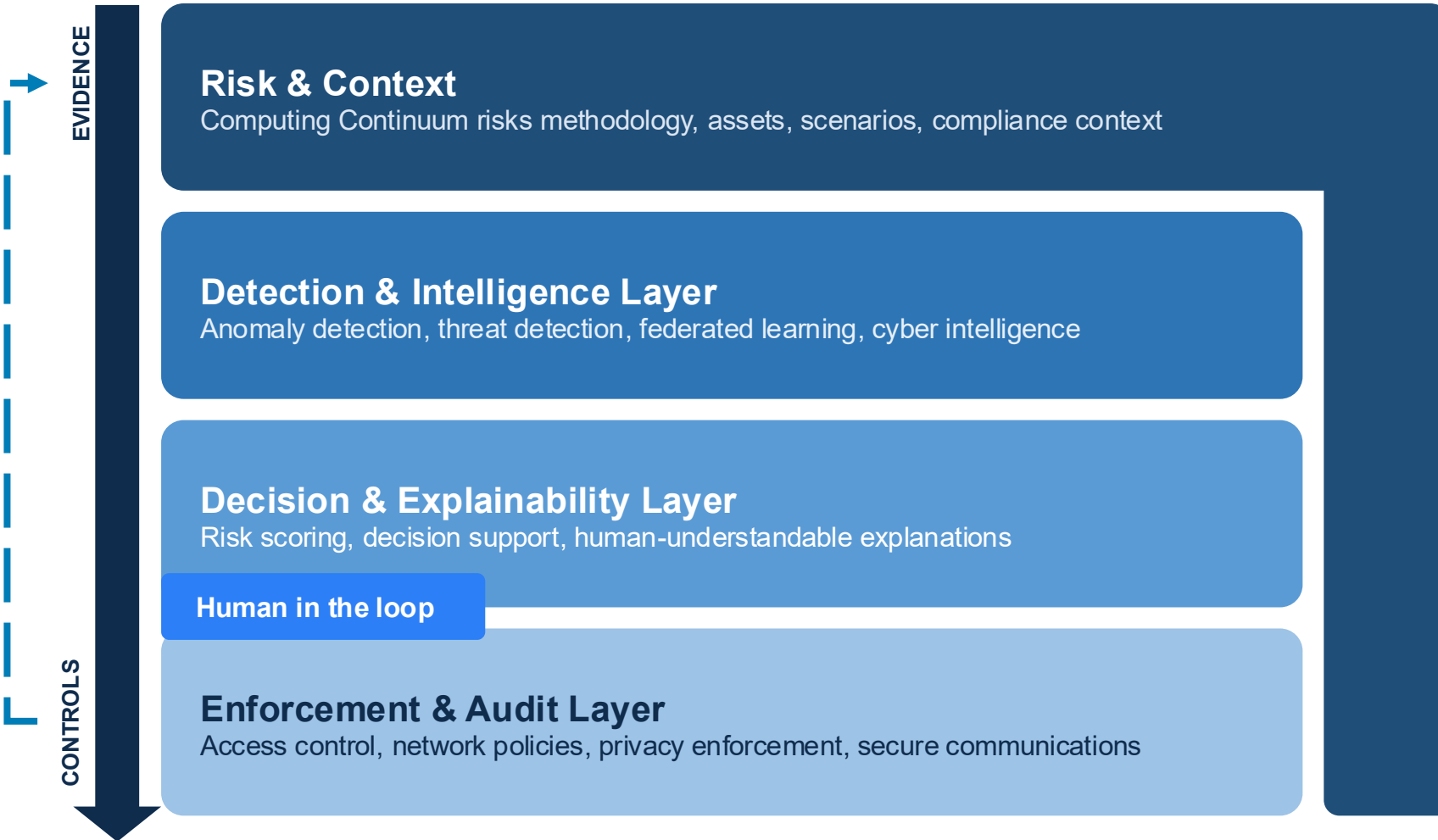
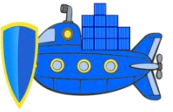
Castle Model of Security



Castle Model in Reality



CyberNEMO Layered Approach



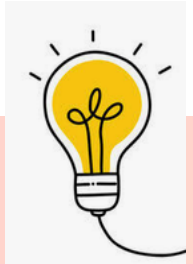
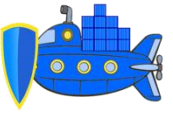
MAIN ARCHITECTURAL IDEA

Transform cyber evidence into enforceable and auditable countermeasures.

Four technical layers move signal from **risk**, through **detection** and **decision**, into **enforceable controls**.



CyberNEMO Layered Toolset (1 / 5)



- Approach tailored on Computing Continuum
 - Heterogeneous, multi-owned, federation
 - Kubernetes –based
 - Context establishment (topology as graph, assessed vulnerabilities)

Infrastructure
&
Workloads

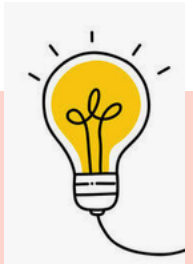
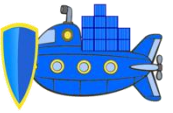
Kubernetes
Cilium

NEMO metaOS
Meta-network controller (mNCC)

Cloud · Edge · IoT
Resources & devices

Services
Workloads and data

CyberNEMO Layered Toolset (1 / 5)



- Complementarity among Enforcers
 - Different layers and functionalities
 - L2S-M,
 - CCIPSaaS
 - cDNS
 - CNPM/L7FM
- OpenC2

Network &
Privacy
Enforcement

ZTNA

Secure communication (CCIPS), Policy enforcement (L2S-M, Netbird), Proof of Transit (PoT)

PPE

Privacy & consent

CNPM

Policy templates as countermeasures (L7FM)

cDNS

Secure DNS (RPZ)

Infrastructure
&
Workloads

Kubernetes

Cilium

NEMO metaOS

Meta-network controller (mNCC)

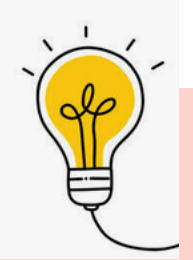
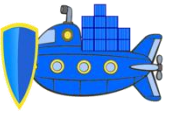
Cloud · Edge · IoT

Resources & devices

Services

Workloads and data

CyberNEMO Layered Toolset (1 / 5)



- Complementarity among Detectors
 - NADA (network flows)
 - DLMD
 - AIFWaaS
 - cDNS (Kubernetes flows)
 - ZT-FML
 - Third party (Falco)
- IDMEFv2

Detection

AI-FWaaS

HTTP ingress

cDNS

DNS plane

DLMD

Lateral movement

ZTNA

Network anomaly
(NADA, Whiteshark)

ZT-FML

Model & Data
poisoning

CASB

Runtime security
(Falco)

Network & Privacy Enforcement

ZTNA

Secure communication (CCIPS), Policy enforcement
(L2S-M, Netbird), Proof of Transit (PoT)

PPE

Privacy & consent

CNPM

Policy templates as
countermeasures (L7FM)

cDNS

Secure DNS (RPZ)

Infrastructure & Workloads

Kubernetes

Cilium

NEMO metaOS

Meta-network controller (mNCC)

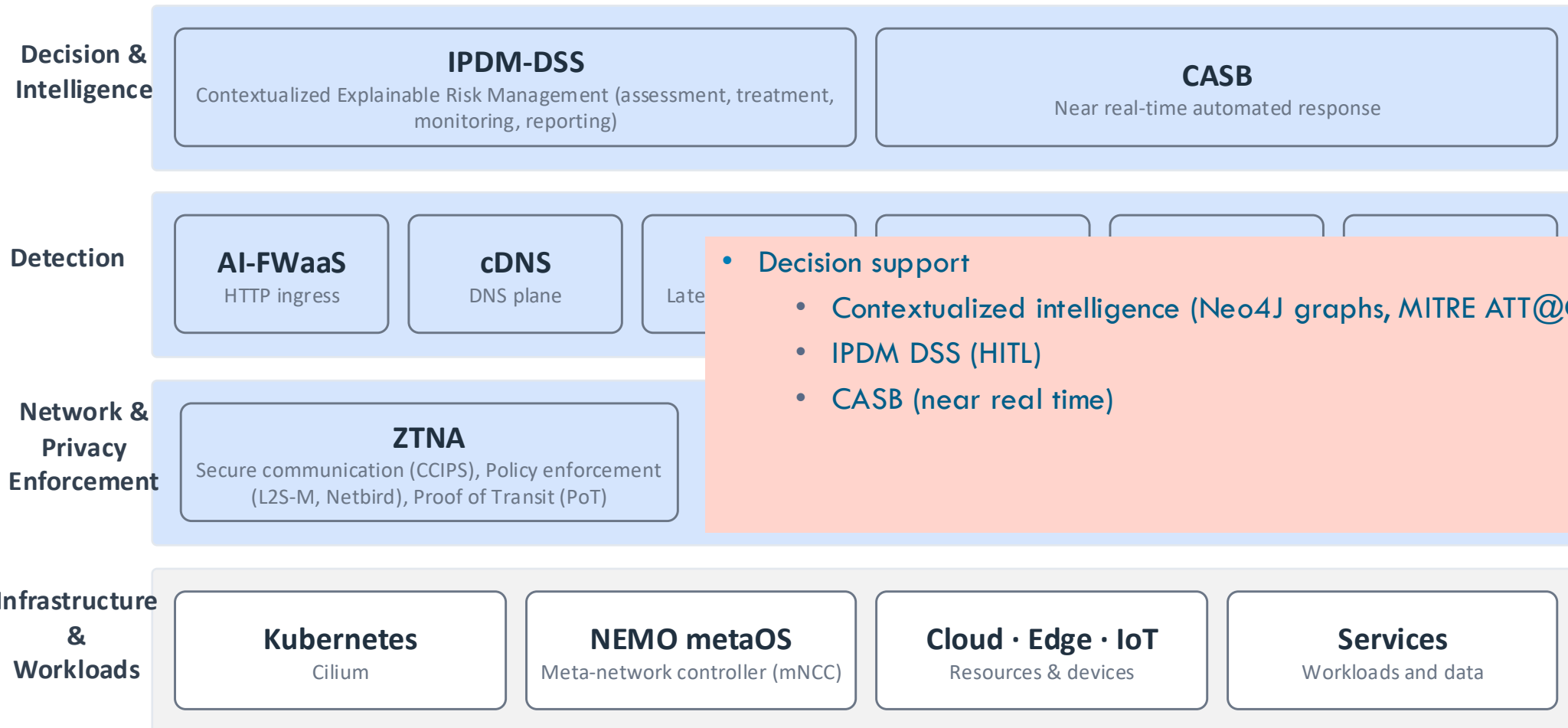
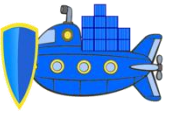
Cloud · Edge · IoT

Resources & devices

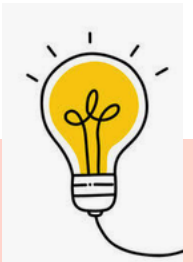
Services

Workloads and data

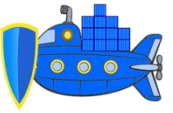
CyberNEMO Layered Toolset (1 / 5)



- Decision support
 - Contextualized intelligence (Neo4J graphs, MITRE ATT@CK)
 - IPDM DSS (HITL)
 - CASB (near real time)



CyberNEMO Layered Toolset (1 / 5)



Assurance & Collaboration

ACA

Accreditation, Certification, Auditing

SAAM

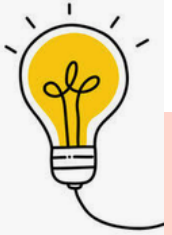
Systemic Risk Assessment, pan-European CTI hub

Decision & Intelligence

IPDM-DSS

Contextualized Explainable Risk Management (assessment, monitoring, reporting)

- Coverage of full service provision lifecycle
 - Deployment (ACA-Auditing, Certification, Accreditation)
 - Runtime
- Collaboration and knowledge Sharing
 - STIX-based CTI exchange among peers
 - Improved NIS2-based knowledge sharing
 - System risk analysis



Detection

AI-FWaaS

HTTP ingress

cDNS

DNS plane

DI

Lateral movement

(NADA, Whiteshark)

poisoning

(Falco)

Network & Privacy Enforcement

ZTNA

Secure communication (CCIPS), Policy enforcement (L2S-M, Netbird), Proof of Transit (PoT)

PPE

Privacy & consent

CNPM

Policy templates as countermeasures (L7FM)

cDNS

Secure DNS (RPZ)

Infrastructure & Workloads

Kubernetes

Cilium

NEMO metaOS

Meta-network controller (mNCC)

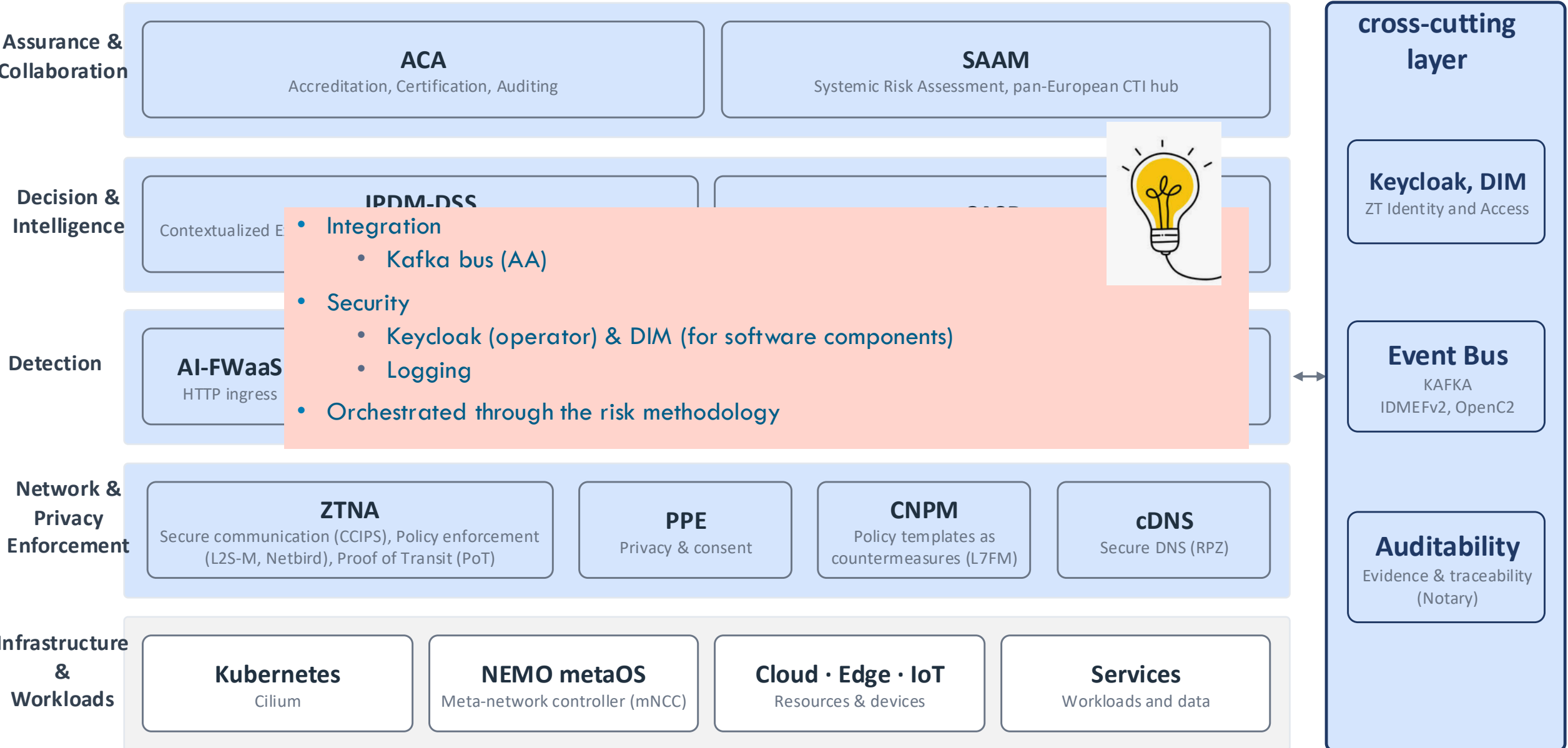
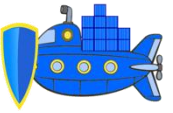
Cloud · Edge · IoT

Resources & devices

Services

Workloads and data

CyberNEMO Layered Toolset (1 / 5)



CyberNEMO Repository



🏠

Q Search or go to...

Group

CyberNEMO project

Manage

Plan

Code

Deploy

Operate

Analyze

Help

Eclipse Research Labs / CyberNEMO project

CyberNEMO project

Subgroups and projects

Shared projects

Shared groups

Inactive

🔄

Search (3 character minimum)

Q

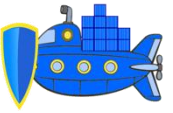
Name

↑

>	C	Cybersecurity Tools as a Service	🌐	👤 1	📁 3	👤 1
>	H	Human Explainable AI and Intelligence Amplification	🌐	👤 0	📁 1	👤 1
>	S	Stream Event Processor	🌐	👤 0	📁 3	👤 1
>	T	Trial Data	🌐	👤 0	📁 4	👤 1
	X	XAI Tools for Continuous System Risk Analysis	🌐	👤 0	📁 0	👤 1
>	Z	Zero Trust Federated Learning	🌐	👤 0	📁 1	👤 1
>	Z	Zero Trust Network Access	🌐	👤 0	📁 7	👤 2
	A	ACA	🌐	★ 0		2 weeks ago
	C	ci-cd-integration	🌐	★ 0		3 weeks ago
	C	Continuum Access Security Broker - CASB	🌐	★ 0		2 weeks ago

Copyright © Eclipse Foundation AISBL. All rights reserved. Privacy Policy | Terms of Use | Copyright Agent

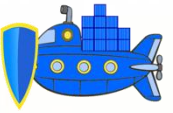
<https://gitlab.eclipse.org/eclipse-research-labs/cybernemo-project>



Some Initial Results

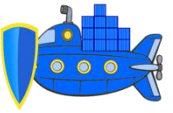
- ZT-FML secure aggregation protocol with 100+ mobile devices confirms scalability: aggregation completes in 18ms client-side, meeting the KPI target
- L2S-M generates 50 network micro-segments in 3.5s
- IPDM-DSS Knowledge components discover, map and populate topology graph and provide risk contextualization for each asset
- OSCAL automates compliance via certification profiles (NIST SP 800-204, MEF 118)
- ISACs contacted on CTI sharing.

The way forward: Pilots validation



6 verticals: Energy & Water (Italy), Healthcare (Bulgaria), Media (Spain), Smart Farming & Supply Chain (Greece)

Real test cases, varying exposure to the computing continuum.

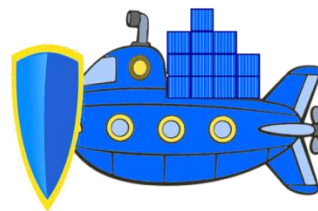


Evaluation Objectives (and Challenges)

- Verify layered functionalities (detectors, enforcers)
 - Attack simulator
 - Hosts may ban the pilot environment due to attacks
 - Intrinsic difficulties for new attack patterns (anomaly detection)
- Employ pilot environment
 - Use cases and scenarios available
 - Custom environments not using Kubernetes
 - Interested in operational aspects (indirectly connected with CC security)
- Evaluate decisions taken
 - Verified view of context
 - Quantitative assessment of countermeasure impact (e.g. availability)

Thank you for your attention

Andreas Papadakis
papadakis@synelixis.com



CyberNEMO

SYNELIXIS

Telefónica

ECLIPSE
FOUNDATION



POLITÉCNICA

netcompany
intrasoft

Maggioli

SPACE

THALES



SIEMENS

CyberSocial Lab.

ENTERSOFT



UNPARALLEL



Sphinx
Technology
Solutions

SORBONNE
UNIVERSITÉ

DNV



EWTH AACHEN
UNIVERSITY



eng

CYBERTECH
ENGINEERING GROUP