Resilmesh
securing cyber infrastructures

Cyber Situational Awareness and Resilience in the Resilmesh Project

Lukáš Sadlek
Masaryk University, CSIRT-MU

CSNOG 2026 – 22 January 2026

Funded by the European Union

Resilmesh

securing cyber infrastructures

About the Project

Funded by the European Union

Resilmesh
securing cyber infrastructures

Essential Information

- **Programme and type:** Horizon Europe (Innovation Action)
- **Duration:** 36 months (10/2023 – 09/2026)
- **Consortium:** 14 partners – 9 countries
- **Budget:** € 5.6 millions

To deliver an open and extensible security operations platform with advanced cyber situational awareness and detection / response capabilities to manage security and resilience in complex and dispersed digital services and infrastructures.

Project Overview

Funded by the European Union

Resilmesh
securing cyber infrastructures

Partners

Research & Technology	UMU, TUS, RHUL, MUNI, JR, KEMEA, JAMK
Industrial	GMV, MONT, F6S, SLP
End Users	INFOCERT, ALIAS, CARM

Funded by the European Union

Resilmesh

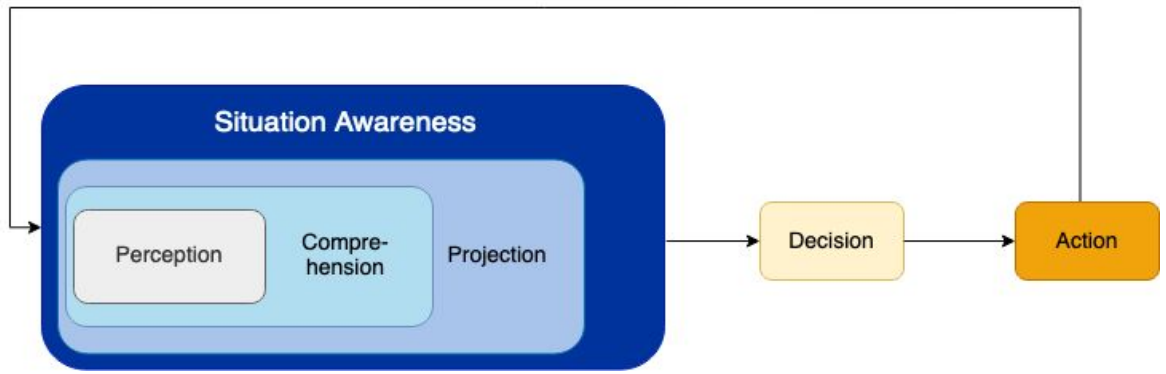
securing cyber infrastructures

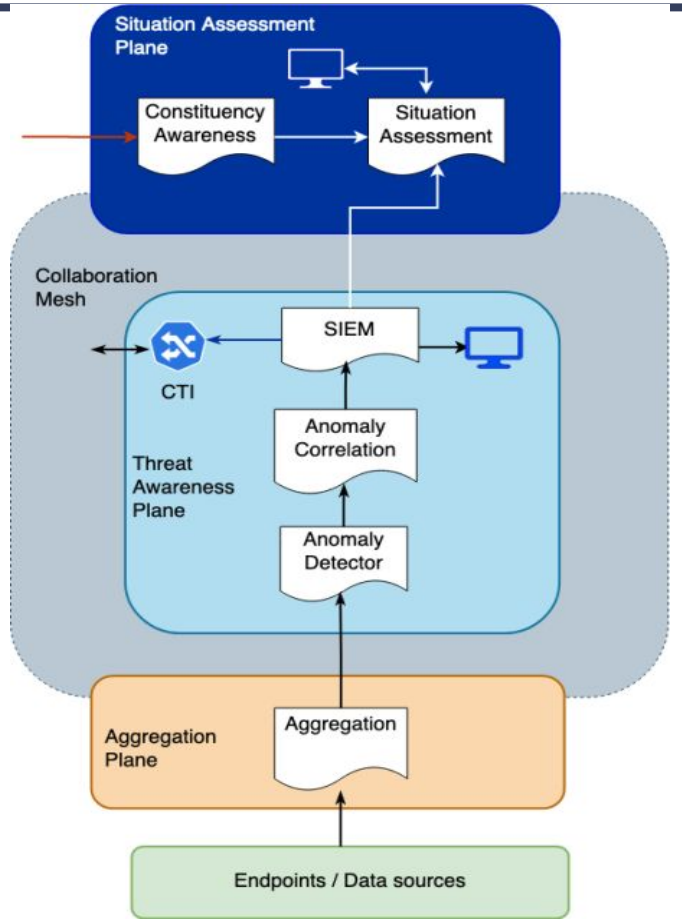
Technical Concept and Components

Funded by the European Union

Cyber Situational Awareness

- Ability to understand **the current state** of network environment
- Can improve **cyber resilience** against attacks





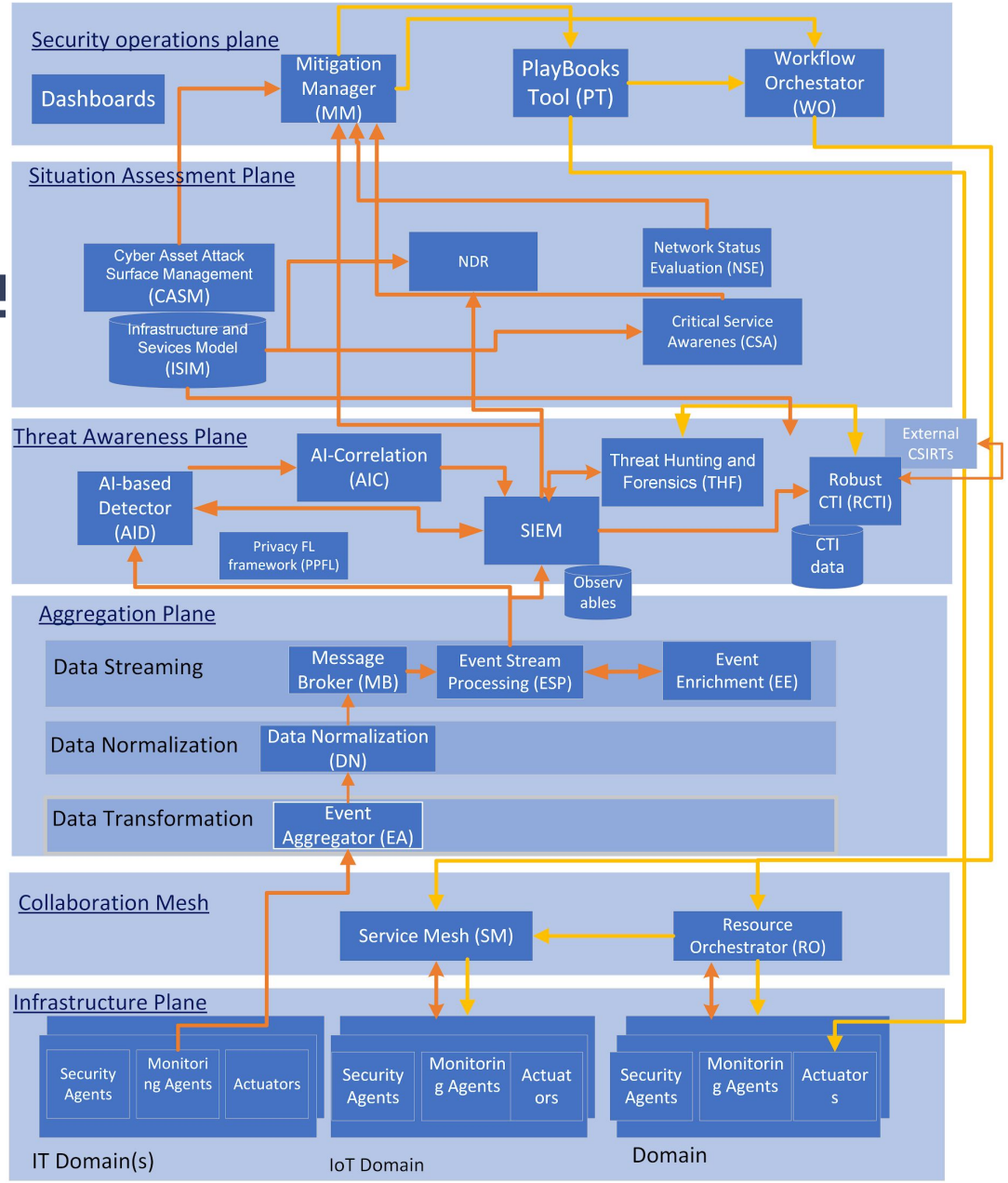
- **End-to-end data pipeline** containing information processing steps
- **Starts** with emission of the event from the endpoint
- **Ends** with consumption for situation assessment

Funded by the European Union

Resilmesh
securing cyber infrastructures

Functional Architecture

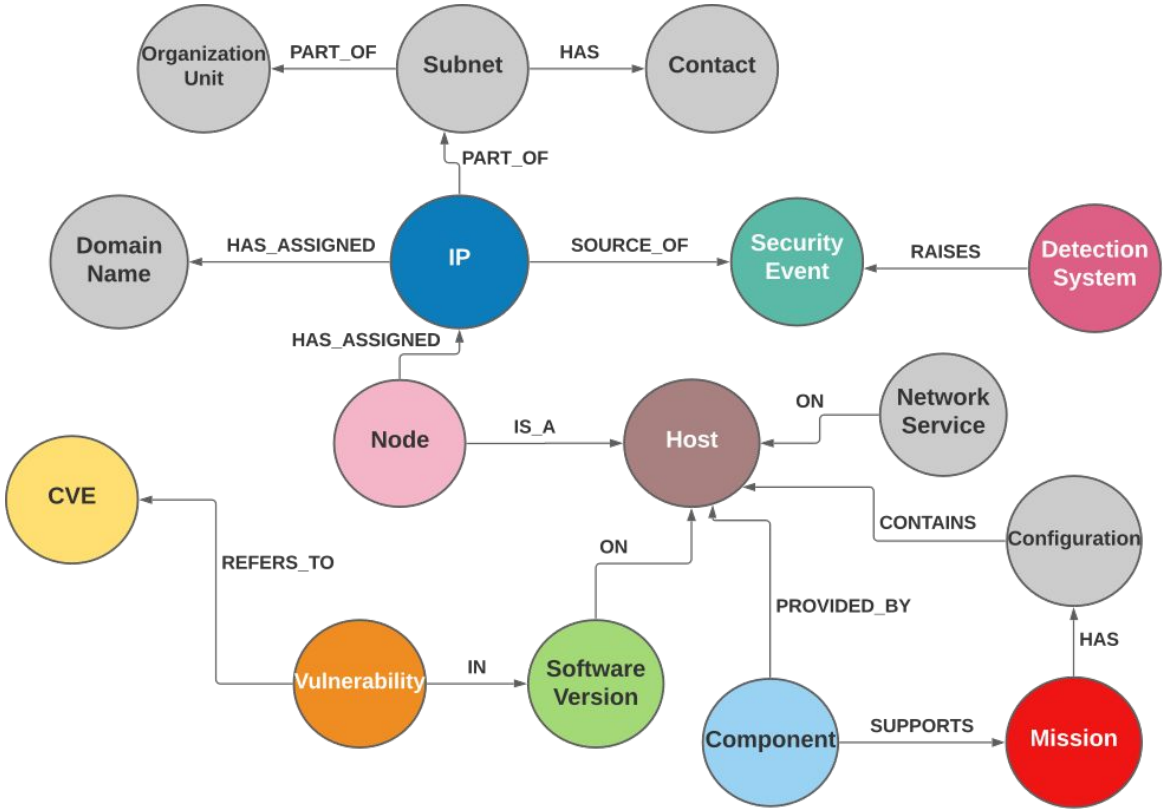
- Inspired by **Security Operations and Analytics Platform Architecture (SOAPA)**
  - **Security Operations Layer** – contains elements of the collaboration function plus SOAR (Security Orchestration, Automation, and Response) functions
  - **Analytics Layer** – contains threat awareness and situation assessment
  - **Software Services Layer** – contains parts of the collaboration mesh and aggregation
  - **Distributed Data Services Layer** – contains aggregation functions
- **Functionality of layers** is provided by components
- **Proactive and reactive** communication of components



Funded by the European Union

ISIM – Infrastructure and Service Information Model

- **Knowledge graph** of local network
- **Nodes** – entities (e.g., hosts, services, networks, users, vulnerabilities)
- **Edges** – relationships (e.g., vulnerability found on host and host connected to network)



Funded by the European Union

Resilmesh
securing cyber infrastructures

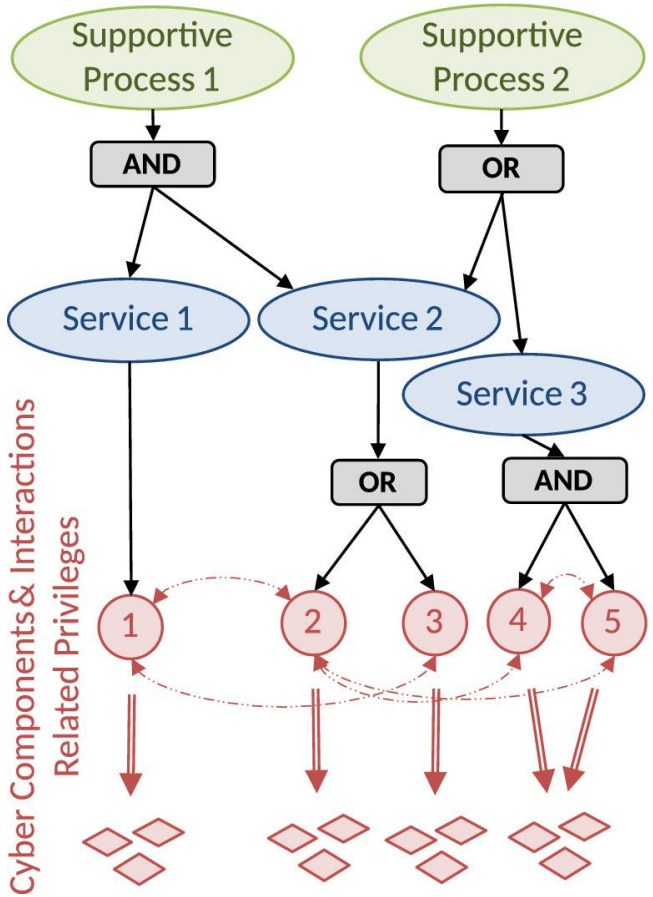
CASM – Cyber Asset Attack Surface Management

- **Task** – enumerate cyber assets and vulnerabilities automatically
- **Implementation** – split into multiple workers of Temporal.io
    - **CVE worker –** identifies CVEs based on Common Platform Enumeration
    - **Scanning workers –** Nmap asset scanning, Nmap topology scanning, nuclei scanning, and “custom” EasyEASM scanning
    - **Enrichment worker –** indicators from cyber threat intelligence from industrial partner

Funded by the European Union

CSA – Critical Service Awareness

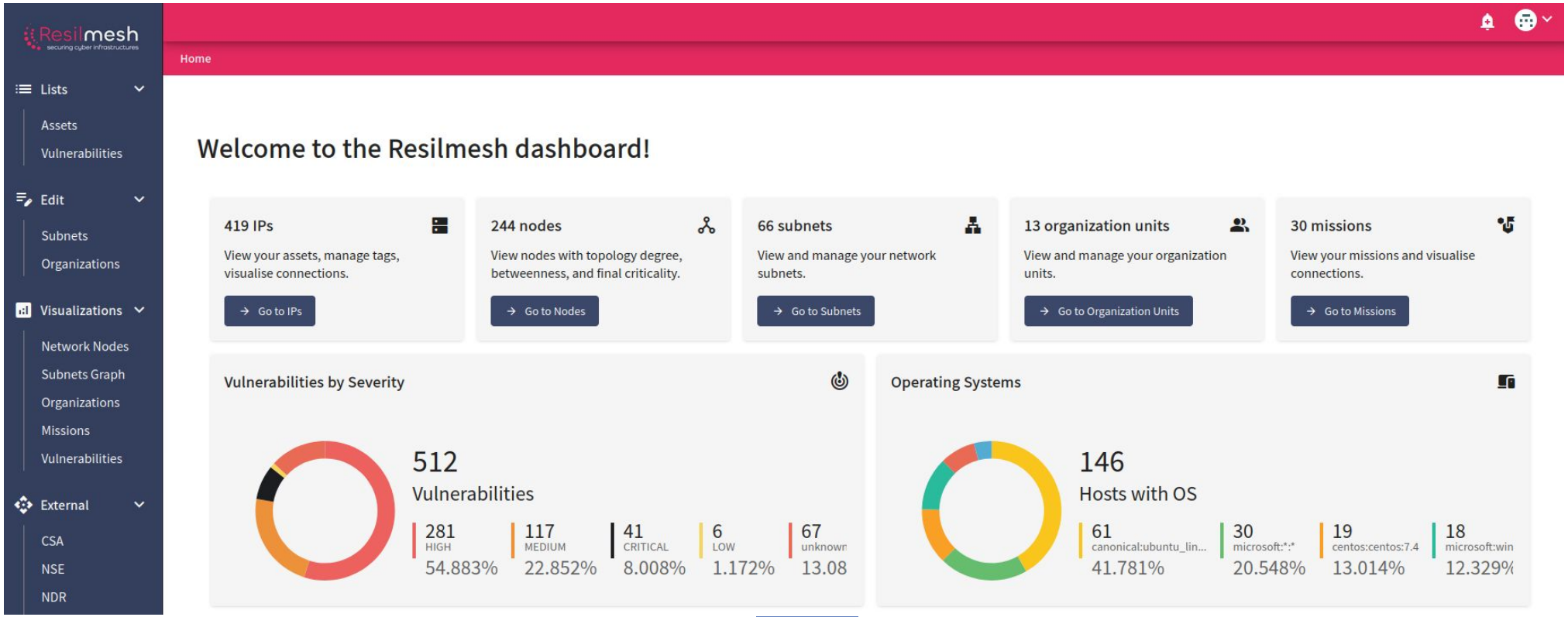
- **Task** – map critical assets and their dependencies
- **Data model** – 3-layer mapping with AND/OR notation
- **Example** – robotics
- Used in **computation of criticalities** from missions



Funded by the European Union

SACD – Situation Awareness Consolidated Dashboard

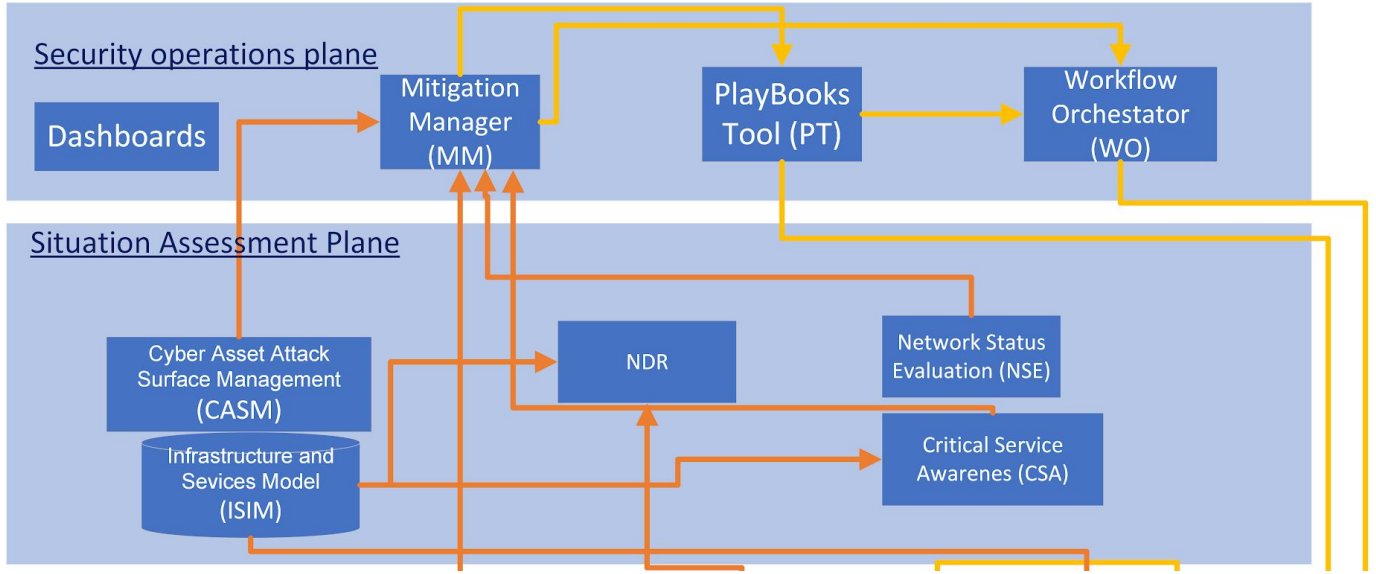
- **Panels** allow interaction with **ISIM data**



Funded by the European Union

Dependent Components

- **Network Status Evaluation (NSE)**
  - Risk assessment
- **Network Detection and Response (NDR)**
  - Raw network traffic
- **Mitigation Manager (MM)**
  - Selects mitigation
- **Playbooks Tool (PT)**
  - Playbooks with mitigations



Funded by the European Union

Resilmesh

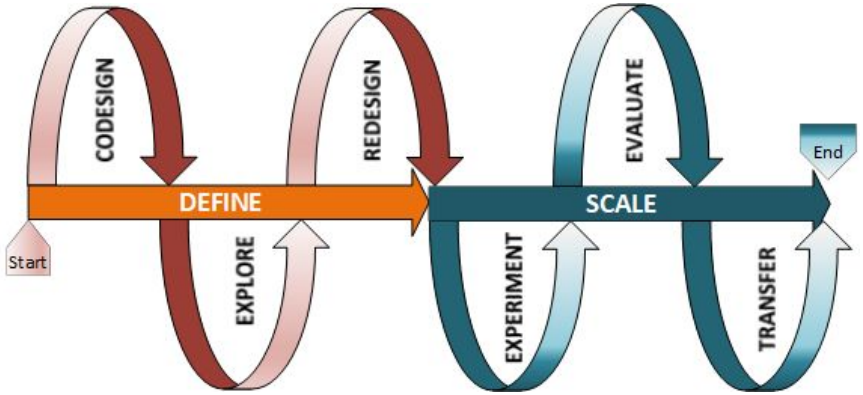
securing cyber infrastructures

Evaluation and Results

Funded by the European Union

Development Methodology

- **Two phases**
  - **Define** – scope, design, and the first implementation
  - **Scale** – the second version, evaluation, and transfer of results
- **Two pilots**
  - **Pilot 1** – end users explore prototype, including functionality from open call
  - **Pilot 2** – usability and performance of the Resilmesh system



Funded by the European Union

Cascade Funding

- **Mechanism** of European Commision to distribute public **funding**
- **Beneficiaries** – start-ups, small and medium-sized enterprises (SME), and other
- **Purpose** – uptake or development of digital innovation
- **Technology Centre Prague** (tc.cz) – support for open calls
- **National portal** on the European Research Area (eraportal.sk)
- **Open Calls** in Resilmesh
- **Expert evaluators** evaluate meaningfulness of proposals

Funded by the European Union

Open Calls

- Open Call 1 – **Extend**
  - **Develop technologies** that can extend the capabilities of Resilmesh
  - Call opened in August 2024
  - **4 projects, € 90 K** per project, **9 months** duration
  - **Results:** cloud-based cybersecurity platform, smart buildings managed by SCADA, photovoltaic installations, EV charging infrastructure
- Open Call 2 – **Experiment**
  - **Demonstrate and validate** use of Resilmesh in new use-case domains
  - Call opened in September 2025
  - **5 projects, € 70 K** per project, **7 months** duration
- **Evaluators** – eight evaluations (€ 900 compensation)

Funded by the European Union

Resilmesh
securing cyber infrastructures

Results

- **Short-term outputs**
  - **Tools, algorithms,** and **processes** to improve cyber resilience of critical infrastructure
  - Cyber situational awareness becomes a **practically applicable** concept
- **Technology Readiness Level**
  - Improvement **from 3 – 5 to 5 – 7** depending on individual components
- **Long-term outcomes**
  - **Increased resilience** and **awareness** of security sector and service providers
- **Open calls** represent opportunities to participate
- **Horizon Booster** supports dissemination and commercialisation

Funded by the European Union

Resilmesh
securing cyber infrastructures

Thank you
for your attention!

Questions?

Project's website: resilmesh.eu
Contact: sadlek@ics.muni.cz

Funded by the European Union