DYNAMO - Dynamic Resilience Assessment Method including combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors

Critical sectors and infrastructures, such as energy, transportation, and health, are key drivers for technological, organisational, social, and economic innovation and well-being for individuals and the society. Sustainable progress in these domains depends on the availability of a continuous business even when disrupted by a cyberthreat. It is clearly observable that systems and infrastructures will become more complex in the future and the failure of a single element increases the probability of producing cascading effects with unexpected consequences. The scope of DYNAMO is to combine the two fields of business continuity management (BCM) and cyber threat intelligence (CTI) to generate a situational awareness picture for decision support across all stages of the resilience cycle (prepare, prevent, protect, response, recover). Professionals from different backgrounds will work together with end-users to develop, refine, and combine selected cybersecurity and BCM tools into a single platform to provide decision support and awareness to Chief Information Security Officers (CISOs), cybersecurity practitioners and other stakeholders. The initiative focusses on the needs of end-users operating in critical sectors and support of their daily tasks. DYNAMO is applicable also in the business practices of SMEs lacking the knowledge and resources to afford CISOs or several cybersecurity practitioners combining this role with competences comprehensive enough to assist the daily tasks and react to potential cyber threats.

In alignment to end-user needs, human factors, high ethical standards and societal impacts, DYNAMO includes the following goals:

Resilience assessment as basis for BCM

- An assessment with different levels of detail, offers with varying existent data a fast or detailed evaluation of the investigated sector and helps to identify critical processes.
- End-user data will be integrated to measure determined performance targets. With respect to the functional description, AI-based approaches will be used for a deeper understanding and potential self-learning of the interconnected processes.
- The results generate knowledge concerning susceptibility and vulnerability of the investigated sector.
- The solutions support the BCM with respect to the five resilience phases.

Leveraging CTI

- CTI will be improved with respect to existing solutions (H2020 ECHO, PANACEA).
- The H2020 Early Warning System (EWS) will be extended and integrated. A Malware Information Sharing Platform (MISP) will be used to raise the situational awareness between different security actors.
- The CTI approach delivers data that will be integrated into the resilience and BCM approach. The use of AI will support the development process. Developed solutions will be integrated with the Cyber Knowledge Graph to visualize the analysis of threat intelligence.

DYNAMO

The **multilevel approach of DYNAMO** addresses five phase representation of the resilience-cycle and helps to:

- Identify critical assets and functions of a critical sector (prepare);
- Consider cyber-risks which are known, but also acknowledge the unknown (prepare, prevent);
- Save sensitive data (prevent, protect);
- Test the response plan to ensure the effectiveness (prepare for later response);
- Train business stakeholders concerning their responsibilities before an attack with the simulation of a potential attack (prepare) and during an attack (response);
- Integrate AI-based solutions to accelerate the recovery behaviour (recover);
- Measure the effectiveness (return of investment) of resilience enhancement measures in alignment to the 4 R's of resilience (rapidity, robustness, resourcefulness, redundancy);

By integrating the previously listed tangible outcomes, the DYNAMO approach will support different stakeholders of critical sectors to increase their resilience situational awareness.

The DYNAMO platform will be able to collect organisation's skills data, elaborate and create tailored organisational training to improve organisational resilience which will be demonstrated within three different (cross-) sectoral use-cases.

Find out more about this Project:
https://horizon-dynamo.eu/

DYNAMO

Project Coordinator

Fraunhofer EMI , GERMANY

Project Coordinator Support

Technikon, AUSTRIA

Call: HORIZON-CL3-2021-CS-01 (Increased Cybersecurity 2021)

Topic: HORIZON-CL3-2021-CS-01-01

Budget

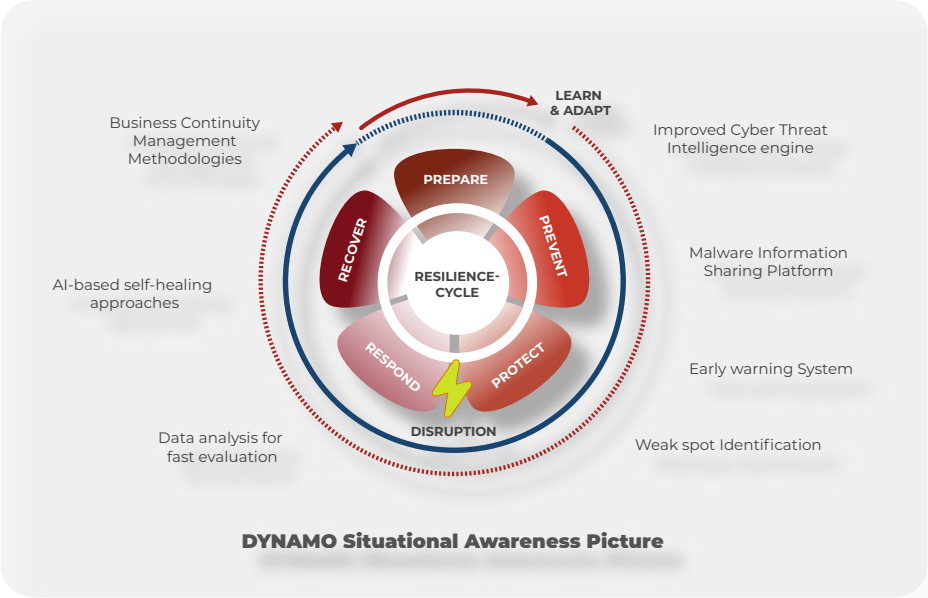
€ 5 Million
100% EU-funded

Consortium

15 Partners
10 Countries

Duration

36 Months
10/2022 - 09/2025



DYNAMO Situational Awareness Picture

The DYNAMO platform will be iteratively developed, with explicit end-user joint application development (JAD) activities. In every phase of the project, and in every activity, there is close stakeholder cooperation, both through the DYNAMO stakeholder reference group (SRG), the scenario development teams and their local support partner(s), and through interaction with associated project partners and their networks. Every step includes feedback sessions with stakeholders, for requirements gathering, analysis, design, development, and prototyping. Evaluation trials for benchmarking as well as stakeholder consultation and impact creation activities will all be implemented to refine use-cases and user requirements, deeply rooted in practice, and clearly identifying end users' needs. In general, the systematic integration of end-user considers the identification of what is currently applied and what is missing; the definition of requirements, use-cases; the evaluation/verification of intermediate results; the application of the DYNAMO platform; how to empower with DYNAMO capabilities, aligned to DYNAMO principles.

Partners

1. Fraunhofer Institute for High-Speed Dynamics Ernst-Mach-Institut (Fraunhofer EMI) Germany
2. Technikon Forschungs- und Planungsgesellschaft mbH, Austria
3. Ethniko Kentro Erevnas Kai Technologikis Anaptyxis, Greece
4. Factor Social - Consultoria em Psico-Sociologia e Ambiente, Portugal
5. Laurea-ammattikorkeakoulu OY, Finland
6. Naval Group Belgium, Belgium
7. Kentro Meleton Asfaleias, Greece
8. KPMG, Ireland
9. VisionSpace Technologies Gmbh, Germany
10. Telelink Business Services Group, Bulgaria
11. Fondazione Policlinico Universitario Agostino Gemelli IRCSS, Italy
12. RHEA Group, Belgium
13. CRBC, CUBS, UCC, Ireland
14. IRT SystemX, France
15. ENGIE Laborelec, Belgium

Funded by the European Union

Funded by the European Union under grant agreement no. 101069601. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Follow DYNAMO on:

@DYNAMO_HEU

DYNAMO Horizon Europe project 101069601