March 2025 | 3rd Newsletter

DYNABIC NEWSLETTER

Edition 1, No. 3

Content :

- Initial version of the DYNABIC Components
- Second DYNABIC Day and Hackathon
- DYNABIC Key Exploitation Results Videos
- Forthcoming events

First evaluation of the DYNABIC Components - Special mention of NIS2 Directive

During the fourth quarter of 2024, the first evaluation of the 7 DYNABIC key exploitable results has been conducted. This evaluation was made in the context of our four use cases in the Transportation, Health, Energy, and Telecommunications domains. The evaluation was very positive, and all the tools proved to be highly innovative and relevant.

The assessment of the NIS2 Directive implementation and coverage by the DYNABIC framework was also performed. This assessment aimed to evaluate the validity and completeness of the threat intelligence generated by the solution. Experts from the DNSC partner in DYNABIC, the Romanian CERT authority, were provided with detailed descriptions of threat information events produced by CTI4BC (Cyber Threat Intelligence and Incident Reporting tool). These events incorporated inputs from other DYNABIC components: (i) security events from AWARE4BC (Cyber-physical system Monitoring and Business Continuity Situational Awareness component), (ii) risk profiles and information from RISK4BC (Real-time Risk Management for Business Continuity component), and (iii) incident response information from SOAR4BC (Security Orchestration Automation and Response for Business Continuity component). The evaluation focused on key areas such as timely incident reporting, structured and actionable sharing, risk assessment and management, incident response, data privacy and anonymization, and human-in-the-loop validation. While the experts generally confirmed that the evaluated NIS2 requirements were correctly implemented, they also provided feedback and suggested improvements for the final version.

We will leverage the feedback from the use case providers and stakeholders to improve our solutions in the second phase of the project. A final evaluation will be conducted in the second half of 2025. The open access components will soon be made available on the DYNABIC GitLab repository, stay tuned!

Second DYNABIC Day & Hackathon

The Second DYNABIC-Day was organized in January in Sophia Antipolis, France. The event provided DYNABIC with the opportunity to meet companies and to introduce our use case in the EV charging station domain and two of our key exploitable results: AWARE4BC for security and situational awareness and SIM4BC for threats simulation.

Late January we organized the DYNABIC Hackathon in University Côte d'Azur (Nice, France). The event gathered over 100 attendees, bringing together students and professionals. The Hackathon's primary objective was to showcase and evaluate the advanced software tools developed within the

More specifically, two software tools focusing on Dynamic Business Continuity and enhancing the resilience of critical systems against advanced cyber-physical threats were presented:

- Risk Management Tool (RISKM4BC)
- Incident Detection and Resilience Monitoring Tools (AWARE4BC)

The experimental scenario, provided by Ferrovial (a portugese Highway Operator), consisted in simulating a potential cyberat-

Forthcoming Events

- 3rd ECSCI workshop; April 2025
- **DYNABIC at the Hacking village of the Barcelona Cybersecurity Congress**
- STAM workshop at ARES 2025

By the end of the hackathon, participants were provided with a survey providing us with relevant feedback and suggestions for improvement. Overall, the first feedback from the participants was very positive! The team will reports these results in a forthcoming research paper!

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070455. **Disclaimer:** Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the European Commission can be held responsible for them.

DYNABIC NEWSLETTER

March 2025 | 3rd Newsletter

Clusters & Synergies:

- European Cluster for Securing Critical Infrastructures (ECSCI)
- Innovation Cluster for Electrical Power and Energy Systems (CyberEPES)
- EC Horizon Results Booster (HRB)
- ECCO's group on resilient systems.

Videos of the DYNABIC Key Exploitation Results

MADT4BC

AVATAR4BC

SIM4BC

CTI4BC

AWARE4BC

SOAR4BC

RISKM4BC

DYNABIC Consortium

dynabic@gmail.com

@DYNABIC

@DYNABIC

https://dynabic.eu

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070455. **Disclaimer:** Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the European Commission can be held responsible for them.