PRESS RELEASE

The ECHO network closed its operation by presenting the innovative cybersecurity software solutions developed under the project

4 years, 32 consortium partners, 14 additional consortium participants, 20 EU countries, 6 innovative cybersecurity assets, 14 software prototypes, 18 technology roadmaps, 7 demonstration cases, 45 demonstration videos, 97 scientific publications – and a lot of effort, research, joint work, expertise, and knowledge sharing. The ECHO project, launched by the European Commission to pool the knowledge of European ICT professionals to strengthen the EU's autonomous cyber defense, celebrated its highly successful operation with a final event involving all partners at the Royal Military Academy in Brussels.

In 2018, the European Commission, under the umbrella of the H2020 Programme, selected four pilot projects to address the Horizon 2020 Cybersecurity call “Establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap”.
Four years later, on 24 February 2023, the ECHO project (the European network of Cybersecurity centres and competence Hub for innovation and Operations) held its closing event at the Royal Military Academy premises in Brussels. With a consortium consisting of 32+14 partners from public, private, and research organisations from 20 member states, many innovative solutions and cutting-edge technologies have been developed, tackling significant cybersecurity challenges. The event included presentations, demonstrations, and feedbacks, highlighting the effectiveness and impact of the project’s outcomes in strengthening the proactive cyber defense of the European Union and enhancing Europe’s technological sovereignty through effective and efficient multi-sector and multi-domain collaboration.
Six key assets have been developed by the project:

- ECHO Early Warning System: a secured and collaborative information-sharing platform of cyber-relevant information;
- ECHO Multi-sector Assessment Framework: transverse and inter-sector needs assessment and technology R&D roadmaps;
- ECHO Federated Cyber Range: an advanced cyber simulation environment supporting training, R&D, and certification and a market platform for cyber ranges and cyber-related services;
- ECHO Cyber Skills Framework: Cyber skills reference model and associated training curriculum;
- ECHO Security Certification Scheme: development of sector-specific security certification needs within the EU Cybersecurity Certification Framework from ENISA as a benchmark of cybersecurity certification to be obtained as a market differentiator;
- ECHO Governance Model: management of direction and engagement of partners and of the transition to the project's future network.

In addition to these, ECHO Early Warning System plug-ins, several software prototypes, and two technological roadmaps have been developed and put at disposal of the European cybersecurity community (AI CISO and AI ML Cybersecurity for Aviation Space and Maritime Autonomous Transport Roadmaps). The ECHO consortium has achieved with its outcomes significant results in addressing pressing cybersecurity challenges in many areas. By developing and implementing innovative solutions and technologies, with effective cooperation and embracing a culture of continuous innovation, the project has remained agile and responsive. The consortium's commitment to advancing the field of cybersecurity in the EU will even continue after the formal end of the project, with the transformation from the ECHO project organization to a Collaborative Networked Organization (CNO), further exploiting the developed assets, software prototypes, and other innovations.

'ECHO produced tangible valuable technical results: we managed to provide a direct contribution to many cybersecurity research and innovation topics and directly mitigate several important challenges identified in 2018 at the European level. Our technical outputs reached a high technical readiness level, thanks to a rigorous engineering, market-oriented process: a portfolio of products and services, ready to be exploited in the market and ranging from federation of cyber ranges, cyber threat intelligence processing and sharing, risk analysis, and sector-specific training portfolio.
During our journey, we demonstrated, together with the other three Pilot Projects, that a large European community including academia, research, and industry (small, medium, and large) can work very effectively together towards common goals, bridging the gap between research and industry and advancing the state-of-the-art for the benefit of the entire community. This is one of the most valuable results of our efforts: building a strong community that will work together in the next years and constitutes the first vibrant embryo of the European Cybersecurity Competence Centre' – agreed the leaders of the project, Prof. Wim Mees, Project Coordinator, from the Royal Military Academy of Belgium and Matteo Merialdo, Project Implementation Coordinator, from RHEA Group.

more information: www.echonetwork.eu
contact for further interviews: Matteo Merialdo, m.merialdo@rheagroup.com