CONCORDIA, ECHO, SPARTA and CyberSec4Europe Outcomes and beyond!

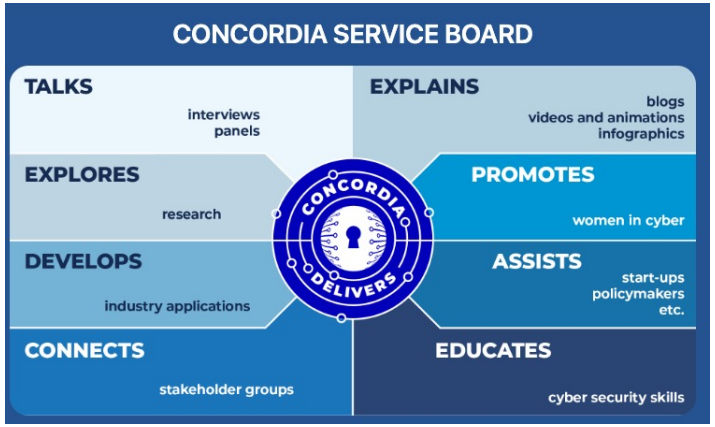
Despoina Antonakaki (FORTH, TUC)

despoina@ics.forth.gr – dantonakaki@tuc.gr

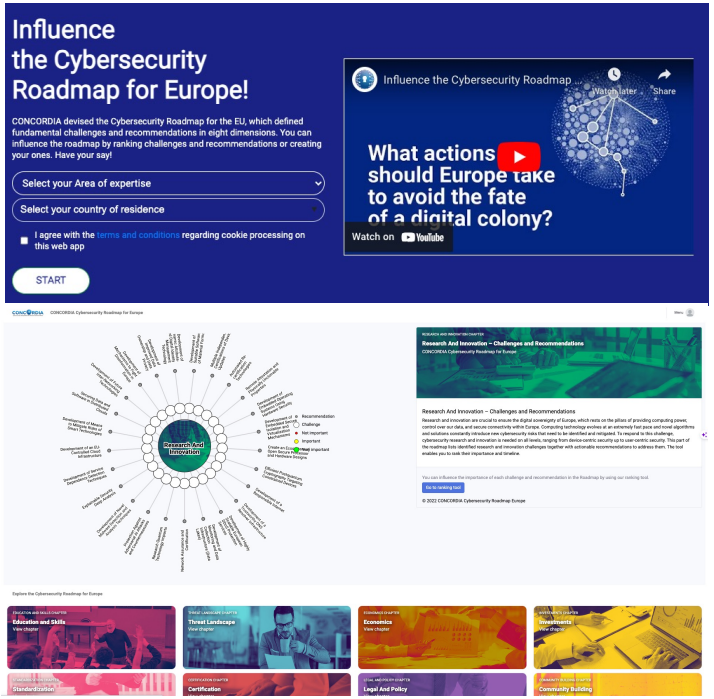
Achieved objectives - experiences

- Delivered 21 results strengthening EU cybersecurity [Policy, Technology Tools, Education, Technology Pilots, Certification and Research(> 300 scientific publications)]
- CONCORDIA & pilots ecosystem positioned in a Cybersecurity Competence Network with leading research, technology, industrial public competences to build the European Secure, Resilient and Trusted Ecosystem, with CODE research centre as coordinator and hub, and ENISA as secretary.
- Links technical and social sciences
- 56 institutions across EU, consisting multi-stakeholder ecosystem from industry, start-ups, public bodies:
  - Universities, Research centres, Private companies & Public bodies from 17 EU member states & Switzerland, Norway, Israel and UK, coordinated by University of Bundeswehr Munich.

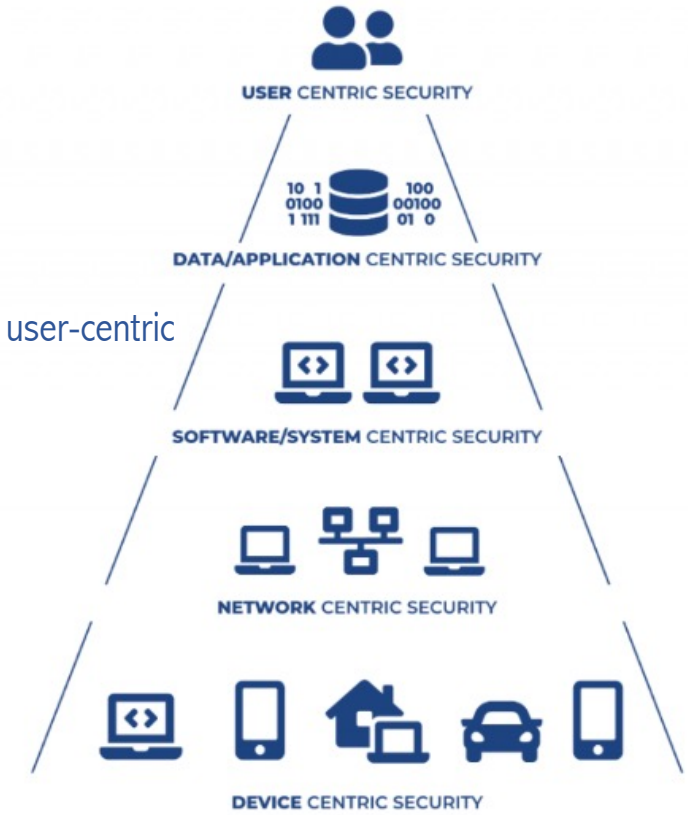
- The four-year (2019- 2023) €16M project (plus €7M industrial funding) covered a wide range of topics
  - cyberattacks on critical infrastructure
  - information security and data protection
  - certification
  - competence building
- Using an open, agile and adaptive governance model and processes.



Achieved objectives - experiences

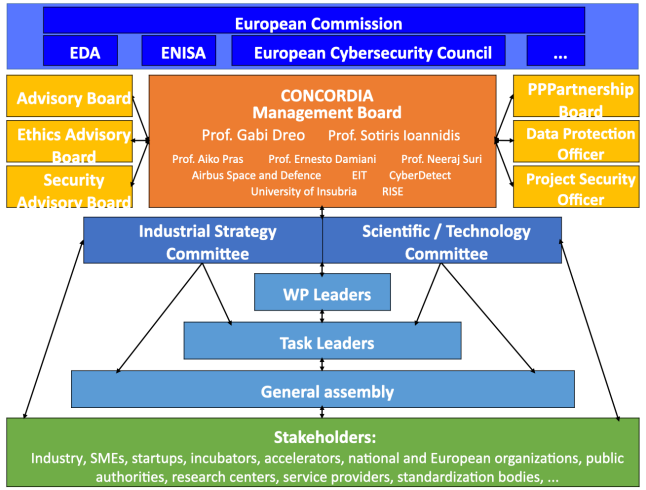


- Devised a CS roadmap to identify powerful research paradigms:
  - hands-on experimental validation,
  - prototype and solution development - agile way - quickly identify successful/unsuccessful potential product development
- Developed next-generation CS solutions
  - holistic end-to-end data-driven approach from:
    - data acquisition
    - data transport
    - data usage
- addressing device, network, software-system, data-application and user-centric security.



- Scaled up existing research and innovation with virtual lab and services.
- Identified marketable solutions - grew pioneering techniques towards fully developing their transformative potential.
- Developed sector-specific (vertical), cross-sector (horizontal) industrial pilots with building incubators

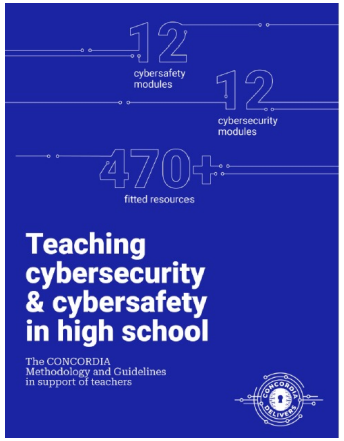
Achieved objectives - experiences



- Open Calls- entrepreneurs & individuals: stress their solutions with development.
- Advisory Board: leaders of industry, standardization, policy and politics
  - strategic advice
  - connect with possible clients & users of developed solutions, other projects and research initiatives & important standardization and certification institutions
- CONCORDIA Monitoring Board has been developed for continuous gathering of feedback from CS community.

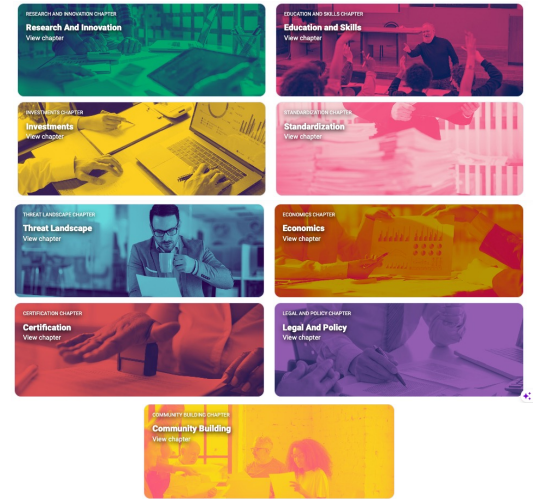
Mediated between multiple communities

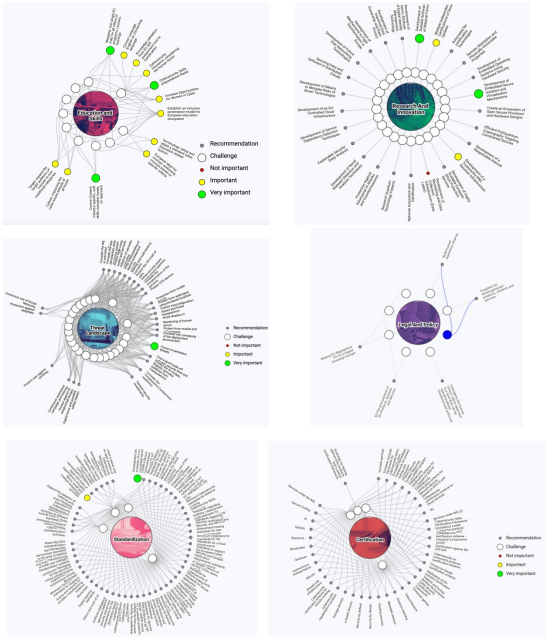
- Established European Education Ecosystem for Cybersecurity
- Extended traditional training courses with new virtual courses (MOOCs and SPOCs) - outreach activities, including high-school curricula development, competitions, cyber ranges
- Provided expertise to European policy makers and industry



Outcomes, lessons

- Results provide valuable input to ECCC & NCCs:
  - ➢ to whole European CS community,
  - ➢ strengthen & speed up research, development & innovation
- Set strategic recommendations for CS in EU published under Roadmap for Cybersecurity in Europe.
  - R&I, education, economics and investment, law, and certification and standardization in a holistic way.
- Revised new strategy describing nine fundamental dimensions affecting CS, - where current focus should be.





- KYPO Cyber Range Platform awarded by 2021 EC Innovation Radar competition in Disruptive Tech category
- Defence against DDoS attacks addressed by DDoS Clearing House
- Sharing data and experience of experts in face of attacks, helping & prepare organizations
- Developing Cyber Threat Intelligence platforms for telco and finance sectors

https://concordia.monitorboard.nl/roadmap/

Policy

What is it and what is it intended for?

What action should Europe take to build and sustain resilience and digital sovereignty?

CONCORDIA CS Roadmap defined fundamental challenges and recommendations in nine dimensions.

- Threat Landscape
- Research and Innovation
- Education and Skills
- Economics
- Investments
- Legal and Policy
- Certification
- Standardization
- Community Building

1.https://www.concordia-h2020.eu/roadmap/
2.https://concordia.monitorboard.nl/roadmap/

What is it and what is it intended for?

Women in Cybersecurity initiative is a CONCORDIA task implementing actions to incentivise women to join the field of cybersecurity.

- We created a Women in Cyber – A Manifesto for TODAY, a document stating CONCORDIA's objectives for women's inclusion.
- To achieve these goals, we focused on three types of actions:
  - Diversity & Cybersecurity webinars,
  - Awards for Women in Cyber
  - Women in Cyber role models gallery of postcards.

1.https://www.concordia-h2020.eu/concordia-service-women-in-cybersecurity/
2.https://www.concordia-h2020.eu/wp-content/uploads/2019/09/WomenInCyberMANIFESTO.pdf

What is it and what is it intended for?

Build a community and establish a liaison with stakeholders. Different institutions represent different competencies and, with their different levels of involvement, that's why we introduced three stakeholders groups involved parties could join:

- Cybersecurity Competence Centers and Agencies Stakeholders Group (NSG),
- Observer Stakeholders Group (OSG) and
- Liaisons Stakeholders Group (LSG).

Reached >500 people (300 European organizations) to inform

- Newsletter every three months,
- Providing security expertise, & CS research,
- Joining discussions in EU institutions
- Open Door event every October

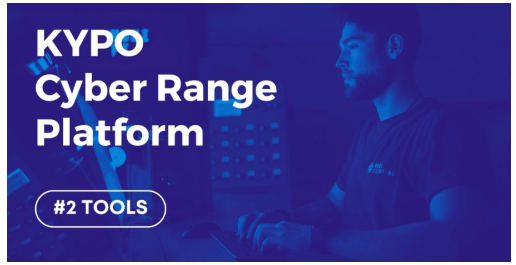
1.https://www.concordia-h2020.eu/concordia-service-community-pact/
2.https://www.concordia-h2020.eu/wp-content/uploads/2021/03/Deliverables_D4.8.pdf

Tools

What is it and what is it intended for?

KYPO Cyber Range Platform is a flexible, scalable, and sophisticated virtual environment. [Masaryk University since 2013].

- Several years of experience using cyber ranges in education, cyber defense exercises, and training.
- CONCORDIA project released KYPO CRP as open-source in 2020.
- Aims to help solve high amount of missing CS experts by providing a platform for development, and execution of CS training and exercises.



1.https://crp.kypo.muni.cz/
2.https://twitter.com/KYPOCRP

What is it and what is it intended for?

To build a comprehensive European cybersecurity ecosystem, we focus on cybersecurity's technical and economic aspects.

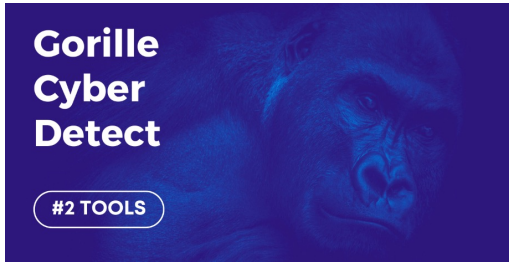
- CyberTEA defines a clear methodology for CS planning and investments.
- integrates set of **tools** to help decision-makers during the different planning steps.
- (i) SECAdvisor, calculates optimal investment in CS based on different economic models like Gordon-Loeb and ROSI,
- (ii) MENTOR, supports CS management to recommend services for the prevention and mitigation of cyberattacks, and
- (iii) SecBot, conversational agent focuses on helping non-experts users to make informed and efficient CS decisions.

1.https://www.concordia-h2020.eu/blog-post/on-the-cybersecurity-planning-and-investments-an-approach-with-economic-bias/
2.https://www.youtube.com/watch?v=QYdGO_rxj5s

What is it and what is it intended for?

Gorille is an innovative malware detection tool [by start-up Cyber-Detect & University of Lorraine].

- Can identify most sophisticated attacks that bypass traditional defence systems based on morphological analysis.
- Allows precise identification of malware families and can address significant attack analysis and remediation tools.



http://www.cyber-detect.com/

What is it and what is it intended for?

Flowmon Probe QUIC plug-in – capability to identify QUIC traffic in the network, extract server name indication (SNI) from handshake and export the SNI as part of enriched metadata using IPFIX protocol.

1.https://www.flowmon.com/en/blog/flowmon-anomaly-detection-misp
2.https://www.concordia-h2020.eu/blog-post/quic-protocol-from-the-monitoring-perspective/

Education

What is it and what is it intended for?

Based on desk research followed by a market validation, we identified a set of knowledge and skills a CS consultant should have.

- Our partners and we created a course called **Becoming a Cybersecurity Consultant,** suitable for **professionals**, CS middle managers, and freelancers.
- After successfully finishing the course in full, the participants are eligible to apply for the C^3 by CONCORDIA certification exam.

1.https://www.concordia-h2020.eu/becoming-a-cybersecurity-consultant/

- **What is it and what is it intended for?**
- The CONCORDIA Governance model for a European Education Ecosystem in Cybersecurity is building on the experience and knowledge accumulated during the project, on several education related activities.
- After identifying the challenges of the ecosystem at the European and national level, and revising different cybersecurity /education related governance models, the document presents the ingredients of a possible governance model.

1.https://www.concordia-h2020.eu/wp-content/uploads/2023/02/CONCORDIA_Governance_model_for_EEEC.pdf

What is it and what is it intended for?

One of the outcomes of CONCORDIA is the Methodology and Guidelines to support high school teachers.

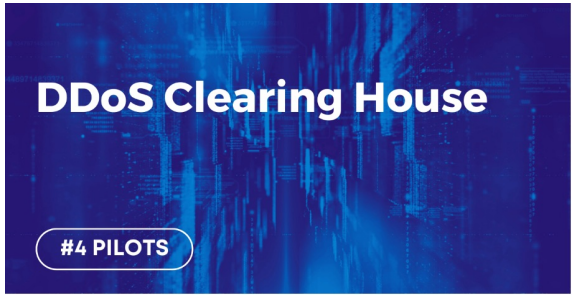
- Methodology proposes an approach based on 3 steps, and suggests building a needs-based and knowledge-based modular portfolio of lessons.
- > 470 targeted resources, Guidelines include 12 cybersafety modules, with topics such as hate speech or fake news, and 12 cybersecurity modules that can help to teach about cyber hygiene, protection of data or, for example, how a computer works.
- Also pointing to related initiatives deployed in different European countries.

1.https://www.concordia-h2020.eu/wp-content/uploads/2022/11/Teach-the-TeachersMethodology-for-publication.pdf

Pilots

What is it and what is it intended for?

- The DDoS Clearing House is a platform used for sharing measurements of DDoS (meta) data between organizations.
- By sharing data and expertise of DDoS attacks, organizations broaden their view of DDoS landscape to an ecosystem wide one, enablin a more proactive and collaborative stance in fighting DDoS attacks.
- We piloted the system in Netherlands and Italy, and it be deployed in production in Dutch anti-DDoS coalition.



1.https://www.concordia-h2020.eu/wp-content/uploads/2023/03/PREPRINT-D3-6_DDoS_Clearing_House_Cookbook.pdf

What is it and what is it intended for?

- CONCORDIA Financial Threat Intelligence Platform adapted to financial entities' needs.
- Provides set of add-ons that work over MISP enhancing security and privacy when threat intelligence information between entities is being exchanged.
- Dashboard has several functionalities, [defining concrete and fine-granular sharing groups to change data and selecting encryption or anonymization details for specific IoC types and fields]
- Automate anonymised information sharing process and score incoming IoCs based on threats trends.

1.https://www.youtube.com/watch?v=cVMmTZTauLE&feature=youtu.be

What is it and what is it intended for?

- In secure communication pilot, we delivered three solutions contributing to security of vehicular communication systems.
- Providing lightweight, hardware-based post-quantum secure authentication as an enabler for all future interaction between vehicles.
- Developed methodology for studying attack propagation in collaborative missions during mission design, planning and execution, and provided an implementation.
- Delivered a fast and efficient routing algorithm to dynamically respond to communication needs.

1.https://ieeexplore.ieee.org/document/9583701

Pilots

What is it and what is it intended for?

- CONCORDIA telecom sector pilot's main objective was to extend and enhance the CONCORDIA Threat Intelligence Platform with three use cases.
- Focused on automated processing of threat intelligence information, preventing flood attacks from IoT devices and handling privacy and anonymity with machine learning.

1.https://youtu.be/vmj_6DjV6Iq
2.https://www.concordia-h2020.eu/sector-specific-pilots/

What is it and what is it intended for?

- Mobile Threat Modelling Framework is a compatible combination of the enterprise, mobile and ICS matrices of the MITRE ATT&CK framework.
- The first iteration of this framework intends to adapt and grow – as we see the need to accommodate more techniques as more attacks become known.
- Our perspective is to have this framework as a de-facto model for all members of the telco cybersecurity (& sharing) community.

1.https://www.concordia-h2020.eu/blog-post/cyber-threat-modelling-for-telco/
2.https://www.concordia-h2020.eu/blog-post/concordia-mobile-threat-modelling-framework/

What is it and what is it intended for?

- FLaaS is a service that enables SMEs and other third-party entities (e.g., mobile application owners) to build Machine Learning (ML) models that help their apps (e.g., for better recommendations, user modelling, etc.).
- Crucially ML learning is performed on user devices, and not on servers of entities, using principles of Federated Learning (FL).

1.https://arxiv.org/pdf/2206.10963.pdf
2.https://dl.acm.org/doi/abs/10.1145/3498361.3539693

What is it and what is it intended for?

- E-health pilots work on digital transformation in health service sector, mainly focus on capturing security and privacy.
- First use-case: medical devices at home that send data between home and the doctor/health care authorities via a secured communication channel.
- Essential to ensure digital identification of the patient, secure data storage, home infrastructure and communication – for today's Wifi world and the 5G near future.
- Open platform addresses mainly EU citizen, as buyer and as user.

1.https://www.concordia-h2020.eu/blog-post/smart-home-and-remote-health-services
2.https://www.concordia-h2020.eu/blog-post/new-shape-of-health-care-with-edge-devices/

Certification

What is it and what is it intended for?

- Information-centric networking is an emerging alternative to host-centric networking designed for large-scale content distribution and stricter privacy requirements.
- This research focused on protecting the network from attacks targeting the content delivery protocols while assuming genuine content can constantly be retrieved from trustworthy nodes.

1.https://ieeexplore.ieee.org/abstract/document/9750109

What is it and what is it intended for?

- C^3 by CONCORDIA is a certification scheme for the cybersecurity consultant role. It is intended to be used by organizations wishing to provide evaluation and certification of the knowledge and skills of professionals based on the Cybersecurity Consultant role profile created by the CONCORDIA project.
- The scheme fulfils the requirements for cybersecurity skills schemes of ISO 17024.

1.https://www.concordia-h2020.eu/wp-content/uploads/2021/11/Concordia_Certification_SchemeC3_v1.pdf

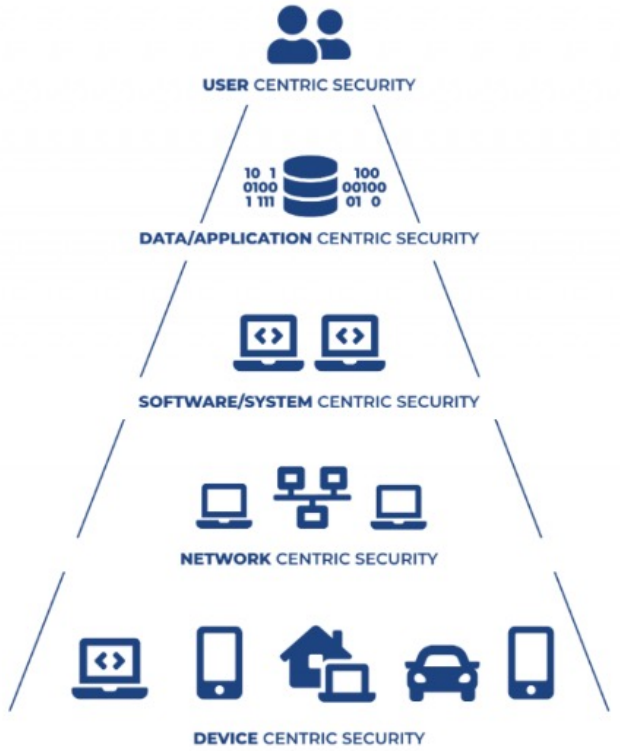
What is it and what is it intended for?

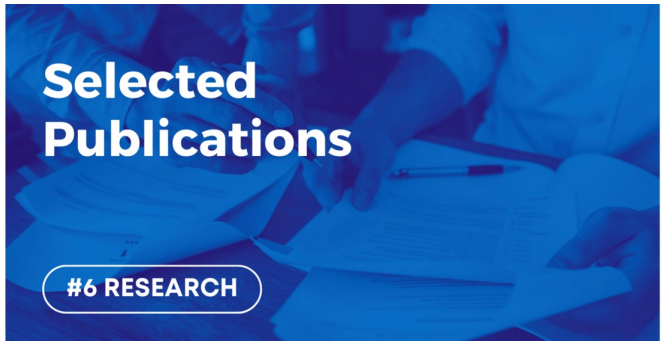
- The CONCORDIA participated through a number of partners in the consultation of the draft version of the EUCS candidate scheme (European Cybersecurity Certification Scheme for Cloud Services).
- Certification scheme for (cloud) services awards a certificate to a service in case it holds a given non-functional property (e.g., confidentiality, integrity, availability).
- Services are then selected on the basis of the released certificates.

1.https://ieeexplore.ieee.org/document/9844845

Research

- The research activities organized into five tasks, each focusing on a particular aspect of cybersecurity.
- Total number of papers entered into EU-ECAS system is even higher since white papers and papers without peer review are not counted.
- Our publications on our website.





Security Aspects	2019	2020	2021	2022	Total
Device	10	23	19	25	**77**
Network	9	30	15	20	**74**
Software and system	8	13	4	7	**32**
Data and application	16	15	18	12	**61**
User security and privacy	16	26	20	18	**80**
Total	**59**	**107**	**76**	**82**	**324**

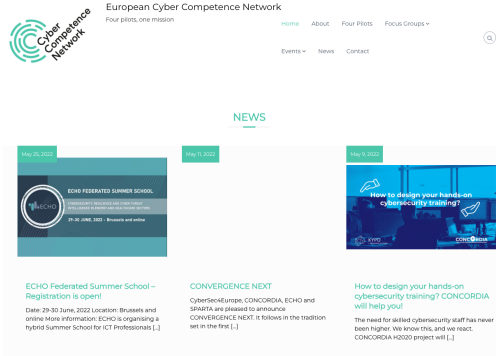
Pilots - CONCORDIA & ECCC

- Horizon 2020 CS call *"Establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap"*.
- Purpose: ECCC & NCCs:
  - retain and develop the CS technological and industrial capacities of EU
  - strengthen and sustain Europe's CS competence
- Different - complementary approach to shared common goals.
- Cooperated & coordinated activities extensively
- Activities: demonstration test- and use-cases in eHealth, finance, telecommunications, smart cities and transportation.
- Use of cyber ranges, training & education programmes
  - Deliver innovative marketable solutions (EU)
  - ➢ address future cross-domain CS challenges to security of Digital Single Market.

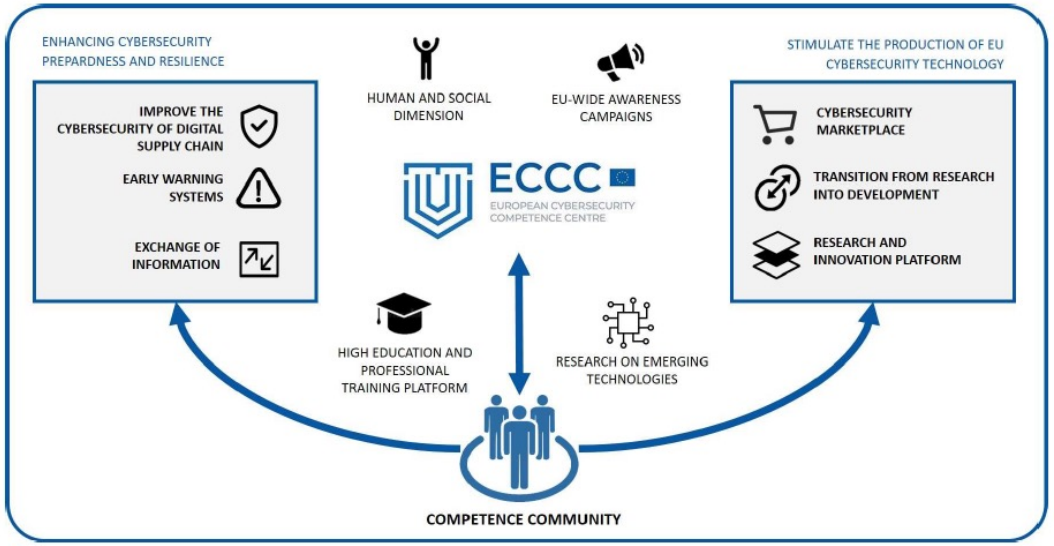
- *We are counting on CONCORDIA, ECHO, SPARTA and CyberSec4Europe to assist us in pooling Europe's cybersecurity expertise and preparing the European cybersecurity landscape in order to efficiently implement our vision for a more secure digital Europe. These projects will assist EU in defining, testing and establishing the governance model of a European Cybersecurity Competence Network of cybersecurity centres of excellence.*

[Joint Communications Cyber Competence Network presentation – June 2021Commissioner for Digital Economy and Society Mariya Gabriel]

- Pilot projects brought together > 160 partners [large companies, SMEs, universities, CS research institutes, from 25 EU Member States and 5 non EU Member States].



Pilots - CONCORDIA & ECCC



Strategic directions for contributions of Competence Community

Views for the ECCC needs input from the community, such as creative ideas and stakeholders' investment priorities.

It's essential to connect to create a fast information loop between the coordination centres and the communities (provide a communication platform).

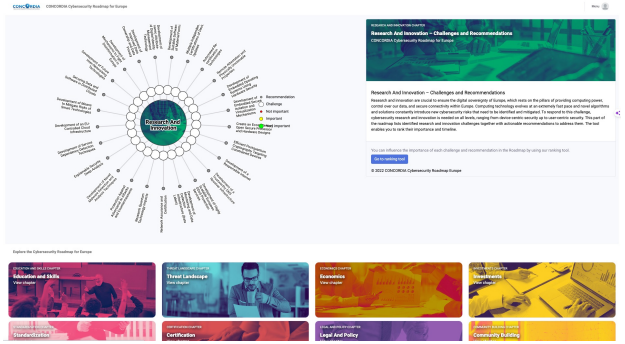
To be part of the community is a commitment to cooperation.

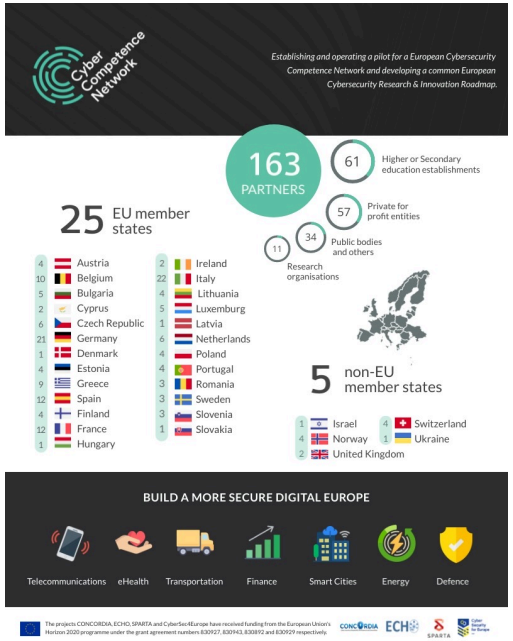
How can the community help the ECCC?

Four pilots ...one mission

- Opened the way for ECCC& NCCs
- Inter-Pilot Roadmap:
  - SPARTA – Technology
  - ECHO - Technology
  - CyberSec4Europe – Composite Tech/App Domains
  - CONCORDIA – Holistic Cybersecurity

Outcome: Integrated Inter-pilot roadmap as input to ECCC/NCCs





2nd ENISA Cybersecurity Market Analysis Conference

https://cybercompetencenetwork.eu

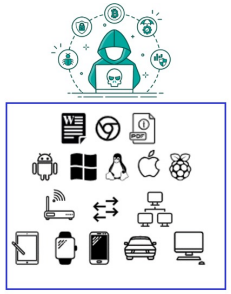
Key Takeaways & beyond…

Investigation during CONCORDIA project sets a clear path for the understanding and adoption of cybersecurity under an economic bias

CS Planning and Economics

Key Takeaways:

- Risk management is an important pillar for CS planning
- Automation needed as input for many planning tasks
- Identification, evaluation & mitigation of risks
- Several frameworks/certifications available, different complexities
- SMEs still struggling with them
- Costs vs Expertise vs Awareness
- CS economics provides models and benchmarks for decision-making
- There is no one-fit-size approach, but real-world applications are possible and needed
- CS roadmap shows long path for next years: costs due to cyberattacks and proactive/reactive mitigation as key pillars



Looking Ahead

- Spin-off projects on CS and economics, certifications, and education
- Move knowledge obtained to market: validate models & benefit real-world users
- Continue evolving tools developed to address CS planning gaps and challenges
- Data gathering, collaborative approaches, and investments decisions

Next projects ECCO:

- ECCO – European Cybersecurity Community [Cybersecurity Community support]
- ECCO - "the European Cybersecurity Community" - is the response to the Tender of the Commission for the support to the development of the European Cybersecurity Community.
- ECCO project is supporting the ECCC and NCCs in building the community, organising events

ECCO
European Cybersecurity COmmunity

ECCO WG on skills

In the ECCO Community Working Groups we present common proposed objectives well connected to ECCO's skills strategy, the European Cybersecurity Skills Academy and aspects linked to the ECCC Strategic Agenda.

Community WG objectives

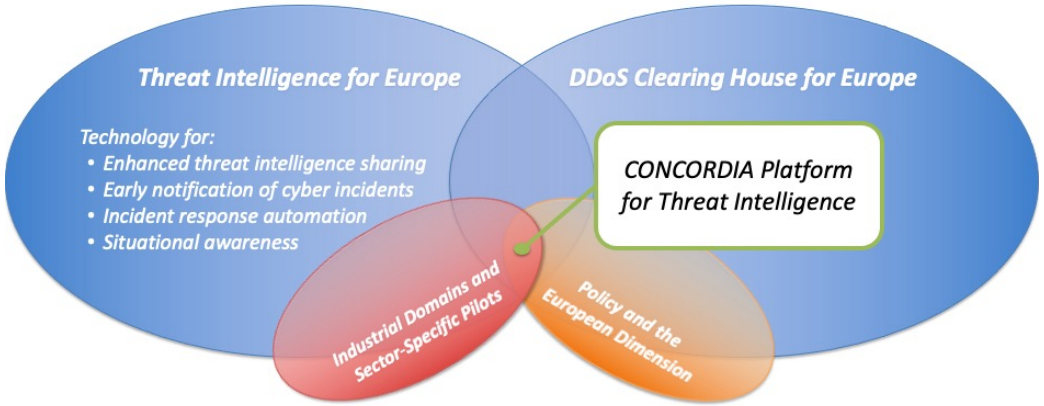
- Build community of experts on skills.
- Promote development of skills and capabilities of cyber- professionals
- Support alignment of curricula in higher education with workforce demand across EU-27.
- Provide recommendations on filling the gaps in professional certification and attestation of skills in cybersecurity
- Facilitate collaboration/common approaches among relevant stakeholders.

If you are interested in joining the ECCO Community WG on Skills, contact Despoina Antonakaki dantonakaki@tuc.gr

ECCO
European Cybersecurity COmmunity

Key Takeaways & beyond…

Threat Intelligence



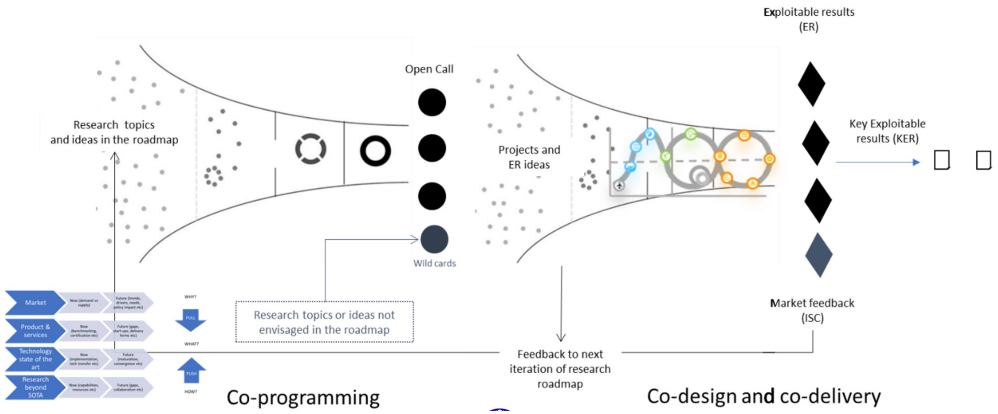
Looking Ahead

- A blueprint for Threat Intelligence handling
- Promoting the CONCORDIA Platform for Threat Intelligence
- Improving the quantity and quality of cybersecurity information exchange in Europe
- Technological solutions
- Internal usage in operation
- Customization (e.g., OT-specific threat intelligence)
- External engagement
- Prolonging the engagement with European stakeholders
- CONCORDIA & pilots as a “platform” for follow-up projects

Key Takeaways & beyond…

Exploitation & Incubators

Co-{Programming, Design, Delivery}



Looking Ahead

- 18 recommendations/comments, including:
  - Create for Local/National/EU CC hubs (acked by NCC/ECCC)
  - Community meeting alignments
  - Align industry-led sprints (prototyping/MVP) with research-led design
  - Execute co-programming sessions for prioritization of research roadmap/open calls
  - Execute co-design sessions for build-up of new proposals
  - Execute co-delivery sessions for solutions that stretch over value chain
  - Analyze financing avenues for cybersecurity hubs
- Successful post-project “research to industry” technology transfer strategy
- A possible roadmap for the industrial community building

Thank you!

despoina@ics.forth.gr

dantonakaki@tuc.gr