D3.6 Report on Concertation Activities

Author(s)	Nicholas Ferguson, Trust-IT
Status	Final
Version	1.0
Date	27 July 2021

Dissemination Level

X	PU: Public
	PP: Restricted to other programme participants (including the Commission)
	RE: Restricted to a group specified by the consortium (including the Commission)
	CO: Confidential, only for members of the consortium (including the Commission)

Abstract:
The document also provides an overview of how the Concertation Meetings became an essential platform and springboard for all WPs in the project and became an essential part of the delivery of project assets. It also provides a full summary of the final Concertation meeting which took place in June-July 2021.

The work described in this document has been conducted within the project cyberwatching.eu. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 740129. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

Document identifier: Cyberwatching.eu – WP 3 – D3.6	
Deliverable lead	**TRUST-IT**
Related work package	**WP3**
Author(s)	**Nicholas Ferguson, Trust-IT Services**
Contributor(s)	**Niccolo' Zazzeri & Julie Arteza, Trust-IT Services; Marina Ramirez, AEI**
Due date	**31/07/2021**
Actual submission date	**28/07/2021**
Reviewed by	**Mark Miller & Victoria Menezes Miller, CPT & Justina Beiliauskaite & James Philpot, DSME**
Start date of Project	**01/05/2017**
Duration	**51 months**

Revision history

Version	Date	Authors	Notes
0.1	15/7/2021	Nicholas Ferguson, Trust-IT	ToC Definition
0.2	22/7/2021	Nicholas Ferguson, Trust-IT	Sections 3-5
0.3	23/7/2021	Nicholas Ferguson, Trust-IT	Sections 3-5
0.4	23/7/2021	Marina Ramirez, AEI & Julie Abergas-Arteza	Section 2 event participants and evidence-based impacts, the main takeaways from Concertation 2021 event 1 and 2.
0.5	26/7/2021	Mark Miller / V. Menezes Miller, CPT & James Philpot, Justina Bieliauskaite, DIGITAL SME	Full document internal review and comment
0.6	26/7/2021	Nicholas Ferguson Julie Arteza & Niccolò Zazzeri, Trust-IT	Internal feedback added, glossary created, evidence-based impact added on 2021 Concertation and Concertation community section added
1.0	27/7/2021	Nicholas Ferguson, Trust-IT	

Executive Summary

Cyberwatching.eu has delivered four Annual Concertation Meetings in its 51 month lifetime. The meetings have been an essential part of the cyberwatching.eu project, bringing together mainly active projects in the area of cybersecurity and privacy and acting as the springboard for future project activities. Key topics in the project have featured in each of the Concertation meetings and have been essential for the completion of tasks in each WP.

Originally designed and for the first two editions delivered, as interactive one-day physical events, the arrival of the COVID-19 pandemic meant that the third and fourth Concertation Meetings were re-designed into online events and re-branded a series of topic-specific webinars. This meant we have been able to reach a broader and larger audience which has gone beyond the EC-funded project community. Inclusiveness though remains at the heart of the Concertation Meetings and with over 120 different projects attending the events.

In this deliverable we report on the final Concertation Meeting whcih was divided into three separate webinars in June and July 2021 (M50-51). The following key topics of the project were covered.

- R&I Landscape and the EU Project radar
- Clustering activities between projects supported by cyberwatching.eu
- Roadmapping activities
- Certification and standardization
- Privacy and emerging technologies
- Support for European SMEs

Table of Contents

Table of Figures

Table of Tables

Glossary

AI	Artificial Intelligence
CSIRT	Computer Security Incident Response Team
cPPP	Cybersecurity Public-Private Partnership
DEP	Digital Europe Programme
EC	European Commission
ECCG	European Cybersecurity Certification Group
ENISA	The European Union Agency for Cybersecurity
ECSO	European Cybersecurity Organisation
HE	Horizon Europe
JCU	Joint Cybersecurity Unit
NIS 2 Directive	Directive on Security of Network and Information Systems
SCCG	Stakeholder Cybersecurity Certification Group
SOC	Security Operating Centres

1 Introduction

Cyberwatching.eu has delivered four Annual Concertation Meetings in its 51 month lifetime. The events are essential for all cyberwatching.eu WPs and are designed to serve five key stakeholders:

European Commission: to gather together projects funded by Unit H1 and to provide status updates from projects. Concertation Meetings have also been the source of gathering recommendations or validation of the EC's own Work Programmes, in particular in the preparation of the Horizon Europe and Digital Europe programmes.

Other policy makers: ECSO and ENISA have been fixtures at the Concertation Meetings to both validate or disseminate results and also as a vehicle to communicate to non-ECSO members in the R&I landscape.

R&I projects: to provide a networking and dissemination opportunity. Concertation meetings have been highly inclusive with as many projects as possible included in the agenda or through data collected and used either for printed service offer catalogue or the EU project Hub. Break-out sessions and clustering have also been a key aspect of the events.

SMEs: For SMEs the benefit of Concertation meetings has been to understand what the key trends in CS&P innovation are and where the research community concentrates its effort. The events allow them to have a better forecast of what is going to trend in the market, what the gaps are and where to concentrate their own innovation potential. In addition, networking in the Concertation meetings with the project community, as well as valuable recommendations and presentations such as EC's overview of cybersecurity priorities in HE and DEP let them get familiarised with the projects ecosystem so they can try to join consortia themselves.

Cyberwatching.eu partners: The Concertation meetings are an essential part of project activities and, as explained in this document, the springboard for many other activities in terms of data gathering, clustering, validation of deliverables, and dissemination of project assets.

The Concertation Meetings were originally designed as highly interactive one-day physical events. Indeed, Concertation 2018 and 2019 were delivered in this format with break-out and World Café sessions. With the COVID-19 pandemic in 2020, this format was replaced by shorter webinars on specific topics and delivered over a series of weeks. This has meant we have been able to reach a broader and larger audience.

This document provides a full summary of the final Concertation Meeting which was held in several parts during June-July 2021 (M50-51) and culminated in a one-day event on 13th July which covered a number of key areas in the project. The report also provides brief summaries of Concertation 2018, 2019, 2020 with full reports included in other WP3 deliverables.

Finally, we provide a full overview of how each Concertation Meeting has contributed to each WP.

2 Concertation 2021

The Fourth Concertation series took place between June and July 2021. It was divided into three separate webinars covering the major pillars of the project

- **R&I Landscape and the EU Project radar**
- **Clustering activities between projects supported by cyberwatching.eu**
- **Roadmapping activities**
- **Certification and standardization**
- **Privacy and emerging technologies**
- **Support for European SMEs**

2.1 Shaping the future of cybersecurity - Priorities, challenges and funding opportunities for a more resilient Europe - 13 July 2021.

This was the main Concertation event of the three, lasting a full day. It had been previously planned for mid-June but was postponed, in accordance with the European Commission to coincide with the release of the new Horizon Europe Programme. Indeed, it was timed to act as a follow up to the cybersecurity Horizon Europe Information Day which took place 30th June. The meeting therefore focused upon the future priorities for Europe, providing details and discussion on the newly published calls.

Figure 1 Concertation 2021 final event banner

Figure 2 Selected speakers featured in live Tweet at the Concertation meeting

Key to the new calls is the **EU Cybersecurity Strategy**[1] which was highlighted and in particular its 3 pillars which cover how Europe can harness tools and resources to become technically sovereign:

1. **Resilience, technological sovereignty and leadership.** This includes the proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive). The Commission proposal expands the scope of the current NIS Directive by adding new sectors based on their criticality for the economy and society, and by introducing a clear size cap – meaning that all medium and large companies in selected sectors will be included in the scope. At the same time, it leaves some flexibility for Member States to identify smaller entities with a high security risk profile.
   The Commission also proposes to launch a network of Security Operations Centres across the EU, powered by artificial intelligence (AI), which will constitute a real 'cybersecurity shield' for the EU, able to detect signs of a cyberattack early enough and to enable proactive action, before damage occurs. This builds on top of the Computer Security Incident Response Teams (CSIRT) includes a reference to the Security Operating Centres (SOC).
2. **Operational capacity to prevent, deter and respond.** This covers the Joint Cybersecurity Unit (JCU) which will provide a virtual and physical platform for cooperation for the different cybersecurity communities in the EU. It will focus on operational and technical coordination against major cross-border cyber incidents and threats. An assessment of the JCU organisational aspects and an identification of EU operational capacities will be published by the end of 2021 while by June 2022 and incident and response plan will be published. This will be operational by the end of 2022 and expanded to industry by June 2023.
3. **Cooperation to advance a global and open cyberspace** – This element covers standards and international cooperation and establishing EU leadership on standards. The Cybersecurity Act is a key element here which came into force in 2019. The EC is currently working on a Union rolling work programme for European cybersecurity certification which will be published in late 2021.

[1] The EU Cybersecurity Strategy online at https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

The cybersecurity framework will feature one framework covering a broad scope which includes products, services and processes as well as an inclusive and transparent governance process which includes the ECCG (European Cybersecurity Certification Group) which is composed of representatives of national cybersecurity certification authorities or representatives of other relevant national authorities; and the SCCG (Stakeholder Cybersecurity Certification Group) which represents cybersecurity experts and advises the Commission and ENISA, the European Union Agency for Cybersecurity, on strategic issues regarding cybersecurity certification.

Priorities, trends and clustering in the R&I landscape

A key feature of the event was also to discuss new partnership opportunities between projects based on the Cyberwatching.eu **EU Project Radar.** Indeed, the Radar was used to demonstrate current funded activities in some of the topics covered in the calls, identifying for participants the projects working in technical areas or vertical sectors. The radar was also highlighted as a useful tool for the process of proposal writing in terms of quickly accessing reliable statistics on these topics such as funding levels and number of projects funded.

Main takeaways:

- Digital sovereignty and autonomy needs to be achieved in Europe. The landscape is very active in this respect with the launch of the Joint Cybersecurity Unit, the EU Competence Centre, and the Cybersecurity Act
- Similarly, these are key themes of the HE and DEP. Both build on past activities and it is imperative that proposals should look into results, reuse them and build upon them.
- Proposals should use the Live EU Project radar to see how they can maximise and build on results:
    - Funding on HE topics + related statistics
    - MTRL scores to understand the state of the art
    - Identify results and cite them

Project clustering

The role of the radar as an essential tool for the formation of six project clusters that cyberwatching.eu has supported. With over 20 projects involved, the projects have collaborated mainly in joint dissemination activities such as the creation of joint webpages[2], and joint webinars. Representatives from each cluster joined a lively panel where the recommendations gathered from each cluster were presented and discussion on the benefit of these types of joint activities were discussed.

Representatives from the following projects participated in the session: SDN-microSENSE, CUREX, InfraStress, SOTER and SAPPAN.

[2] https://www.cyberwatching.eu/cybersecurity-and-privacy-project-clusters

Figure 3 Cluster panellists featured in live Tweets during the event

Main takeaways:

- Clustering and joint dissemination activities, such as those carried out by cyberwatching.eu which supported over 20 projects, boost sharing of information, education and broader outreach for projects – Projects should use EC services such as Horizon Results Booster to continue support for this. For more details see D2.8 Recommendations report on R&I needs.
- To increase impact of clustering - concrete deliverables or real tasks to generate real outputs are key so all members feel that have a hand in their production
- Exploration of dynamic clustering, pilot synergies including testing and trials, data set sharing, and sharing of threat intelligence

Future priorities and EU Cybersecurity Roadmaps

The workshop also saw cyberwatching.eu's continued support to the Competence Centre Pilot projects collaborate with a panel session focusing on the roadmapping, which is helping shape cybersecurity policy in Europe.

Figure 4 Roadmap panellists featured in live Tweets during the event

Main takeaways:

- The competence centre pilot projects have adopted an aligned approach for a common set of research priorities leading to a certain level of common approach toward a roadmap – Technologies, capacity building for a cyber skills framework, building networks
- Continuous public-private dialogue is key for future activities (the Cybersecurity Public-Private Partnership (cPPP) is an example of this)
- Besides the four Competence Centre Pilot Projects, cybersecurity cPPP (ECSO), there are also multiple communities and initiatives all running in parallel – the Blueprint initiative for sectoral cooperation on cybersecurity skills (REWIRE) is just one of them, there is a need to ensure that these efforts are coordinated, complementary and productive (a central 'authority' like the EU Competence Centre should provide coordination among different initiatives)
- Cyber competence network should foster projects and SMEs for a cybersecurity services marketplace (this is actually being accomplished via the efforts of cyberwatching.eu's "handover" of the marketplace to ECSO via a memorandum of understanding – providing proof of cyberwatching.eu's positive impact well beyond the life of the project)

Standards and certification

With the EU Cybersecurity Act coming into force less than a year ago to provide an EU-wide harmonised framework to certify ICT products and services, cybersecurity certification can be a market differentiator for businesses. Certifications can help companies act with confidence and assure their customers and partners of their ability to defend themselves from cyberattacks and data breaches. However, for an SME, micro-enterprise or start-up, taking the first steps to certification can be both complex and daunting. They are essential for the market in terms of enabling consistency among developers and serve as a reliable metric for purchasing security products or systems and creating trust in them. The Concertation Meeting importantly saw the launch of the Cybersecurity Label for SMEs which targets SMEs, especially start-ups and micro-SMEs that are approaching the IT security assurance landscape for the very first time. Presentations also came from Roberto Cascella, ECSO WG1 Standardisation, certification and supply chain management; George Sharkov, European DIGITAL SME Alliance and SBS (also a member of the SCCG); and Chatzopoulou Argyro, TÜV TRUST IT GmbH

Main takeaways:

- International standards should be (re-)used as much as possible for cybersecurity certification: EU intervention here is key.
- Mapping of standards (and de-facto standards) by ECSO and Concordia are important. However, the standards are in specific areas and don't cover the complex landscape. New standards and systematic effort are needed as well as a common taxonomy for SMEs
- Standards experts should use EC services and resources such as StandICT.eu[3] and SBS to contribute to standardization processes and to contribute to the EC's Open Consultation on Cybersecurity standards.
- New solutions and new funding through HE to further address emerging technologies and CS and privacy challenges - Security and privacy by design are essential concepts
- Clear guidelines or practical tools on data protection and cybersecurity by design, especially for emerging technologies like blockchain, are required. Cooperation and a coordinated approach are needed so that appropriate methodologies for privacy by design would be implemented.

Support to European SMEs

Companies are nowadays experiencing cyber-attacks on a daily basis. A cyber-attack can cost them on average €25,000 or more. Smaller businesses are often targetted and are harder hit, suffering repeat attacks, which can lead to damaged reputations and potential bankruptcy and/or closure. Despite this, cybersecurity is still often an after-thought for many small businesses, with only half of European SMEs (Small and Medium Enterprise) investing adequately to address the issue. The EC's Cybersecurity strategy is a commitment to bolstering Europe's collective resilience against cyber threats and to help to ensure that all businesses and citizens can fully benefit from trustworthy and reliable services and digital tools.
The workshop focused on the importance of SMEs to the cybersecurity ecosystem and that greater awareness and eventual uptake of certification and standardization by them being vital for building trust in the digital economy.

Figure 5 Panellists in data protection session featured in live tweet

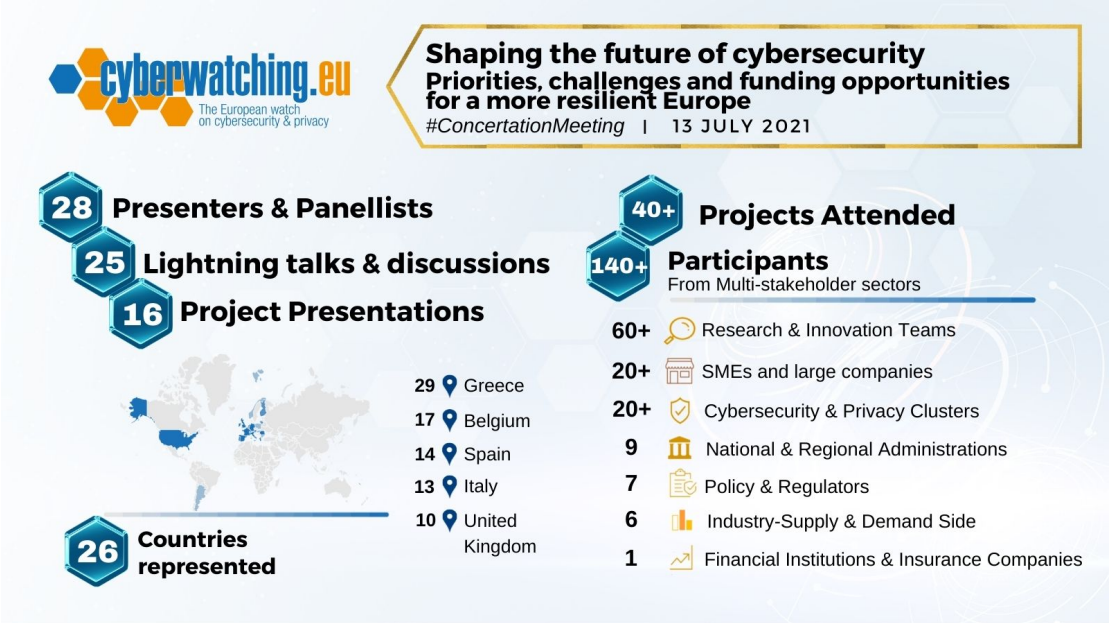
[3] https://www.standict.eu/

Main takeaways:

- European SMEs can be the back bone of EU's digital sovereignty and autonomy.
- SMEs have high exposure to threats and are often not equipped with the right technical and organisational security to meet the challenges.
- SMEs shouldn't be discouraged by the massive and complex amounts of information and procedures.
- Lightweight self-assessment such as Cybersecurity Label[4] should whet the appetite for SMEs advance to certification – SMEs need to aim high! Again, this is an excellent example where cyberwatching.eu is creating a useful tool that will have significant positive impact well beyond the life of the project.
- Certification should drive the growth of the market for SMEs and start-ups, it is is a market differentiator for SMEs:
  - Trusted, reliable & cost-effective.
  - Affordable (accessible), adapted, aware (adopted) to SMEs.
- Standards should be compatible with SME needs and pass the SME-compatibility test.
- The EU shall establish trust through standardisation and certification and provide guidance to SMEs, raise awareness of different assurance levels.
- Tools and solutions need to evolve with the landscape and cannot stay static. They must evolve with the threat landscape.

Event page, presentations and recording available here.

2.1.1 Event participation



2.1.2 Evidence based impact of Concertation 2021

- The presence of the EC, ENISA and ECSO was important for increasing the increasing the impact of the launch of the Cybersecurity Label.
- Similarly, demonstrating how the Radar can be used as a practical tool for participants writing of future proposals for the HE calls was an important. We demonstrated how the radar can be used to find evidence-based statistics, information on state-of-the-art results and finding partners etc. The EC speaker

[4] http://gtt.cyberwatching.eu/Pages/Home.aspx

commended cyberwatching.eu on the radar recommending its use for this purpose and as a way to maximise and build on past results.

- If we compare the usage of the Radar in the period of the event (12-15.07) with the previous period, the Radar has registered an increase of 175% in terms of unique visits with an average time on page of 02:50 minutes against the 00:50 seconds of the previous period, meaning that users not only visited the Radar but have also used it.
- 73% participation rate (105 participants from 144 registrants) for the workshop demonstrates the interest in the topics of the webinar. Questions from audience were also fielded by panellists and speakers demonstrating active participation of the audience.
- The event webpage is one of the 10 most visited pages in 2021.
- Social media engagement: 35 live tweets done, 23.8K organic impressions, 82.3% engagement rate, 125 retweets and 227 likes during the workshop.
- With this event we also gained 25 new Twitter followers and 21 new LinkedIn connections/followers.

2.2 Cybersecurity for Critical Infrastructures – Resilience and trust in the health and energy sectors. – 24 June 2021

The expansion of the threat surface due to global connectivity and the rise of emerging technologies such as IoT and AI is having a significant impact on critical infrastructures and services. Disruption of these ICT capabilities may have disastrous consequences both at national and international level.

The second Concertation workshop focussed on how Europe is addressing the need to effectively protect the Energy and Healthcare infrastructures. Two of the cyberwatching.eu project clusters provided and update of activities in this area and provided recommendations.

Figure 6 Concertation 2021 second event banner

Energy sector and look at how, in addition to the typical threats that plague other industries, it presents certain particularities that require particular attention. Both geographic distance and organizational complexity make the industry vulnerable to cyberattacks, coupling with unique interdependencies between virtual systems and physical infrastructure.
5 EC funded projects presented useful insights and tangible solutions in protecting the electrical power, energy systems and smart grids against cyber-attacks and how to preserve the privacy of the data.

Main takeaways

- A holistic Risk Management Assessment, including the whole supply/value chain and identification of cross-border and cross-organizations risks, is crucial to identify the weaknesses that can drive us to cascading effects, and this will allow us to improve the cybersecurity architecture taking into account both cyber and physical threats. The cyberwatching.eu Risk Assessment Tool addresses this, as an excellent first step, which will have a significant positive impact beyond the life of the project.
- There is also a need for close collaboration between operators for Critical Information Sharing regarding cyber threats from different domains in different countries, including the availability of interoperable platforms, and therefore allowing the design of models for potential cascading effects. This collaboration environment should be reinforced with political willingness from all MS, coordinated by the EC.
- To solve the security problems of combining legacy systems with new IoT devices, first step is the identification of the devices (including encryption and authentication), followed by the certification of systems and devices to assure that comply with a minimum set of security requirements. This also involves the implementation of new devices based on security and privacy by-design and by-default.
- Certification processes are also important when tackling real-time requirements of energy infrastructures. Latency makes impossible to have real-time data collection, so it is necessary to define what “real-time” means, stablishing, through certification processes, the minimum time for reacting to cyber threats or to informing of them. This has to be combined with lightweight threat detection solutions that reduce time consumption and the protection of the data from their origin (through authentication/encryption) through their entire lifecycle.

Healthcare.
Hospitals, Medical Device manufacturers, ICT systems providers and Digital service providers need to act now to demonstrate their products and service's cyber resilience and privacy capabilities, not simply to address the EU regulatory measures (GDPR, MDR, EU Directive 2016/1148) but also to establish patients and medical staff's trust and confidence.
5 EC funded project will present the main challenges facing the medical sector in ensuring secure integration of services that comply to EU regulations.

Main takeaways

- Security governance (roles, policies, procedures, processes…) is of high importance to ensure the adoption of “security and privacy-by-design” approach, so the main healthcare actors have to stablish the right context in

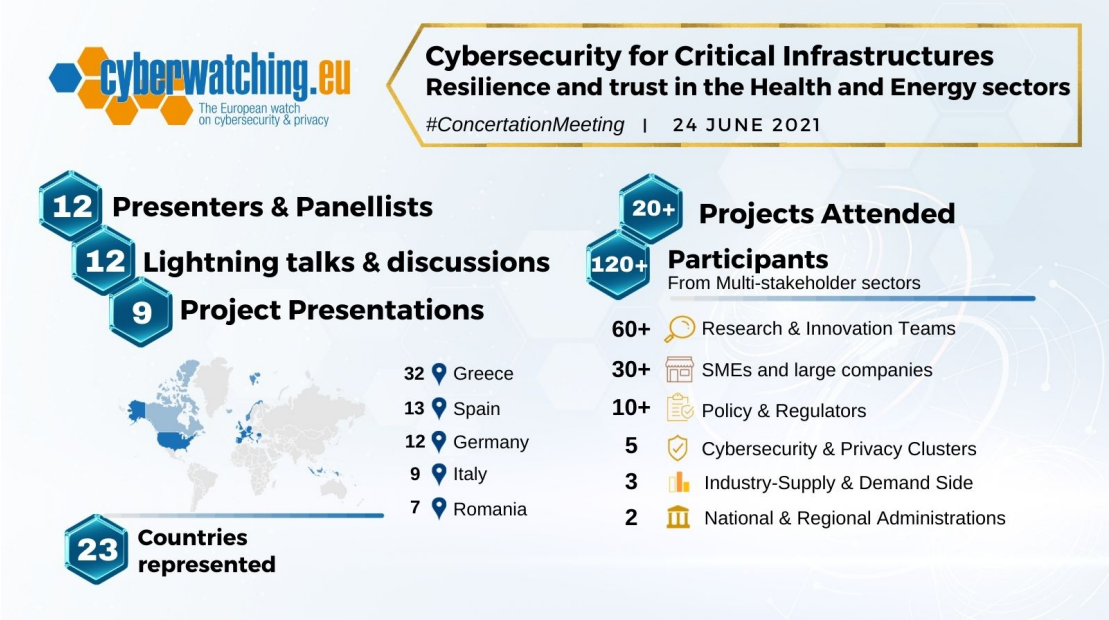
their organization and ensure a proper communication. This has to go hand in hand with security certification, compliance, assessment and auditing, internal and in relation with external providers. Also, hospitals having teams specialized in cybersecurity among their staff would be very valuable, that are able to follow ENISA's guidelines for procurement process (that in future versions could include specific references to security by-design tools).

- Medical devices manufacturers have to implement security and privacy by-design, taking safety also into account and considering the whole lifecycle of the devices (developing, deploying, using and disposing). Equipping medical devices with up-to-date cryptographic techniques is another important aspect. Another important factor is cybersecurity culture, within manufacturers and users of medical devices. Policy-making acting on certification schemes is another key point (not only for final requirements of a product, but also for the engineering process).
- Before deploying and integrating a new medical device into a hospital context, it is necessary a preliminary evaluation and a final decision on the proposed device to ensure that is robust, from the security point of view. From the technical point of view, segmentation of networks is a good practice when introducing a new medical device. There are also tools and methods from the scientific point of view that can analyse if a device has its security compromised, and risk management systems with continuous device monitoring are valuable assets.
- A pandemic situation, like COVID-19, expands the need of telemedicine, and cybersecurity has to be seen as an enabler for ensuring the resilience and prompt availability of key healthcare services, not only from the technical point of view, but also from an educational focus, preventing unsecure behaviours, especially when we are allowing staff working from their houses or managing medical equipment at patients' homes. A recommendation for EC would be to strengthen channels for the promotions to end users of the solutions developed under funded projects. Projects should use EC services such as the Horizon Results Booster [5]. Already cybersecurity projects such as CUREX and PANACEA in the health cluster are doing this.

Event page and presentations available here.

[5] https://www.horizonresultsbooster.eu/

2.2.1 Event participation



2.2.2 Evidence based impact of Concertation 2021

- Following the workshop projects from the Health and Energy clusters applied for the HRB joint dissemination service.
- 75% participation rate (91 participants from 121 registrants) for the workshop demonstrates the interest in the topics of the webinar. Questions from audience were also fielded by panellists and speakers demonstrating active participation of the audience.
- 5 projects updated their information on the Radar as a result of the event.
- The Project Clusters pages in June 2021 registered a 10% increase with respect to the previous month.
- Social media engagement: 11 live tweets done, 8.7K organic impressions, 31.04% engagement rate, 42 retweets and 108 likes during the workshop.
- Through this event we also gained 29 new Twitter followers and 14 new LinkedIn connections/followers.

2.3 Financial Sector Cybersecurity Collaboration and Engagement of Stakeholders – 21 May 2021

The first Concertation workshop focused on cybersecurity in the financial sector, zooming in on the work and recommendations from the 5 projects contributing to the cyberwatching.eu cluster on finance.

Financial Institutions have always been one of the most attractive targets for cyberattacks due to their economical appeal. Nowadays, due to their owned high volume of personal data, more malicious actors are targeting them with innovative and unknown attacks. Due to all these factors, although new technologies and digitalization bring so many benefits to this sector, it also has increased exponentially the attack surface.

Figure 7 Concertation 2021 first event banner

Additionally, another critical issue for the financial sector is the growing attention from European legislators, regulators and standard bodies on cybersecurity issues related to the financial sector. The high volume and complexity of regulations, together with the fragmentation arising from different EU laws across national EU Jurisdictions causes inefficiency and loss of profitability. Cooperation and cyberthreat intelligence sharing are nowadays also a critical necessity in this sector.

The workshop focussed on best practices, motivational factors, and incentives related to collaboration of financial sector cybersecurity stakeholders, such as efforts to share threat intelligence, design common incident reporting workflows, joint risk assessments and others. A panel discussion identified appropriate financial sector specificities, recommendations on engaging the right internal and external parties, and setting clear processes within the community, as well as a process to collaborate with actors outside of the financial sector community.

The workshop also discussed topics of relevance for Digital Operational Resilience Act (DORA) practical implications, such as harmonisation of risk management rules across financial services sectors, incident classification and reporting, or information sharing arrangements and notification of competent authority if they take part in such arrangements.

Main takeaways

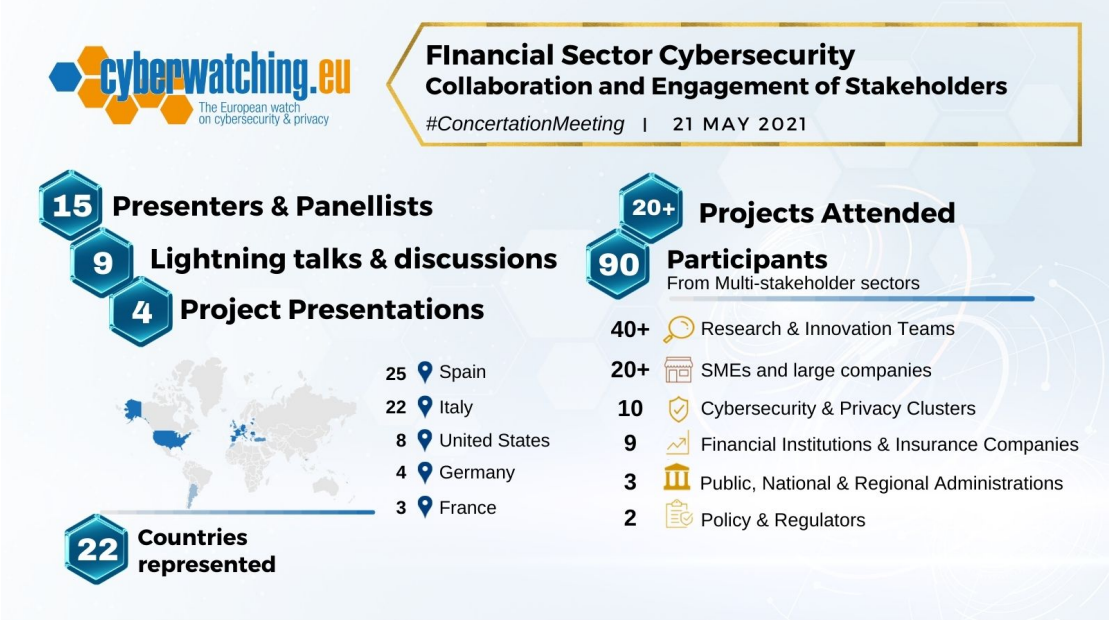
- Banks are traditionally very closed entities. Sharing information is never the focus of financial services providers since it implies to share information about customers (as an exception included in GDPR). Fintech companies are an exception, as they offer digital-based services and, consequently, are less reluctant to the digitise approach of dealing with banking transactions.
- Sharing information and experiences can benefit them, and the supervision from the national financial regulators of the information sharing networks, can generate confidence and therefore help in attracting financial services providers to participate in those collaboration networks. These networks have to build the rules and the framework for sharing information to prevent fraud.
- Pseudo-anonymization processes that protect banks reputation, together with trust in sharing information tools, are other important keys for collaboration.

There is also a need for tools to automate the process of using the information collected from banks and reacting in consequence.

- From the policy point of view, there is also a need for an European consensus on how to manage the exception on GDPR for sharing information in the financial sector, and after the consensus, stablish a set of common rules (notice that PSD2 is a directive, not a regulation, and it has different interpretation).

Event page, presentations and recording available here.

2.3.1 Event participation



2.3.2 Evidence based impact of Concertation 2021

- The webinar gave an opportunity to onboard key players in the financial sector such as CERTFin, Caixabank, Informatique Banque Populaire and the European Finance Forum as a new member of the Cyberwatching.eu expert lists, who provided insightful contents on challenges and opportunities for cybersecurity and privacy, essential to efficiently collaborate and engage with the respective stakeholders.
- 73% participation rate (90 participants from 126 registrants) for the workshop demonstrates the interest in the topics of the webinar. Questions from audience were also fielded by panellists and speakers demonstrating active participation of the audience.
- 3 projects updated their information on the Radar as a direct result of the webinar.
- In terms of social media engagement, a peak of 8.1K total impressions, 19.57% engagement rate with 32 retweets, 46 likes out of 10 live tweets during the event.
- Through this event we also gained 24 new Twitter followers and 30 new LinkedIn connections/followers.

3 Concertation 2020

The Covid-19 pandemic led to many disruptions in 2020, which continue in 2021. The third Concertation Event was originally foreseen in the second quarter of 2020. However, due to the pandemic and country-specific application of regulations, quarantine requirements and confinements, the Event was initially postponed until mid-Autumn 2020 with the hope that travel would resume normally in Autumn 2020. With the continued pandemic restrictions, and after several discussions within the Consortium on how best to resolve this situation, it was decided that the format of the Third Concertation Event would need to be virtual. Instead of holding a single virtual event, it was decided that a series of Webinars would be better suited and different topics could be addressed at intervals, thus avoiding the fatigue of continuous online concentration which has consumed the general method of work today. The following Webinars were, thus, organized:

- Effective Protection of Critical Infrastructures against Cyber Threats (29 October 2020)
- EPES and Smart GRIDS: practical tools and methods to fight against cyber and privacy attacks (12 November 2020)
- Cybersecurity risk management: How to strengthen resilience and adapt in 2021 (23 November 2020)
- Security and Privacy by Design for Healthcare (10 December 2020)

Full details and outputs of the event are available in section 6 of D3.5 Risk and Recommendations on Cybersecurity Services[6].

4 Concertation 2019

The 2nd Cyber Concertation meeting of H2020 projects from unit H1 "Cybersecurity & Privacy"[7] saw over 60 representatives from all projects in the unit[8] in order to discuss a series of topics, including focus on the key topics and collaboration between the newly funded competence centre pilot projects and discussion on future directions for the Horizon Europe and Digital Europe Programmes.

With a series of plenary and break-out sessions, the event also saw collaboration with ECSO secretariat and ECSO WG chairs who led discussion in a number of these sessions.

Two main results emerged from the event:

1. First engagement between competence centre pilot projects and other projects in the unit. The agenda was designed to include sessions to discuss key topics related to projects such as capacity building and cyber-ranges.
2. Collection and report to EC on short, medium and long-term recommendations for the Horizon Europe and Digital Europe programmes. Through break-out sessions, a clear set of recommendations on the following topics were provided.
    a. Cybersecurity skills and training for SMEs
    b. New challenges form emerging technologies including the impact of GDPR
    c. Standards and certification for cybersecurity
    d. Risk management and threat intelligence for SMEs and Public Administrations

[6] https://www.cyberwatching.eu/d35-risk-and-recommendations-cybersecurity-services
[7] https://www.cyberwatching.eu/news-events/events/brussels-second-cw-concertation-meeting-04062019-0
[8] https://www.cyberwatching.eu/brussels-second-cw-concertation-meeting-participants-list

e. International cooperation priorities
f. Cybersecurity priorities for vertical sectors

Full details and outputs of the event are available in section 6 of D3.4 Cybersecurity legal and policy aspects preliminary recommendations and road ahead[9].

5 Concertation 2018

The main focus of the first Concertation Meeting was to bring together EC-funded projects that had been targeted in the first round of radar mapping based on level 1 of the cyberwatching.eu cybersecurity R&I taxonomy. A total of 74 registered participants included:

The first Concertation meeting provided opportunities for visibility for all participating projects through break-out sessions based on the level 1 clustering, panel sessions and the publication of the service offer catalogue. For the EC project officers it was an opportunity to meet numerous projects at the same event and get an update on progress. For projects there was the chance to network based clustering and to already identify new opportunities for collaboration and funding.

In addition, for this first event, a hard copy of the **R&I Catalogue of Services** of projects was compiled and distributed to each participant. Each project provided a service offer with short and attractive texts covering what user needs the project services could solve or how it would improve or is improving the lives of end-users.

Full details and outputs of the event are available in section 6 of D3.2 EU Cybersecurity and Privacy R&I Ecosystem[10].

[9] https://www.cyberwatching.eu/d34-eu-cybersecurity-legal-and-policy-aspects-preliminary-recommendations-and-road-ahead

[10] https://www.cyberwatching.eu/d32-european-cybersecurity-and-privacy-research-innovation-ecosystem

6 The Concertation community

The Concertation meetings is one of the key elements in the community building activities carried out in WP4. They have been essential for collecting data and engagement in particular with the members of EC-funded projects. Concertation 2018 and 2019 were delivered as physical events with project coordinators or partners mainly attending. However, the COVID-19 pandemic meant that the Concertation meetings moved online. This gave us much more flexibility as we moved to shorter session type webinars rather than day-long events. We were also not restricted by capacity or venue-related issues. It also meant that we were able to open up the events to a broader community and beyond the original target community of projects. Travel budget was also saved because of this not only for our project but also our participants'. Cyberwatching.eu's Concertation community is therefore broad and large consisting of cybersecurity and privacy researchers, experts, policy and regulators, and organisations across the globe.

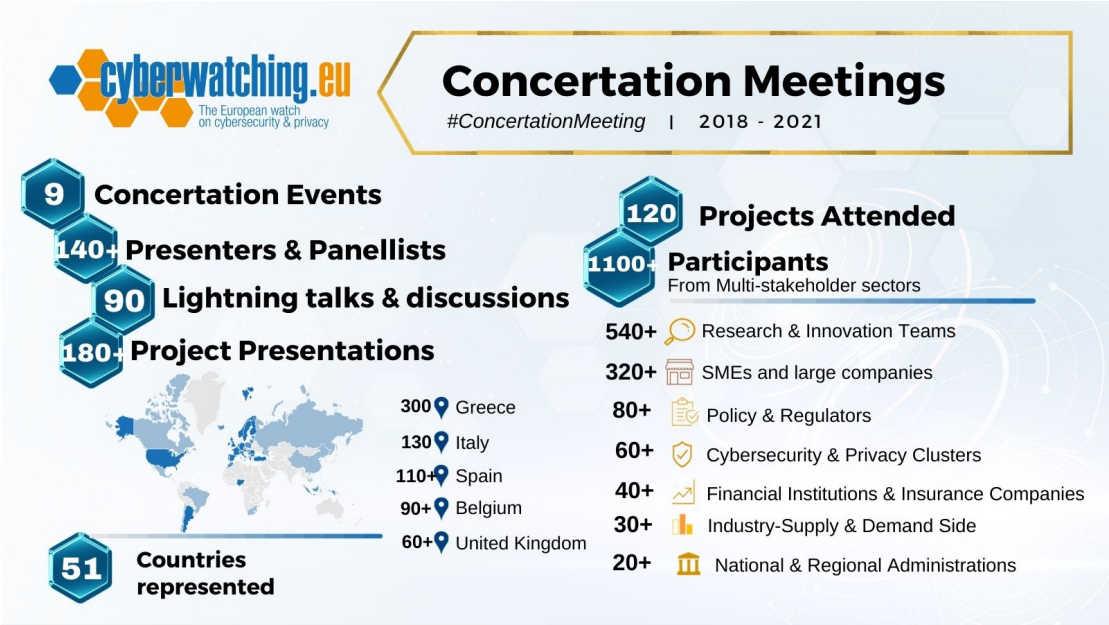


Figure 8 Cyberwatching.eu Concertation Community (2018-2021)

The majority of the concertation community come from European countries (31), besides there are some participants have come from non-European countries, Asia (10), America (8), and Africa (2).

The events have been a vital engagement hook. Over 120 H2020 projects have been included in the agendas as panelists, speakers or chairs. A total of 140 presenters and panellists have also featured in the agendas including the European Commission, ECSO, ENISA and SME clusters.

The multi-stakholder participation at the event highlights the evolution of the Concertation one-day physical events to Concertation Series which feature shorter webinars covering different topics. As stated at the start of this document, with over 320 SMEs and large companies participating at the event, this shows the interest there is from this community in the priorities of the European R&I landscape and the work being done to improve cybersecurity and privacy for this community.

7 Conclusions

The Concertation meetings have been an essential part of the cyberwatching.eu project, bringing together mainly active projects in the area of cybersecurity and privacy and acting as the springboard for future project activities.

Key topics in the project have featured in each of the Concertation meetings and have been essential for the completion of tasks in each WP.

Concertation	2018	2019	2020	2021
EU Project Radar	✓	✓	✓	✓
Project clustering & MTRL		✓	✓	✓
Privacy and emerging technologies		✓		✓
Standards & certification		✓	✓	✓
Recommendations for EC calls		✓		✓
Competence Centre projects		✓		✓
ECSO & ENISA participation	✓	✓	✓	✓
Resources for SMEs	✓	✓	✓	✓

Table 1 Key cyberwatching.eu topics at Concertation Meetings

WP2: EU Project Radar & MTRL clustering

Concertation 2018 saw the publication (and printing) of service offers from 48 different projects. This formed the basis of the eventual online Project Hub and was the first port of call for data collection and direct engagement with the projects in the unit. The first event also saw the first clustering of projects based on taxonomy level one with dedicated break-outs on these topics. The cyberwatching.eu R&I taxonomy was presented at the event (D2.2) and the first round of mapping projects to this was validated. Results from the event fed into the 2018 version of the radar[11] (D2.2).

Concertation 2019 saw the presentation of investment made by the EC in the taxonomy Level 2 categories which was the precursor for the automated statistics on funding levels and project duration based on CS&P topics. The data presented was included in the EC publication “Building strong cybersecurity in the EU” that cyberwatching.eu co-authored with the EC. The event also saw a requirements gathering exercise on support to projects regarding how projects can improve their market readiness levels. This fed directly into the design of the MTRL methodology (D2.3) the MTRL scores collected and which are now part of the radar and the eventual project clusters created in and supported in WP2 (D2.8).

[11] https://radar.cyberwatching.eu/radar/autumn-2018

With the distributed nature of Concertation 2020 due to the COVID-19 pandemic and delayed delivery (The meeting took place in October-November 2020 as reported in full in D3.5) the radar was not the focus of the 2020 Concertation. However, a dedicated series of workshops took place in July 2020 which saw the establishment of the project clusters and the identification of joint priorities and objectives. The Concertation meeting was therefore dedicated to the first public workshops for the clusters with interventions from 16 projects.

Finally, Concertation 2021, saw the evolution of the R&I landscape presented (Radar versions 2018-Live) and the demonstration of how the radar can be a useful resource for information, statistics and partners for proposals for the new Horizon Europe Work Programme. The importance of the radar as a tool for understanding the state of the art and identifying results which could be re-used was highlighted by the EC. The Concertation also saw recommendations from each of the project clusters and specific workshops on the clusters covering finance, health and energy.

WP3 Policy recommendations, Standards, Certification & Privacy

Concertation 2019 was focused on supporting the EC to gather recommendations and priorities for the Horizon Europe and Digital Europe Programmes. These were presented at the event and formed the basis of break-out sessions featuring the project representatives that attended. Recommendations were presented in D3.5 and delivered to the EC. Topics included emerging cybersecurity challenges from emerging technologies and standards and certification for cyber security. The event was also essential for validating content of D3.4 which focused on the impact of GDPR on emerging technologies which has been a continuous topic addressed as part of T3.4. In addition, the recommendations included in the eventual GDPR Temperature Tool were validated. Risk management was also a break-out session topic providing input on this topic for D3.4 and input into the Risk Management tool.

Concertation 2020 included a webinar which addressed the topic of risk management. Here the Risk Management Tool which had been recently launched was presented. The initial concept of the Cybersecurity Label was presented and validated prior to implementation. The session also saw input from 6 projects working in the risk management theme based on the analysis of the Radar.

Finally, Concertation 2021 saw the launch of the Cybersecurity Label. This was a key event for the dissemination of the label towards policy makers with the EC, ECSO and ENISA participating. The label was presented within the framework of the work being carried out on certification as part of the EU Cybersecurity Act other certification-related activities. Standards and certification and privacy challenges and emerging technologies were also key elements in the agenda with priorities and challenges and recommendations from key stakeholders including projects discussed (Output is included in D3.7 and D3.8). There was particular reference to the new HE Work Programme in these sessions. Indeed, the content of the new WP was presented with details of the upcoming calls and topics. Recommendations and regarding the definition of these came in Concertation 2019.

WP4 Engagement and dissemination

The Concertation meeting events have been key for engagement activities and dissemination of cyberwatching.eu results.

ECSO and ENISA have both participated at Concertation Meetings. ECSO in particular have participated in all Concertation meetings using it as an important vehicle to contribute to dialogue and to communicate activities mainly in WG1 Standardisaton,

certification and supply chain management; and WG 6 SRIA and cybersecurity technologies to project community.

The Concertation meetings have also been important for establishing and forging relationships with SME Clusters. The participation of GAIA and ClujIT in Concertation 2018 led to further collaboration with them including promotion of SME-facing outputs such as the GDPR Temperature tool, and the joint webinar on teleworking during COVID-19. This was held with other clusters such as CyberWales and The Hague Security Delta (see D4.5, 4.6 and 4.8).

With the launch of the Competence Centre Pilot projects, Concertation 2019 saw the first joint presentation of all projects in the same panel session. The session was an important vehicle for the EC in terms of encouraging collaboration between the four projects. Since that event, cyberwatching.eu has continued to support this collaboration and has organized other such roundtables with the projects including in Concertation 2021 where the various roadmapping activities were presented and as reported in detail in D4.7. As a result, cyberwatcing.eu has also been invited and presented at a number of events organized by the Competence Centre pilot projects.

WP5 Support to SMEs

With the participation of SME Clusters at Conceration 2018, cyberwatching.eu has tried to include SMEs in what is an EU-Project facing event. The importance of Market readiness of results and the understanding the needs of SMEs, which is often a topic for EC cybersecurity calls, has been a continuous theme at these events. The transformation of the Concertation meetings to online events which have been distributed across different days has also meant that we have been able to reach a broader audience and indeed, SME participation at Concertation 2020 and 2021 was higher. This is also due to the focus on vertical sectors and the promotion of these events to the “cyberwatching.eu webinar” community.

Recommendations from Concertation 2019 regarding SME cybersecurity needs revealed the need for SMEs to have trusted, easily accessible and online resources to raise awareness of cybersecurity and privacy issues and to diffuse best practices. Based on this, partners agreed to convert what would otherwise have stayed as recommendations in deliverables into practical, online resources for SMEs which will be sustained beyond the project lifetime through CyberDIH. This includes the Cybersecurity Label, the GDPR Temperature Tool, the Information Notices Tool and the Risk Management Tool.

For the Concertation 2021, a number of sessions focussed on SME needs in particular regarding standardisation and certification. This was a key given the policy developments already discussed above (e.g. Cybersecurity Act and others). What emerged from the different discussions is that on one hand, SMEs are the most vulnerable part of digital value chains, and they need guidance and access to light-weight certification (such as Label offered by cyberwatching.eu), on the other hand, the front-runner SMEs whose solutions contribute to the European cybersecurity sovereignty also learned how they can: be involved in strengthening European cybersecurity R&D, participate in standardisation, and promote their solutions towards interested SMEs (through marketplace).

Finally, the Concertation meetings raise awareness of the cyberwatching.eu marketplace which hosts just under 100 project results. This will now be sustained by ECSO beyond the project lifetime and the flow of project results into the platform will continue.