Horizon 2020 Program (2014-2020)

Cybersecurity, Trustworthy ICT Research & Innovation Actions
Security-by-design for end-to-end security
H2020-SU-ICT-03-2018


Cyber security cOmpeteNCe fOr Research anD InnovAtion[†]

# Work package 5: *Exploitation, dissemination, certification and standardization*
# Deliverable D5.4: *3rd year report on exploitation, dissemination, certification and standardization*

**Abstract:** This document represents the 3rd year report on activities performed by the CONCORDIA project on exploitation, dissemination, communication, certification and standardization, within the Work Package 5. The effort is reported in three main sections, one for each of the main tasks of this Work Package and builds on the information and activities already described in the reports of the previous years. This deliverable does not reiterate all the information of the previous reports, but only information that is needed to better describe the 3rd year developments. Several key achievements of the consortium within the third year of the project are presented in this document, ranging from the efforts to collect available and reachable incubators and accelerators, the communication activities of the consortium, to the efforts related to the standardization certification.

| | |
|---|---|
| Contractual date of delivery | *M36* |
| Actual date of delivery | *22.12.2021* |
| Deliverable dissemination level | *Public* |
| Editors | *Chatzopoulou Argyro* |
| Contributors | *TUVA, TID, MUNI, ATOS, FORTH* |
| Quality assurance | *Flowmon Networks*<br>*Arthur's Legal*<br>*FORTH*<br>*University of Maribor* |

[†] This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830927.

# The CONCORDIA Consortium

| | | |
|---|---|---|
| UniBW/CODE | University Bundeswehr Munich / Research Institute CODE (Coordinator) | Germany |
| FORTH | Foundation for Research and Technology - Hellas | Greece |
| UT | University of Twente | Netherlands |
| SnT | University of Luxembourg | Luxembourg |
| UL | University of Lorraine | France |
| UM | University of Maribor | Slovenia |
| UZH | University of Zurich | Switzerland |
| JACOBSUNI | Jacobs University Bremen | Germany |
| UI | University of Insubria | Italy |
| CUT | Cyprus University of Technology | Cyprus |
| UP | University of Patras | Greece |
| TUBS | Technical University of Braunschweig | Germany |
| ~~TUDA~~ | ~~Technical University of Darmstadt~~ | ~~Germany~~ |
| MU | Masaryk University | Czech Republic |
| BGU | Ben-Gurion University | Israel |
| OsloMET | Oslo Metropolitan University | Norway |
| Imperial | Imperial College London | UK |
| UMIL | University of Milan | Italy |
| BADW-LRZ | Leibniz Supercomputing Centre | Germany |
| EIT DIGITAL | EIT DIGITAL | Belgium |
| TELENOR ASA | Telenor ASA | Norway |
| AirbusCS-GE | Airbus Cybersecurity GmbH | Germany |
| SECUNET | secunet Security Networks AG | Germany |
| IFAG | Infineon Technologies AG | Germany |
| SIDN | Stichting Internet Domeinregistratie Nederland | Netherlands |
| SURF | SURF BV | Netherlands |
| CYBER-DETECT | Cyber-Detect | France |
| TID | Telefonica I+D SA | Spain |
| RUAG | RUAG AG (as a replacement for RUAG Schweiz AG) | Switzerland |
| BITDEFENDER | Bitdefender SRL | Romania |
| ATOS | Atos Spain S.A. | Spain |
| SAG | Siemens AG | Germany |
| Flowmon | Flowmon Networks AS | Czech Republic |
| TÜV TRUST IT | TUV TRUST IT GmbH | Germany |
| TI | Telecom Italia SPA | Italy |
| Efacec | EFACEC Electric Mobility SA (as a replacement for EFACEC Energia) | Portugal |
| ARTHUR'S LEGAL | Arthur's Legal B.V. | Netherlands |
| eesy-inno | eesy-innovation GmbH | Germany |
| DFN-CERT | DFN-CERT Services GmbH | Germany |
| CAIXABANK SA | CaixaBank SA | Spain |
| ~~BMW Group~~ | ~~Bayerische Motoren Werke AG~~ | ~~Germany~~ |
| NCSA | Ministry of Digital Governance - National Cyber Security Authority | Greece |

| | | |
|---|---|---|
| RISE | RISE Research Institutes of Sweden AB | Sweden |
| Ericsson | Ericsson AB | Sweden |
| SBA | SBA Research gemeinnutzige GmbH | Austria |
| IJS | Institut Jozef Stefan | Slovenia |
| UiO | University of Oslo | Norway |
| ULANC | University of Lancaster | UK |
| ISI | ATHINA-ISI | Greece |
| UNI PASSAU | University of Passau | Germany |
| RUB | Ruhr University Bochum | Germany |
| CRF | Centro Ricerche Fiat | Italy |
| ELTE | EOTVOS LORAND TUDOMANYEGYETEM | Hungary |
| Utimaco | Utimaco Management GmbH | Germany |
| FER | University of Zagreb, Faculty of Electrical Engineering and Computing | Croatia |

# Document Revisions & Quality Assurance

**Internal Reviewers**

1. FORTH (review lead)
2. Flowmon Networks
3. Arthur's Legal
4. University of Maribor

**Revisions**

| Ver. | Date | By | Overview |
|---|---|---|---|
| *0.01* | *25/10/2021* | *Chatzopoulou Argyro* | *Table of Contents* |
| *0.02* | *10/11/2021* | *Nicolas Kourtellis and Aljosa Pasic* | *Material for T5.1* |
| *0.03* | *11/11/2021* | *Martin Horák, Christos Papachristos and Maria Mastoraki* | *Material for T5.2* |
| *0.04* | *11/11/2021* | *Chatzopoulou Argyro* | *Material for T5.3* |
| *0.05* | *03/12/2021* | *Chatzopoulou Argyro, Martin Horák, Nicolas Kourtellis and Aljosa Pasic* | *Changes performed following the internal review* |
| *0.06* | *20/12/2021* | *Chatzopoulou Argyro, Martin Horák, Nicolas Kourtellis and Aljosa Pasic* | *Changes performed following the internal review round 2* |
| *0.07* | *21/12/2021* | *Chatzopoulou Argyro, Martin Horák, Nicolas Kourtellis and Aljosa Pasic* | *Final Changes before release* |
| *1.00* | *06/05/2022* | *Chatzopoulou Argyro* | *Changes after external review Reay for publication* |

# Executive summary

The present document is the third deliverable of Work Package 5 (WP5), and represents the 3rd year report on exploitation, dissemination, communication, certification and standardization. The work package's objective is to enhance the impact of CONCORDIA's outcomes through strategic exploitation, dissemination, and standardization.

WP5 is organized into three main tasks for:

- exploitation and incubators
- dissemination and communication
- certification and standardization

This deliverable D5.4 has three main sections, one for each of these corresponding tasks. In each of these sections, the achievements of the consortium within the third year of the project are described. This deliverable builds on the information and activities already described in the reports of the previous years. This deliverable does not reiterate all the information of the previous reports, but only information that is needed to better describe the 3rd year developments.

Overall, the activities performed in this project demonstrate that the consortium has achieved all Key Performance Indicators (KPIs) defined in the Description of Action (DoA) and related to this WP for the duration of the third year of the project. We elaborate on the KPIs achieved in the Introduction of the deliverable.

In general, the effort to collect and report the activities performed by each partner within this work package revealed a great wealth of different activities. In particular, the consortium partners have performed communication and dissemination activities to promote the project, its goals and its results, efforts to improve existing standards and create new certifications and standards. In addition, several partners have demonstrated great reach to many incubators and accelerators that can help CONCORDIA in the near future to deploy its novel technics and build successful and profitable business models around them. Finally, the efforts related to certification and standardization have already provided outcomes.

Within this year's deliverable (as also in the one of the previous year), a separate section has been included per task to provide a summary of the effect of the COVID-19 pandemic crisis on the activities related to the relevant task.

# Contents

# 1. Introduction

CONCORDIA project has defined in its main activities the WP5, whose purpose is to boost the impact of the project through strategic activities in exploitation, communication, dissemination, and standardization. From an exploitation perspective, WP5 develops a comprehensive plan that will be executed during the project, in alignment amongst others with the partners' commercial and research interests. This plan will help the project reach its objectives while at the same time help partners to push their cybersecurity-related technology built within CONCORDIA to the EU market. The project, via WP5 activities, is also committed to strong dissemination and communication via various tactics and multiple audiences. Furthermore, the standardization activities in WP5 aim to enhance the impact of CONCORDIA by transferring project results to relevant industry standardization and best practice working groups.

WP5 is broken down into 3 main tasks, that allow CONCORDIA to build on necessary activities in exploitation, dissemination, communication, certification and standardization:

- Task T5.1: Exploitation and incubators (Lead: TID & ATOS)
- Task T5.2: Dissemination and communication activities (Lead: MUNI)
- Task T5.3: Certification and standardization activities (Lead: TUVA)

**Key Performance Indicators on Impact:**
The project has defined a list of KPIs to quantify the impact of the project's results. Next, we selected the KPIs that are relevant for the activities pertaining WP5 (all KPIs are listed in the DoA), and report progress made for each of these KPIs, at the end of the M36 of the project (i.e., ¾ of the project's duration):

Table 1: Performance of CONCORDIA against specific KPIs

| General KPI | Goal in 4 years | Performed in M1-M36 | Unit of measure |
|---|---|---|---|
| CONCORDIA in social media | 15000 | 56 000 + | Views + Likes (see Section 3 for details) |
| Publication of Case Studies Documents – White Papers | - | | Blog posts (see Section 3 for details) |
| Downloads for public deliverables, prototypes, promotional material | 500+ | 9170 + | Downloads |
| Dissemination material in the form for documents, papers, deliverables, technical reports, presentations, fact sheets | - | Done | Flyers, deliverables, papers, technical reports, presentations, etc. (see Section 3 for details) |
| Organization of workshops and conferences | At least 1 major event and 3 | | Open Door Event (see Section 3 for details, and Deliverable D4.9) |

| | | | |
|---|---|---|---|
| | satellite or special events | | |
| Targeted focus groups with EU officials, policy makers, ECSO and cPPP officials | - | Done | Engagement with key stakeholders via meetings and group activities (see Section 3 for details) |

To reach these KPIs, the project has invested a lot of effort in the dimensions of exploitation via different avenues, dissemination, communication, standardization, and certification.
The project had several achievements in this Work Package, that are reported in separate sections, one per main Task.

- Efforts on Exploitation (Section 2):
  - 32 incubators and accelerators have been identified, information was collected for each one, including number of start-ups they support, capital, market focus, maturity of start-ups supported, contact information, etc.
  - 32 exploitable results have been identified, that can lead to separate start-ups or new business units within the partners reporting them.
- Efforts on Dissemination and Communication (Section 3):
  - 37 events / conferences / invited talks / seminars held or attended by the consortium partners and its members.
  - 35 blog posts published on CONCORDIA website or in prominent technology websites, written by CONCORDIA partners explaining technology they built, their services offered, etc.
  - 39 infographics and 27 videos that communicate the main contribution
  - 16 960 users visited the CONCORDIA website from around the world during the third year of the project.
  - 284 Twitter posts / 260 Facebook posts / 316 LinkedIn posts.
  - 18 000 of total engagements across social media platforms.
  - 31 announcements posted on the CONCORDIA website.
  - 19 news and other activities providing high publicity to the project's activities.
- Efforts on Certification and Standardization (Section 4)
  - 36 Standards Developing Organizations have been identified from the consortium partners as organizations developing standards that are relevant to the work performed within the CONCORDIA project.
  - CONCORDIA partners have declared that they participate in 66 activities of Standards Developing Organizations and Stakeholder Groups.

**Structure of the deliverable:**
In the next three sections, we analyse the objectives of the main tasks of WP5, discuss the strategy adopted to achieve them, highlight the progress of each task and the relevant impact of the COVID-19 pandemic crisis up to the submission date of this deliverable. Section 5 contains the conclusions that can be drawn about the activities described in this deliverable.

The following is a high-level map to this document:

**Section 1** : Contains the introduction to the document and its content
**Section 2** : Contains information on Exploitation
**Section 3** : Contains information on Dissemination & Communication
**Section 4** : Contains information on Certification & Standardization

**Section 5** : Contains the concluding remarks to this document

**Annex A** : Minutes for ISC semi-annual meetings in Year 3.
**Annex B** : Contains the Report from the first pilot phase of the $C^3$ by CONCORDIA
**Annex C** : Contains more information regarding the efforts regarding the possible certification of cybersecurity MOOCs.

# 2. Efforts on Exploitation

## 2.1. Objectives of this Task (T5.1)

The CONCORDIA project aims to achieve its goals on exploitation of its results from academia and industry, by focusing on the different sub-objectives, detailed in task T5.1 and old task T3.5 of the project and in the Grant Agreement of the project:

- To analyse the exploitation possibilities of the CONCORDIA project, based on the list of the exploitable results.
- To develop exploitation channels around specific incubators and by supporting cybersecurity start-up ecosystem.
- To support business-oriented promotion of key exploitable results (KER) in order to ensure early market adoption and user onboarding.

The activities of this task (after the merging of T3.5 and T5.1 was approved in amendment AMD-28 at the end of Y2 and reported in Deliverable D5.3[1]) are the following:

- **A1:** Set-up innovation and exploitation steering sub-committee: meet twice/year to review potential of technology, pilots, and technical progress made by each partner.
- **A2:** Guide and support partners to develop business plan to formalize exploitation strategy based on tech results and Intellectual Property Rights (IPR) protection. The sub-committee will identify novel ideas worthy of support, patentability, promotion of top candidates, etc.
- **A3:** Set-up protected *knowledge management area* in CONCORDIA website (e.g., within Confluence space) for controlled dissemination and exploitation.
- **A4:** Perform commercial exploitation based on strong CONCORDIA industry, outcomes used internally in consortium and externally in incubators and new start-ups.
- **A5:** Create environment for deployment and validation of prototypes before large-scale roll-outs.
- **A6:** Carry-out continuous sector monitoring, attending special interest group (SIG) meetings with key stakeholders who are invited to demo-days, and kept informed of CONCORDIA's progress and are actively involved in its ecosystem.
- **A7:** Support and guide partners in EU knowledge sharing through workshops, events, and interaction with stakeholders
- **A8:** Provide support of services related to incentive models for threat intelligence data sharing.

## 2.2. Strategy to achieve Task Objectives

The overall strategy of the project for achieving the revised T5.1's objectives has been to put effort during the third year of the project in the following steps:

- Maintain the Industrial Strategy Committee (ISC) active and engaged with the exploitation efforts of the project, including collecting ideas on how to achieve the expected outcomes from this task, as well as discussing, filtering, providing advice on and prioritizing the received input from partners and key stakeholders outside the project. Related activities: A1, A5, and further discussed in Section 2.6.
- Receive input (via surveys) from partners for critical activities of this task such as declaration of exploitable results, important technology built, available or reachable

[1] CONCORDIA Deliverable D5.3: 2nd year report on exploitation, dissemination, certification and standardization

incubators and accelerators, business models, etc. Related activities: A2, A3, A4, and further discussed in Section 2.2.1.
- Communicate to partners material collected and placed in the knowledge management area of CONCORDIA (Confluence tables and pages), and request for further input, corrections and updates, as well as communicate potential avenues for knowledge sharing in events with key stakeholders Related activities: A3, A7, and further discussed in Section 2.2.2.
- Consult with external key stakeholders for extracting new insights and capturing important trends outside the project, as well as incentives for knowledge sharing on threat intelligence. Related activities: A6, A7, A8 and further discussed in Section 2.2.3.

### 2.2.1. Strategy in collecting and ranking partner input

In order to collect and rank input provided from the partners, the ISC followed the same strategy described in last year's Deliverable D5.3, Section 2.2.2., and for brevity, it is omitted from this deliverable.

### 2.2.2. Strategy to promote exploitable results

We perform continuous monitoring of the cybersecurity sector via participation to key events in industrial and academic meetings, as well as demonstration and innovation days organized by CONCORDIA or other cybersecurity initiatives (e.g., Cyberwatching.eu). This activity is executed in collaboration with partners in WP3 (T3.4). Furthermore, in order to communicate our conclusions from the exploitable results (ER) collection effort, and ISC prioritization of key exploitable results (KER), we participated in events targeting potential users. At COD event, for example, we presented the process for collection of KERs of the project, and demonstrated with demos and other means the technology and the use-cases of the project (e.g., Demo of the Collaborative KYC, panel discussion on the Code of Engagement for the Trusted Threat Intelligence Sharing Platform, etc.). We also regularly participate in conferences, industrial fora and meetings to promote KERs, and keep potential early adopters engaged with the project and involved in the CONCORDIA ecosystem.

## 2.3. Exploitable Results

Exploitable Result (ER) is considered any form of tangible or intangible project result:
- **Intangible result:** technical or business consulting, system integration capacity, etc.
- **Tangible result:** software component, tool, prototype, service suite, etc.

Such items are candidates to become CONCORDIA ERs. Each ER has an assigned owner that serves as the main contact point. Also, when possible, the partners were asked to briefly discuss the level of maturity of the declared ER, and even use a Technological Readiness Level (TRL)[2] encoding to declare the maturity of the ER. The list of collected ERs is reviewed by the ISC every six months, during the regular biannual meetings.

The last round of input (December 2021) received from 26 partners revealed 32 ERs. A brief analysis of the declared items follows. The majority of ERs declared are software and services (~75%), with other ERs such as reports, processes, etc., completing the other ~25%.

[2] TRL: https://ec.europa.eu/research/participants/data/ref/h2020/other/wp/2016_2017/annexes/h2020-wp1617-annex-g-trl_en.pdf

In general, we had the following breakdown on eight types of ERs declared:

- Software: 19 (some software ERs were declared as service as well)
- Service: 9 (some service ERs were declared as software as well)
- Standardization: 1
- Certification: 2
- Report: 3
- Process/Methodology: 1
- Course: 1

In particular, we had software ERs being declared such as the following:

- QUIC Flowmon Probe plug-in
- MISP to Flowmon ADS integration
- TLS Flowmon Probe plug-in
- Flowmon to MISP integration
- Financial Threat Intelligence Platform
- Telco Threat Intelligence Platform (TIP)
- Threat Modelling Framework for mobile network
- DDoS clearing house
- Gorille Cloud
- deNAT: Detection of IoT models behind a home NAT using LightGBM
- Efficient Graph-based Malware Detection using Minimized Kernel and SVM
- Passwordless Authentication and Identity Verification KYC Solution
- DeepStream: Autoencoder-based stream temporal clustering
- Efficient Cyber Attack Detection in Industrial Control Systems Using Lightweight Neural Networks and PCA
- Patient platform as part of the demo for remote health service from home
- MMU-based access control for libraries (Prototype (Open-source Software)
- SecRiskAI (Prototype (Open-source Software)
- SERViz (Prototype (Open-source Software)
- SecBot (Prototype (Open-source Software)

Furthermore, we had services ERs being declared such as the following:

- Centralized Clearing House (CCH)
- Certified Cybersecurity Consultant - C3 by CONCORDIA
- Financial Threat Intelligence Platform
- Certification scheme for Cybersecurity MOOCs
- Federated Learning as a Service
- Patient platform as part of the demo for remote health service from home
- Reference architecture for e-health pilots
- Reference architecture for Automotive pilots
- Industrial-grade BC/ IoT system for the Automotive supply chain

Finally, we had other types of ERs being declared such as the following:

- Course "Becoming a Cybersecurity Consultant"
- Cybersecurity Threat Landscape (technical aspects)
- Methodology for developing and deploying courses for professionals
- OASIS standardization for cyber intelligence

- Ministerial Decree (Legislation)

These ERs were collected from 19 industrial and 7 academic partners. The majority (65%) of ERs that reported Technical Readiness Levels (TRL) are still in their early stages of maturity (TRL3-4), covering different industrial sectors and pilot tasks. On the other hand, all declared ERs that were reported with specific technical readiness, are expected to be elevated with respect to technical readiness by the time the project is completed (M48). In fact, this readiness gets the declared ERs closest to the market (TRL7-9). Next, we outline some interesting breakdowns on maturity, industry involved and CONCORDIA task related to their definition and applicability.

Current Technical Maturity:
- TRL3-4: 19
- TRL5-6: 4
- TRL7-9: 4

Envisioned Technical Maturity:
- TRL3-4: 8
- TRL5-6: 7
- TRL7-9: 12

Industries involved:
- Telco
- Finance
- Operators of Essential Services / Digital Service Providers
- E-health
- Automotive
- Any industry sector (60% of ERs declared they are applicable to any sector)

CONCORDIA Tasks involved / applicable:
- T2.1, T2.2, T2.3, T2.4
- T3.1, T3.2, T3.4
- T5.3

## 2.4. Start-up ecosystem

The methodology for data collection of relevant incubators and accelerators reachable by the consortium followed the same process as the one reported in D5.3, Section 2.4, and is omitted from this deliverable for brevity. We achieved a new higher number of 32 relevant entities by end of Y3, in comparison to 26 by end of Y2. In Y3 of the project, CONCORDIA also continued its collaboration with ECSO on start-up activities and enhanced this effort with additional collaboration with the other 3 pilot projects, not only on start-ups, but also on SME issues.

We have interviewed several start-ups for the CONCORDIA newsletter, such as Gaptain[3], Firmalyzer[4] and PHYSEC[5], which is a start-up that was named the winner of ECSO's European Cybersecurity STARtup Award by an independent jury.

The European Cybersecurity STARtup Award was created to increase the awareness and visibility of state-of-the-art cybersecurity companies in Europe, both at the European and the global levels. Besides this initiative, CONCORDIA also supported other ECSO initiatives, such as Investors Day. On the 15th -16th of June, ECSO held its 9th Cyber Investor Days, organised together with the National Cybersecurity Centre of Portugal (CNCS), while the 10th Cyber Investor Days, will take place on 1st – 2nd of December in Helsinki, Finland.

In 2021, ECSO presented several other initiatives that started in this organisation, such as dialogue on creation of cybersecurity specific investment fund, with the support from CONCORDIA.

Furthermore, the CONCORDIA PECS-UP newsletter had two issues dedicated and distributed to start-ups in Q1 and Q2 of 2021[6], while in Q3 and Q4 this newsletter was converted into sections of the larger CONCORDIA community newsletter, to reach a wider audience. Topics covered include deep tech, open innovation, overview of pre-seed accelerators for the commercialisation of academic work in the realm of cybersecurity, news from venture capital markets as well as information about many funding opportunities, including those from European Innovation Council[7], which has earmarked around €4bn to invest directly into start-ups.

Along these collaborative efforts of T5.1 during Y3, various issues were discussed among start-ups and other stakeholders. Fragmentation of EU cybersecurity market is often mentioned as one of the main barriers for any company, and in the case of start-ups it is even more pronounced. It is not only referring to issue of scale or access to market, but also to the other barriers that entrepreneurs can face, related to access to talent or capital. Some start-ups, for example, have this dilemma: to launch their business locally or EU-wide. Many start-ups do not have a physical office anymore, which is already a "declaration of intentions". Start-up risk factors are often triggered by local conditions, such as a change in the local rules, or the rise of a local champion.

One idea is to use cybersecurity community (CC) marketplace, which was already suggested as one of the strategic directions for the future European Cybersecurity Competence Centre, as the entry point and window for start-ups with the emphasis on early product and prototype visibility to reach larger audience, but also potential partnerships quickly. "Try before buy" or "test before invest" (for start-ups that look for investors) services could also be reflected in the envisioned marketplace. Also, we should remember that start-ups often struggle to show proof of value (PoV), and might need subsidy models involving the assumption that demand will grow after successful adoption through PoV executed in the framework of CC pilots (such as CONCORDIA pilots).

[3] https://gaptain.com/
[4] https://firmalyzer.com/
[5] https://www.physec.de/
[6] https://www.concordia-h2020.eu/news/4-pect-up-newsletter-2021-pan-european-cybersecurity-start-up-community/
[7] https://ec.europa.eu/research/eic/index.cfm

## 2.5. Industrial Strategy

### 2.5.1. Cross-Pilot Level

Network effect, economy of scale, partnerships for economic development, impact of support activities such as education, certification, and other issues have a prominent role in the exploitation of project results, and we have grouped these issues under the name "community factor".

This effort also triggered a slightly different innovation and exploitation strategy, as this factor in desirability (for example: Is threat intelligence sharing desired by the large community of relevant stakeholders?), feasibility (for example: Is trust scaling needed for wide EU adoption of threat intelligence sharing feasible?), and sustainability (for example: Is there an open community to maintain and support technical evolution of threat intelligence sharing platform?), has received more prominent role. In addition, the strategy was updated to work on ecosystem development and alignment at EU & MS level with vision and objectives of the European Cybersecurity Competence Center (ECCC). In October 2021, ENISA, ECSO and the four pilot projects (CONCORDIA, SPARTA, CS4EU, ECHO) submitted four recommendations to the ECCC, as a result of long consensus process about the future priorities of ECCC. Some of these strategic directions have to do with the exploitation, and are based on the CONCORDIA approach, such as acceleration of the investment in the development and production of cybersecurity products and services resulting from EU research activities.

In relation to marketplace as one of these strategic directions and objectives for the ECCC and community, CONCORDIA will start publishing (campaign CONCORDIA Delivers) and promoting ERs on its webpage (now we already have a few assets listed on https://www.concordia-h2020.eu/). This is not yet considered to be "exploitable results catalogue" or marketplace, but as a step in this direction, a meeting was organised with the SPARTA project, that has more advanced catalogue of results, so that the two projects could cross-feed their ER catalogues. Stimulating cost-efficient instruments for exploitation of results that rely on "community factor" described above, should also be considered.

Management of ideas and results (different maturity, moving at different speeds of TRL and Market Readiness Level (MRL) according to CONCODIA methodology (with yearly aggregation and ranking) would definitely increase impact and improve agility of ecosystem. However, optimization of data collection, in order to reduce overhead, needs to be considered.

### 2.5.2. Industrial Strategy Committee

Following this direction towards contributions of the CC to the ECCC, the CONCORDIA ISC was formed earlier-on in Y2, to take-on, among others, the responsibilities of the exploitation and innovation subcommittee as defined in the new task T5.1 of the GA. The ISC meets twice per year to review the potential of technology built within the project's technical work packages and use case pilots, and assess technical progress made from the partners towards the exploitation of the technology built. Furthermore, the committee is due to identify novel ideas worthy of support by the consortium in different ways. For example, some projects may need help with patenting and other IPR protection, PR and other media support, guidance in developing business plans, etc. The committee is also responsible for formalizing the exploitation strategy based on these technology results.

The committee's initial formation has 22 members (1 from each industrial partner at the time) and 1 chair (from ACS partner). The committee has met in the following times:

1) July 2020
2) December 2020
3) June 2021 (meeting minutes in Annex A
4) November 2021 (meeting minutes in Annex A)

This formation is re-assessed when new industrial members join CONCORDIA.

Among the ongoing tasks of the committee are the following:

1) Define and adapt (within the context of the project) what ERs are, as explained in subsequent subsection.
2) Redefine the important dimensions that should be collected from partners regarding ERs.
3) Redefine the important dimensions that should be collected from partners regarding the incubators and accelerators available within or associated with the consortium.
4) Perform assessment and ranking of collected ERs, to select Key ERs with high ROI.
5) Open or maintain channels of communication with said entities.

### 2.5.3. ER ranking into KERs

The ISC performed a ranking of 17 selected ERs from the list of all declared ERs, in order to assess which ERs will be the Key ERs for Y3. The ISC focused on tangible ERs such as the ones defined as software and/or service. The ISC assessed each ER on the following four dimensions, on a scale from 1 to 5:

A. Market Demand or Market Readiness Level (based on knowledge of market)
B. Innovation Potential (based on declared value proposition canvas if available, or knowledge of state of art)
C. Technical Maturity (based on declared TRL, knowledge of ER and the state of art space)
D. Network effect (why it should be done/promoted in CONCORDIA instead of another EU project, OR if the ER would benefit greatly by interacting with the CONCORDIA community and beyond)

The overall results for all selected ERs were the following:

| Exploitable Result | A | B | C | D |
|---|---|---|---|---|
| QUIC Flowmon Probe plug-in | 3.89* | 3.30 | 3.67* | 2.80 |
| Centralized Clearing House Service | 4.00* | 3.70* | 4.22* | 4.00* |
| DDoS Clearing House Service | 3.73* | 3.91* | 3.91* | 4.54* |
| Threat Intelligence Platform (TIP) | 3.40 | 3.40 | 3.20 | 3.64* |
| Financial Threat Intelligence Platform | 3.63* | 3.50 | 3.63* | 3.89* |
| Threat Modelling Framework for mobile network | 2.90 | 3.80* | 2.80 | 3.64* |
| Passwordless Authentication & Identity Verification Solution (KYC) | 3.33 | 3.22 | 3.50* | 3.10 |
| deNAT: Detection of IoT models behind a home NAT using LightGBM | 3.14 | 3.44 | 3.00 | 3.00 |
| Flowmon to MISP integration | 3.55 | 3.30 | 3.44 | 3.45 |

| | | | | |
|---|---|---|---|---|
| Patient Data Platform | 3.57 | 3.43 | 2.71 | 3.43 |
| Federated Learning as a Service | 3.13 | 4.22* | 3.29 | 3.63 |
| Gorille Cloud | 3.33 | 3.67* | 3.38 | 2.89 |
| Reference architecture for Automotive pilots | 2.88 | 3.25 | 2.88 | 3.50 |
| Reference architecture for e-health pilots | 3.63* | 3.38 | 2.71 | 3.67* |
| Industrial-grade BC/ IoT system for the Automotive supply chain | 3.13 | 3.50 | 2.88 | 3.14 |
| Cyber Attack Detection in Industrial Control Systems | 3.00 | 3.67* | 2.75 | 3.13 |
| DeepStream: Autoencoder-based stream temporal clustering | 2.75 | 3.38 | 2.71 | 2.86 |

The top five for each dimension were marked with red colour and asterisk. In some cases, we observed a tie, and therefore top 6 were marked. We have two ERs that mark high (top 5) in all 4 dimensions: a) *Centralized Clearing House Service*, and b) *DDoS Clearing House Service*. Also, the *Financial Threat Intelligence Platform* marked top 5 in 3 out of 4 dimensions.

Overall, using this ranking process, the ISC has found the 5-6 Key ERs of CONCORDIA for Y3, and is planning to support and promote them further to be shown to key stakeholders, as well as for demo events and help getting out in the EU cybersecurity market.

## 2.6. Promotion of results

Next, we outline a list of activities relevant to the task's goals, as well as demonstration of internal collaboration between CONCORDIA partners, or external collaboration with the other three pilot projects and key stakeholders:

- CONCORDIA-T5.1 (Aljosa Pasic-ATOS) attended a session called "Transfer to SMEs via demonstrators" of the virtual conference "Shaping a globally secure Industry 4.0 Ecosystem – Enabling international interoperable security policies". (January'21)[8]
- CONCORDIA-T5.1 (Aljosa Pasic-ATOS & Nicolas Kourtellis-TID) performed a first meeting with the SPARTA pilot project representatives for discussing potential collaborations between the two pilots on knowledge management tools. In fact, an outcome of the meeting was the definition of various actions to enable collaboration in knowledge exchange and in support to exploitation. Clustering and reporting of assets, as well as the workflow for feedback (e.g., market desirability, community value etc) was discussed, based on the pre-existing tool from SPARTA asset catalogue. (March'21)
- CONCORDIA-T5.1 (Aljosa Pasic-ATOS) attended the CERIS – SSRI virtual event about SMEs and start-ups in EU security R&I work programme. (April'21)[9]
- CONCORDIA-T5.1 (Jose Ruiz-ATOS) participated in an online panel discussion called "Developing SME Cybersecurity Resilience in Europe", organised by the pilot project CyberSec4Europe. The panel explored issues relating to developing SME's awareness of cybersecurity in order to improve resilience and responses to cyber-attacks. (May'21)[10]

[8] https://www.plattform-i40.de/IP/Redaktion/DE/Veranstaltungen/2021/2021-01-28-conference-it-security.html
[9] https://eu.eventscloud.com/file_uploads/ee5daa73b082a4c8763f3319c470ec8b_20210430-CERISSSRIWebinaragenda-final2.pdf
[10] https://digital-strategy.ec.europa.eu/en/events/developing-sme-cybersecurity-resilience-europe

- CONCORDIA-T5.1 (Aljosa Pasic-ATOS) participated in a collaboration with Cybersec4Europe pilot project. This was a workshop on Financial Threat Intelligence sharing under the name "Financial Sector Cybersecurity Collaboration and Engagement of Stakeholders" [11] , and was organized together with CONCORDIA T2.2 and performed online. This event, as well as the follow up in December'21, was organized by WP5 as a support for market uptake of exploitable results of CONCORDIA, in this case Financial Threat Intelligence Platform. The event was focused 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. Collaboration with the other pilots was achieved through invitation to Cybersec4Europe incident reporting platform demo. (May'21)
- CONCORDIA-T5.1 (Aljosa Pasic-ATOS & Nicolas Kourtellis-TID) performed a second meeting with the SPARTA pilot project representatives for discussing follow-up on collaboration for the knowledge management tool. The SPARTA representatives provided a demo of the RAMP tool and platform[12] for efficient management of research assets, or as we call them in CONCORDIA, ERs. (June'21)
- CONCORDIA-T5.1 (Nicolas Kourtellis-TID) participated in a panel organized by the DIGITAL SME Working Group Cybersecurity and Data Protection & Cyberwatching.eu regarding SME Impact & Opportunities[13]. In the panel, there were representatives from all 4 Cybersecurity Competence Centre Pilots, the EU Commission, Digital SME and ENISA, who were all part of the panel, as well as participants from all over EU. The topic was focused on opportunities for SMEs or Digital Innovation hubs to engage with the 4 pilot projects. Each of the 4 pilots presented their project and their vision and activities for engaging with the various SMEs inside their individual project, as well as the EU cybersecurity SME ecosystem at large. The CONCORDIA project explained its strategy to identify ERs from its research outcomes and how to push those in the market with the help of Incubators and Accelerators within the project's reach. (July'21)
- CONCORDIA-T5.1 (Aljosa Pasic-ATOS & Nicolas Kourtellis-TID) participated in a meeting between the 4 pilots called Start-Ups & SMEs Focus Group. Besides initial contribution for bootstrapping the Focus group, CONCORDIA participants also prepared material for follow-up by suggesting several common services, including:
    - Providing info about activities, goals, and results for start-ups/SMEs (e.g., CONCORDIA newsletter)
    - Enabling communication and exchange of knowledge
    - Sharing success and best practice stories
    - Education for entrepreneurs
    - Assessing EU cybersecurity agenda for the SME/start-up community, spot gaps and opportunities
    - Connecting large industry and start-up/SME community stakeholders
    - Providing details on innovation or start-up contest and awards
    - Providing joint 4 pilot policy feedback on SME and start-up issues
    - We also started working on supporting service scope and function (e.g., broker, marketplace for SME/start-ups etc) and service features/capabilities (e.g., training, access to finance, etc.) (September'21)

[11] https://www.youtube.com/watch?v=y-S0OudWRqE
[12] https://ramp.c3.lu
[13] https://www.digitalsme.eu/events/cybersecurity-competence-centre-pilot-projects/

- This year at COD2021, CONCORDIA went one step further than last year's COD, by presenting demos of some Key ERs, such as collaborative KYC and DDoS clearing house, while engagement of end users was addressed through session Code of Engagement for the Trusted Threat Intelligence Sharing Platform. (October'21)
- The CONCORDIA partner KYPO was named a finalist of Inno Radar prize[14] in the Final event. (October'21)[15]
- CONCORDIA-T5.1 (Aljosa Pasic-ATOS) participated in a follow-up of the May event for Financial Sector Cybersecurity Collaboration and Engagement of Stakeholders. (December'21)

## 2.7. Impact from COVID-19 pandemic crisis

As explained in D5.3, the pandemic affected or even interrupted the work of several CONCORDIA teams, either academic or industrial, and hindered or even stopped their technical progress. This situation persisted in this year (Y3). The impact of COVID-19 is detailed more clearly in the corresponding deliverables due in M36, and we encourage the reader to check those for more details. Overall, there was a marked slowdown in getting closer to ERs that are demonstrable to key stakeholders, or even worthy of pushing to an incubator / accelerator to hit the market.

That said, the CONCORDIA partners were able to react to the Task 5.1 calls for:

- Defining (or adapting) their ER
- Providing more information about their ER's novelty and value
- Helping T5.1 leader with assessing the landscape of technology built within the project.

Due to these efforts, we succeeded in collecting a sufficient number of ERs (32), which is even higher than Y2 (30), and some more incubators and accelerators in reach of the consortium (32) in comparison to Y2 (26).

However, there were several efforts impacted by COVID-19 regarding Task T5.1, which were planned for execution during Y3, but COVID-19 has severely slowed them down. They are now being planned for execution in the upcoming and final year of the project.

## 2.8. Next Steps

During the first three years of CONCORDIA, we have had innovative ideas and ERs at different levels of technological and market maturity, which is exemplified by the starting and finishing TRL of ERs. This was already expected in an ecosystem such as CONCORDIA, with many parallel researches and use-cases, and was anticipated by the choice of "spiral" methodology (see D6.2) where different ERs would receive a different treatment according to their maturity level and actual needs. Besides, CONCORDIA also focused on the integration of the previously separated or unrelated ERs, which resulted in more robust value propositions with solid chances of adoption and sustainability plans.

For the next and final year Y4, we plan efforts such as the promotion of Key ERs, as identified by the ISC, into the cybersecurity market. For this, we will engage the Incubators and Accelerators entities that have been collected so far and are in reach of the consortium,

[14] https://www.innoradar.eu/innovation/40258
[15] https://www.innoradar.eu/innoradarprize

so that they help us with this process of defining proper and competitive business models, as well as building successful start-up teams for carrying out the work needed to bring Key ERs to the market.

Also, another effort will be the active collaboration and ER/data/intelligence/tool sharing between CONCORDIA and the other 3 pilots. This effort started already this year, but was not particularly easy to execute, since the COVID-19 pandemic restricted resources of many partners across all 4 pilots, with respect to access to labs and offices, planning of collaborative or brainstorming meetings, etc.

Also, in the final year of innovation and exploitation activities, we propose to further cluster ERs and innovative ideas according to their TRL and the expected support services. These clusters include:

- Capacity building cluster (CB): ERs that need support in terms of capacity building, such as training in managerial or entrepreneurial skills.
- Access to market cluster (A2M): ERs that need support in terms of access to finance, access to clients, IPR or business development.
- Technology maturation cluster (TM): ERs that need support for the further development or integration with the other technologies or assets.
- Partnership and networking cluster (P&N): ER owners that are looking for the specific partnerships, e.g., outsourcing, system integration, resellers, etc.

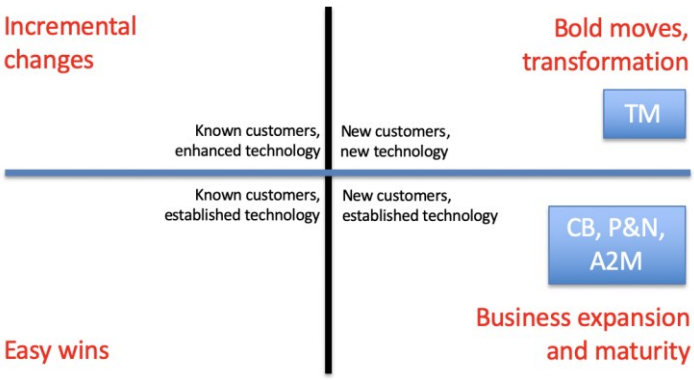



Figure 1: Potential ER clustering based on TRL and expected support services

# 3. Efforts on Dissemination & Communication

This section reports on the work executed in task T5.2 on Dissemination and Communication activities, with respect to the dissemination and communication strategy of the CONCORDIA project. The reported effort is organized in the following three sections:

1. The description of goals and objectives of this Task (Section 3.1).
2. The strategy to achieve these goals (Section 3.2).
3. The description of communication and dissemination activities performed in the third year of the project (Section 3.3).

The goals of the dissemination and communication task (Section 3. 1) and the strategy (Section 3.2) have been already defined and described in D5.3 but we decided to include them here as well for completeness.

## 3.1. Objectives of this Task (T5.2)

Dissemination and communication activities are essential for the CONCORDIA project and a dedicated task was designated for their implementation. The purpose of T5.2 and its main challenge, is to boost the impact of CONCORDIA project through dissemination and communication. In order to address this challenge effectively, the T5.2 uses the strategic approach based on the following logic (Figure **2**). Firstly, the general communication and dissemination goals were defined. These goals are aligned to the project objectives and they serve as the main guiding principles for our dissemination and communication. Secondly, specific communication and dissemination objectives were defined in order to implement the general goals. Thirdly, the communication and dissemination strategy was built in order to achieve the objectives.


Figure 2: CONCORDIA dissemination and communication logic

Whereas the general dissemination and communications goals remain the same during the whole project, dissemination and communication objectives can be updated in order to take into account internal evaluations, reviewers' recommendations, phase of the project or the context in general.

Dissemination and communication objectives of the project were focused especially on publicity and branding during the first year of the project. The objectives were updated during the second year of the project in order to reflect the dissemination phase of the project (see Table 4) and the reviewers' recommendations. During the third year of the project, we continued with this communication approach. We still significantly focus on content marketing tactic. This is described in the section which deals with communication objectives. Involvement in communication activities and work on the communication goals of the project is a common task of all partners. A communication group oversees coordinating and implementing strategic communication activities. The group is led by Masaryk University (MUNI) and has three members who deal with the communication

activities and three members from other tasks who provide insight and help with coordination.

**Dissemination and communication goals:**

We defined four general dissemination and communication goals, which are aligned with the CONCORDIA objectives. These goals are aligned to the project goals and they serve as the main guiding principles for our dissemination and communication. They remain the same during the whole project.

Table 2: CONCORDIA communication goals

| Goal | Description |
|---|---|
| 1 | To build and to position the CONCORDIA brand to strengthen trust and raise awareness about the project. |
| 2 | To enhance the impact of CONCORDIA's outcomes by spreading knowledge and disseminating project results through all relevant channels to the outside world. |
| 3 | To exploit consortium communication potential by internal dissemination, gathering content about members activities and actively fostering their engagement. |
| 4 | To participate in building a common brand and in coordinated communication activities with the other cybersecurity pilots (SPARTA, ECHO and CyberSec4Europe). |

**Dissemination and communication objectives:**

In order to achieve the aforementioned goals, we defined specific objectives that will be executed by the project. These communication objectives defined below in Table 3 can be updated during the project in order to support communication goals appropriately.

Table 3: CONCORDIA Dissemination and Communication Objectives (DCO)

| DCO | Name | Description | When |
|---|---|---|---|
| 1 | Project website | We will create and regularly iterate the project website (www.concordia-h2020.eu). It will serve as a single-entry point to all the information about the project (project's presentations, deliverables, events, papers and publications, news, software updates etc.) and will support all of our communication goals. We expect more than 5,000 accesses per year worldwide. | M2 creation / continuous updates |
| 2 | Content Marketing | We will focus on the preparation of our own unique content with the purpose to show what we do and enhance the impact of our results. Especially we will focus on producing blog posts, newsletters, infographics, videos and webinars.<br><br>The number of unique materials generated is counted as KPI-DC-3 and downloads of them are counted as KPI-DC-4 (500). | M6–M48 |

| DCO | Name | Description | When |
|---|---|---|---|
| | | | |
| 3 | Social Media | We will actively use social media channels (Twitter, LinkedIn and Facebook) to promote our results, increase trust and build community. The activity will be monitored based on the total number of views and likes (15,000 as KPI-DC-10). | M1-M48 |
| 4 | Campaigns | We will lead communication campaigns – planned and coordinated communications activities focused on boosting the impact of concrete outcome (e.g., event, software, deliverable). | M15-M48 |
| 5 | Events | We will participate in relevant events in order to build our brand and share our results. | M1-M48 |
| 5 | Publicity | We will exploit all relevant communication opportunities which will occur during the project to support our communication goals. We will focus on media relations and we will also engage in cybersecurity initiatives, education activities, targeted focus groups with EU officials, policymakers, ECSO and cPPP officials and other stakeholder organizations. | M1-M48 |
| 6 | CCN communication activities | We will participate in coordinated communication activities with the other pilots (ECHO, SPARTA, CyberSec4Europe). This includes meetings, group calls, chairing the coordination communication group for six months every two years, preparation of events, and creating relevant content. | M1-M48<br>- chairing the coordination communication group for six months every two years (start M1-M6) |
| 7 | Visual Identity | We will prepare and constantly apply a CONCORDIA visual identity in order to build our brand. Specifically, this means the logo and various types of templates. | M1-M3 preparation<br>M3-M48 application |
| 8 | Offline activities | We will prepare printed materials (e.g., banners, posters and flyers) to raise awareness regarding the project and build the CONCORDIA brand by delivery of key messages to our target audiences. | M1-M48 |
| 9 | Publicity | We will exploit all relevant communication opportunities which will occur during the project to support our communication goals. We will focus on media relations and we will also engage in cybersecurity initiatives, education activities, targeted focus groups with EU officials, policymakers, ECSO and | M1-M48 |

| DCO | Name | Description | When |
|---|---|---|---|
| | | cPPP officials and other stakeholder organizations. | |
| 10 | Internal communication | We will spread knowledge within the consortium, and we will actively foster the consortium members and our partners to engage in dissemination and communication activities. We will provide regular internal instructions for our partners which accurately describe what to do to support our goals while keeping communications consistent. | M1-M6 preparation, M6-M48 regularly updates and reminders |

**Communication phases:**

CONCORDIA communication and dissemination activities are, in general, divided into five distinctive phases, as explained in Table 3: the starting phase of the project, the phase where publicity about the project is increased, the phase for disseminating project results, the closing phase where the project is finishing, and finally, the phase after the project's termination, in which we further promote the CONCORDIA's results to influence the definition of the future cybersecurity roadmap of EU. In every phase, we adjust our dissemination and communication objectives in order to reflect the phase specifics.

Table 4: CONCORDIA communication phases

| Phase | Description | Time | Dependencies |
|---|---|---|---|
| I. Starting phase | The purpose of this phase is to prepare the basic starting points for the successful implementation of communication activities. Especially, preparation of basic communication channels, the formation of a communication group and specification of communication strategy. | M1-M6 | |
| II. Publicity phase | The purpose of this phase is to increase publicity of the project and support the building and positioning of the CONCORDIA brand. We use a wide range of communication tactics and focus on professionals and the general public. We try to communicate with them in particular the basic facts about the project and our key messages. | M6-M15 | Cooperation of Consortium |
| III. Dissemination phase | At this phase, in addition to strengthening our brand, we will focus primarily on sharing project results and increasing their impact. | M15-M36 | Technical and scientific achievements of the project and Cooperation of Consortium |
| IV. Closing phase | This phase will build on the activities of the previous ones and, moreover, its purpose will be to promote the | M36-M48 | Technical and scientific |

| Phase | Description | Time | Dependencies |
|---|---|---|---|
| | cybersecurity roadmap (Task 4.4) and summarize the overall results and benefits of the CONCORDIA project. | | achievements of the project and Cooperation of Consortium |
| V. After project phase | During this phase, we will ensure that the website will stay alive for at least three (3) years after the completion of the project. This way all available material will be available to future projects and whoever is interested in the outcomes of CONCORDIA. The social media channels will also be active because the results of the project can also be found through those channels as well through internet search engines. | Three years | |

## 3.2. Strategy to achieve Task Objectives

In order to achieve our goals, we focus on strategic planning. Our communication strategy answers the following questions:

- What do we want to communicate?
- To whom do we communicate?
- How do we communicate?

Therefore, our dissemination and communication strategy consists of three parts which are interconnected and based on our dissemination and communication goals and objectives.

- CONCORDIA narrative, key messages and content
- Target audiences
- Dissemination and Communication tactics


Figure 3: CONCORDIA dissemination and communication strategy

### 3.2.1. CONCORDIA narrative, key messages and content

This section describes what we will communicate. The core of this part is our narrative which summarizes the brand story of our project, this narrative is then delivered in key messages and in our content. Figure 4 represents the simple scheme of this hierarchy.


Figure 4: Hierarchy of CONCORDIA dissemination and communications outputs

**CONCORDIA narrative:**
CONCORDIA narrative is the overreaching leitmotiv for our dissemination and communication activities. Its purpose is to maintain brand identity consistency in our communications. The narrative can be summarized as follows: European cybersecurity competencies are fragmented. Our mission is to lead their integration to build the European Trusted, Secure and Resilient Ecosystem for Digital Sovereignty of Europe.

**Key messages:**
CONCORDIA communications group uses two types of key messages. The first type is key messages which are coined for every communication campaign according to its audience and the objective of the campaign (e. g. call to participation/action or messages to raise awareness). These key messages are not listed here. The second type is key messages about the project itself. Their purpose is consistency in communication about the project identity. These key messages are listed in the Table 5.

Table 5: CONCORDIA key messages

| Topic | Message |
|---|---|
| Who we are and what is our purpose | We are a dedicated consortium of more than 50 partners. Our purpose is to lead the boosting of Europe's cybersecurity future. |
| What we do | We are leading the integration of Europe's excellence cybersecurity competencies into a network of expertise to build a secure, resilient and trusted ecosystem in Europe. |
| Why it matters | The cybersecurity ecosystem will be one of the pillars of Europe's future. We need to be secure and resilient against cybersecurity threats which are increasingly relevant to our whole society and also to the life of each of us. |
| What is our relation to other cybersecurity pilots | We are one of several Horizon 2020 projects, all of which share the purpose to help the EU retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market and to strengthen Europe's cybersecurity and place Europe in a leading position in cybersecurity. |
| How we differ from other cybersecurity pilots | • We comprehensively interconnect academia, SME, CERTs, public bodies, policymakers and moreover we have engaged several strong industry partners to ensure the lasting impact of our work.<br>• CONCORDIA is the first competence network which takes a holistic, scalable and technology-adaptive data-centric approach to cybersecurity.<br>• We are developing solutions like Threat Intelligence for Europe, DDoS Clearing House as building blocks of a European cybershield.<br>• We are developing innovative cybersecurity solutions with the industry in five vertical sectors.<br>• We are building a comprehensive European cybersecurity educational ecosystem. |
| What are the benefits of the CONCORDIA? | Creating a European cybersecurity competence network will bring many benefits. In fact, it will:<br>• Unite the fragmented European cybersecurity landscape which will lead to better cooperation and better use of research results.<br>• Bring innovation into research, education, policy, roadmaps and governance.<br>• Increase industry impact by actively considering its problems.<br>• Develop industrial pilots and next-generation cybersecurity solutions.<br>• Launch Open Calls to allow entrepreneurs and individuals to stress their solutions with the development.<br>• Devise a cybersecurity roadmap to establish technology, socio-economic, legal and privacy directions for Europe.<br>• Provide expertise to European policymakers and industry.<br>• Improve quality of life through advanced and safer services in Telecommunications, e-Health, Finance and e-mobility.<br>• Enhance Europe's digital sovereignty. |
| Call to action | Follow us on:<br>• Website: https://www.concordia-h2020.eu<br>• Twitter: https://twitter.com/concordiah2020<br>• LinkedIn: https://www.linkedin.com/in/concordia-h2020/<br>• Facebook: https://www.facebook.com/concordia.eu/ |

**Content:**
Three main categories of content were identified for CONCORDIA. These categories consist of topics on which we focus in our communications.

Table 6: CONCORDIA content

| Category | Topics |
|---|---|
| Facts about the project | This covers many topics which are not directly related to our results. For example, our successes, introducing of project partners, "backstage" information, planned actions, consortium internal events, etc. |
| Project results | Most of our content is focused on the results of work from WP1, WP2, WP3, WP4, WP5 and W6. |
| Reactions to context | In addition to the planned content of the first two categories, we will focus on production of content that will react to ongoing events relevant to the CONCORDIA project. |

### 3.2.2. Target audience

This section describes our target audience. Since CONCORDIA project has a large scope the simplification of segmentation is needed. The most relevant target audience groups were defined in relation to project objectives.

**Community of cybersecurity professionals**
Cybersecurity community at European level is the crucial target audience for CONCORDIA. Whether decision-makers or practitioners, they can benefit from CONCORDIA multidisciplinary approach to cybersecurity since it deals with a wide range of tasks (technical, legal, societal, economical). We will focus on building trust with the cybersecurity community and sharing of our results.

**CONCORDIA stakeholders**
The subsystem of the cybersecurity community is CONCORDIA stakeholders, a cybersecurity subjects who have already relation with CONCORDIA. Task 4.6 is focused on this audience.

**Scientific community:**
We address the scientific community to enhance the impact of CONCORDIA's multidisciplinary research outcomes. Targeted dissemination and communication activities are performed by the traditional means (conferences, workshop, papers) and communication group also disseminate the results to the cybersecurity community and to other relevant audiences.

**Private sector**
The private sector is the end costumer of CONCORDIA. Whether it's start-ups, SMEs or big industries, they all can strongly benefit from CONCORDIA outcomes. Targeted communication will be achieved via cooperation with specialized tasks (e. g. T5.1 Exploitation and Incubators). Communication with the private sector will build on existing relationships and informal communication channels. It will also be supported by media relations, social media, content marketing and printed materials.

**Public bodies and cybersecurity initiatives**
Our goal is to establish cooperation with public bodies and cybersecurity initiatives at European level in order to become CONCORDIA stakeholders. As in the private sector, we want to present our results to these entities and at the same time, we want to participate in their communication activities. National cybersecurity authorities, ENISA, ECSO, ECHO, SPARTA, CyberSec4Europe, Cyberwatching, etc. are particularly relevant.

**Media and the general public**
Media are mainly intermediary for reaching other target audiences. Our approach to the media is based on a selection of the most promising outcomes with a strong story. We will share them with specialized media at first. If relevant we will also address the mainstream media at European and national level to reach the general public in order to demonstrate the benefits of our project for everyday life.

**Consortium members**
We address the consortium members and partners to support the image of CONCORDIA's brand, to enhance the impact of CONCORDIA's outcomes and to exploit consortium communication potential.

### 3.2.3. Dissemination and communication tactics

This section describes which communication tactics (channels, methods and materials) we use to deliver our messages to the defined target audiences. Of course, not all communications tactics are relevant to all audiences in every case. Therefore, they need to be carefully chosen in order to fulfil the objective of the concrete communication action.

**Project website (www.concordia-h2020.eu):**
This is a single-entry point to all the information about the project (project's presentations, deliverables, events, papers and publications, news, software updates, etc.). This channel is relevant to all our target audiences and all our communication goals. The project website will also be propagated by all other channels. Website's traffic will be monitored via Google Analytics.

**Social media:**
These are in general relevant to all our target audiences, and they will primarily support the building of the CONCORDIA's brand, raising public awareness and enhancing the impact of CONCORDIA's outcomes. We will use these channels:

- Twitter: https://twitter.com/concordiah2020
- Facebook: https://www.facebook.com/concordia.eu/
- LinkedIn: https://www.linkedin.com/company/concordia-eu/

**Media**
Media are in general powerful channel for reaching our audiences. We will use press releases to inform these media about our most promising outcomes.

**Channels of cybersecurity initiatives and projects:**
These channels (e.g., Cyberwatching.eu platform, social media channels of cybersecurity projects, their websites) are very relevant for CONCORDIA since they have an audience which is important for our project. Therefore, we will actively ask for support by other projects and initiatives.

**Consortium members and partners owned media:**
There is huge potential in partners' owned media (their websites, social media channels, bulletins, events, etc.) for spreading the knowledge and project results. These media have the potential to help us reach our communication goals and address multiple audiences.

**Cyber Competence Network (CCN) pilots coordinated channels:**
CCN communication channels (website, Twitter, media relations, materials, etc.) are important tools for coordinated communications about CCN and they can also boost the communication activities of each pilot.

**Internal communication channels:**
Such channels will be used to transfer knowledge and project results within the consortium and also to gather the content about consortium members activities and foster their engagement. The main communication channels of CONCORDIA are:

- Email (Email mailing lists)
- Synchronized file repository (GIT, Confluence)
- Audio/video conferences
- Physical face-to-face meetings.

They are described in more detail in the Project Handbook (Deliverable D6.1).

**Printed materials:**
Items such as roll ups, banners, posters, flyers, etc., are a complementary communication channel designed to raise awareness of the project and build its brand by delivery of project key messages to our target audiences.

**Visual identity:**
By visual identity is meant especially the logo and templates for presentations, printed materials and posters. Visual identity is an essential tool for brand building, as it represents one of its most visible external representations. Together with our narrative and key messages, visual helps us to be consistent in our communication activities.

**Content marketing forms:**
We will use different forms to deliver our content. Especially relevant are blog posts, news items, copywrited texts, videos, infographics, white papers, deliverables, presentations and webinars. This list is not restrictive. On the contrary, we can use also other content form if it makes sense in given context.

**Communication campaigns:**
Communication campaigns are important communication tactic of CONCORDIA project. Coordinated communication activities in given period of time will boost a concrete topic much better than individual promotional acts. Our approach is based on using various forms of contents and all relevant channels to promote selected topic (e.g., event invitation, software release, important article).


Figure 5: CONCORDIA campaigns approach

## 3.3. Dissemination & Communication Activities

This section describes the dissemination and communication activities carried out during the third year of the CONCORDIA project. It is structured according to our dissemination and communication objectives, which were mentioned in the previous paragraphs.

### 3.3.1. CONCORDIA website

The CONCORDIA website (www.concordia-h2020.eu) is the main entry point to all the information about the project and also one of the main dissemination channels. Our target audiences are able to gain access to CONCORDIA results, publications, news and new tools developed in the context of this project through the website. During the third year of the project, we updated the homepage to improve the look and feel of the website. In order to better reflect the project targets and results, the Assets menu were enriched with new choices and content. The website has been regularly updated with new content (news items, websites, blog posts, events, etc.). The current version of the homepage is presented in Figure 6.


Figure 6: CONCORDIA website (homepage)

More information on how the website has been implemented, the various sections offered to the visitor and some more technical details are included in the deliverable "D5.1: Website and Social Media presences", which is listed under the Publications sections. In this section, we will provide some statistics for the third year of the project (2021).

**Website Visitors and Trend:**

The users that were served by the CONCORDIA website per week during the third year of the project can be seen in the Figure 7. We can see that almost 17000 users were recorded in this period. This means that we had an approximate of more than 55 visits on average. Last year's total users for almost the same time period were about 10000 users. The increase was about 70%. The spike during March is probably due to the traffic produced by the online plenary meeting that we had, while the increase that is visible in July is in accordance with the introduction of the sector-specific pilots and visibility that the CONCORDIA gained from the CODE annual conference that took place at that period. The figure also presents that these visitors created 23K sessions against the website which resulted in 46K served webpages.

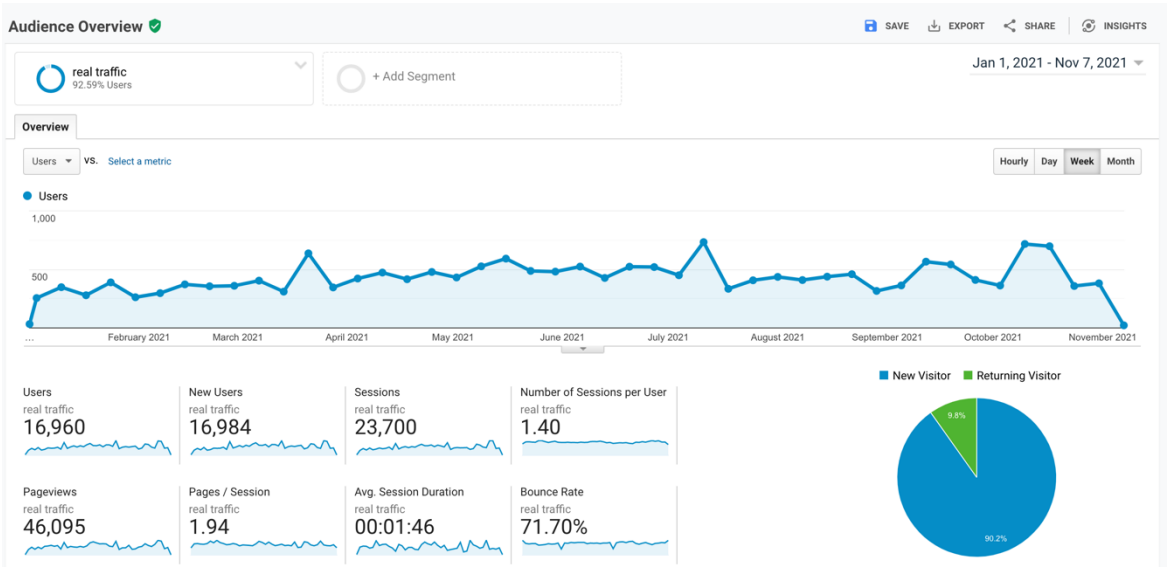



Figure 7: Users per week that visited the CONCORDIA website

Figure 8 presents the most popular pages of the website during the reporting period. Naturally, the most visited page is the welcome page followed by the Events Archive page which leads to our Cybersecurity Events Calendar. Users' pages are a new entrance to the website since from this year the users that have stored courses to the CONCORDIA courses map have accounts to our website with all the data concerning their courses. CONCORDIA Open Door Event continues to attract the interest of the visitors as well as the Consortium page and the Becoming a Cybersecurity Consultant page. It seems that the visitors were interested to learn more about the CONCORDIA consortium and their point of view through the CONCORDIA's weekly blog. Moreover, we can see that visitors are also interested in KYPO Cyber Range and in the CONCORDIA courses map.

Additionally, in Figure 9 we show the geographic origin of the visitors who requested all the previously mentioned pages from the CONCORDIA webserver. Most visitors come from Europe and Asia, followed by visitors from America and Africa.

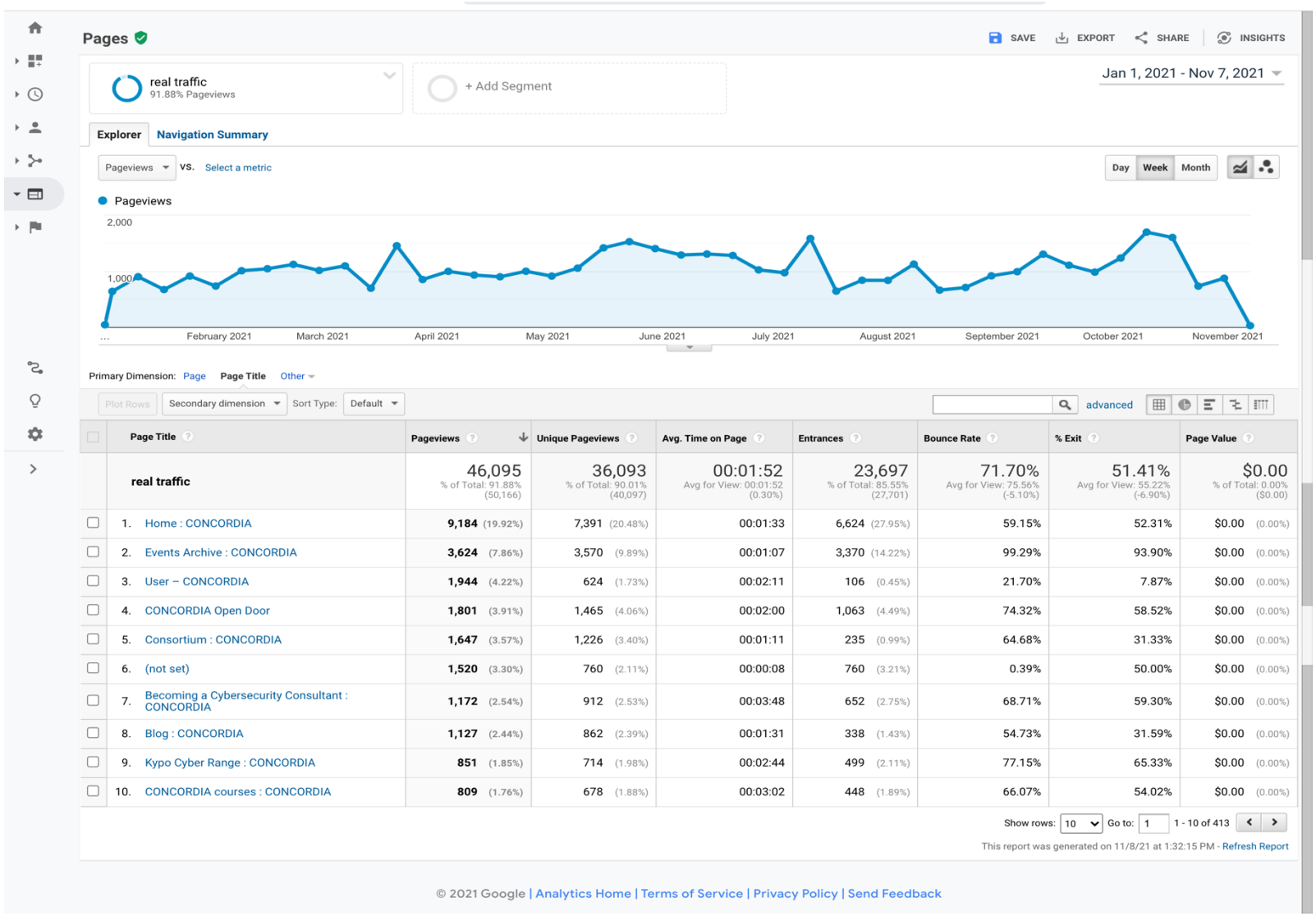
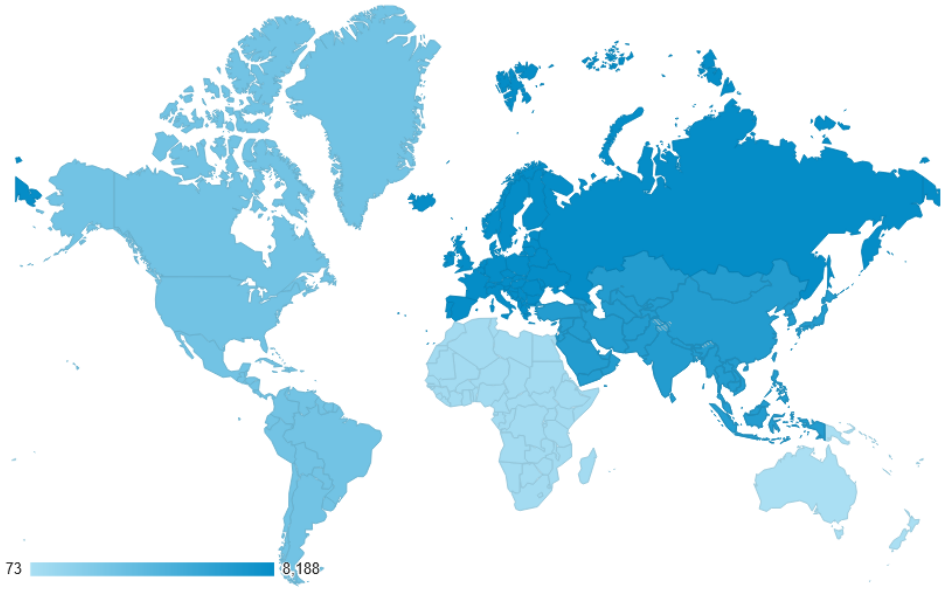



Figure 8: CONCORDIA pages with the most page views




Primary Dimension: Country City **Continent** Sub Continent

Secondary dimension ▾ advanced

| Continent | Acquisition | | | Behavior | | | Conversions | | |
|---|---|---|---|---|---|---|---|---|---|
| | Users ↓ | New Users | Sessions | Bounce Rate | Pages / Session | Avg. Session Duration | Goal Conversion Rate | Goal Completions | Goal Value |
| | 18,318<br>% of Total: 100.00% (18,318) | 18,332<br>% of Total: 100.04% (18,324) | 27,704<br>% of Total: 100.00% (27,704) | 75.56%<br>Avg for View: 75.56% (0.00%) | 1.81<br>Avg for View: 1.81 (0.00%) | 00:01:31<br>Avg for View: 00:01:31 (0.00%) | 0.00%<br>Avg for View: 0.00% (0.00%) | 0<br>% of Total: 0.00% (0) | $0.00<br>% of Total: 0.00% ($0.00) |
| 1. Europe | **8,188** (44.34%) | 8,081 (44.08%) | 14,716 (53.12%) | 63.29% | 2.36 | 00:02:37 | 0.00% | 0 (0.00%) | $0.00 (0.00%) |
| 2. Asia | **6,737** (36.48%) | 6,715 (36.63%) | 8,254 (29.79%) | 90.97% | 1.16 | 00:00:15 | 0.00% | 0 (0.00%) | $0.00 (0.00%) |
| 3. Americas | **2,835** (15.35%) | 2,829 (15.43%) | 3,556 (12.84%) | 87.96% | 1.23 | 00:00:16 | 0.00% | 0 (0.00%) | $0.00 (0.00%) |
| 4. Africa | **440** (2.38%) | 440 (2.40%) | 815 (2.94%) | 81.84% | 1.29 | 00:00:20 | 0.00% | 0 (0.00%) | $0.00 (0.00%) |
| 5. (not set) | **195** (1.06%) | 194 (1.06%) | 273 (0.99%) | 89.01% | 1.12 | 00:00:02 | 0.00% | 0 (0.00%) | $0.00 (0.00%) |
| 6. Oceania | **73** (0.40%) | 73 (0.40%) | 90 (0.32%) | 80.00% | 1.36 | 00:00:45 | 0.00% | 0 (0.00%) | $0.00 (0.00%) |

Figure 9: Users from various continents visiting the CONCORDIA website

### 3.3.2. Content marketing

Last year, we changed our communication focus from publicity and brand building to production of our own unique content and we continue with this communication tactic. The purpose is to show what we do and enhance the impact of our results. However, we did not resign from our communication goals since content production is effective way how to build reputation in organic way.

**Blog posts:**
We regularly deliver blog posts to our target audience. Our blog posts cover wide range of topics since they are written by CONCORDIA partners with different backgrounds in cybersecurity. We focus on what we do and where are the benefits in our blog posts. The blog posts are intended for cybersecurity professionals in general. Since the last review we have published 35 blog posts and we have 90 blog posts in total on our website.

Table 7: CONCORDIA Blog posts

| Topic | Link |
|---|---|
| An interview on our new research paper – A Novel Intrusion Detection System Against Spoofing Attacks in Connected Electric Vehicles | https://www.concordia-h2020.eu/blog-post/an-interview-on-our-new-research-paper-a-novel-intrusion-detection-system-against-spoofing-attacks-in-connected-electric-vehicles/ |
| A novel Cybersecurity Maturity Assessment Framework (CMAF) | https://www.concordia-h2020.eu/blog-post/a-novel-cybersecurity-maturity-assessment-framework-cmaf/ |
| The impact of State–sponsored Trolls during the 2016 US Presidential Election Discourse | https://www.concordia-h2020.eu/blog-post/the-impact-of-state-sponsored-trolls-during-the-2016-us-presidential-election-discourse/ |
| A new method to detect exploitable smart-home devices connected behind a NAT | https://www.concordia-h2020.eu/blog-post/a-new-method-to-detect-exploitable-smart-home-devices-connected-behind-a-nat/ |
| Smart Home and remote health services | https://www.concordia-h2020.eu/blog-post/smart-home-and-remote-health-services/ |
| CONCORDIA Start-up Community: Where do we find the greatest hits of EU cybersecurity new wave? | https://www.concordia-h2020.eu/blog-post/concordia-start-up-community-where-do-we-find-the-greatest-hits-of-eu-cybersecurity-new-wave/ |
| Securing Electric Mobility Charging Networks | https://www.concordia-h2020.eu/blog-post/securing-eletric-mobility-charging-networks/ |
| Women in Science, ICT and Cybersecurity | https://www.concordia-h2020.eu/blog-post/women-in-science-ict-and-cybersecurity/ |
| Swedish National Cybersecurity Node for Accelerating Innovation and Research in Cybersecurity | https://www.concordia-h2020.eu/blog-post/swedish-national-cybersecurity-node-for-accelerating-innovation-and-research-in-cybersecurity/ |
| Threats, Gaps and Challenges in the Era of COVID-19 | https://www.concordia-h2020.eu/blog-post/threats-gaps-and-challenges-in-the-era-of-covid-19/ |
| Challenges for Secure and Trustworthy UAS Collaboration | https://www.concordia-h2020.eu/blog-post/challenges-for-secure-and-trustworthy-uas-collaboration/ |
| Using the Data of the CONCORDIA Threat Intelligence Platform for Situational Awareness | https://www.concordia-h2020.eu/blog-post/using-the-data-of-the-concordia-threat-intelligence-platform-for-situational-awareness/ |
| DNS Resolvers and DdoS: The Good, the Bad and the Ugly | https://www.concordia-h2020.eu/blog-post/dns-resolvers-and-ddos-the-good-the-bad-and-the-ugly/ |

| | |
|---|---|
| New DdoS classifiers for the DdoS Clearing House | https://www.concordia-h2020.eu/blog-post/new-ddos-classifiers-for-the-ddos-clearing-house/ |
| Quo Vadis European Digital Sovereignty? | https://www.concordia-h2020.eu/blog-post/quo-vadis-european-digital-sovereignty/ |
| On the Recommendation of Protections Services | https://www.concordia-h2020.eu/blog-post/on-the-recommendation-of-protections-services/ |
| Roadmap for the 1st CONCORDIA Cybersecurity Skills Certification Scheme | https://www.concordia-h2020.eu/blog-post/roadmap-for-the-1st-concordia-cybersecurity-skills-certification-scheme/ |
| Building Machine Learning Models with Privacy by Design in Mind | https://www.concordia-h2020.eu/blog-post/building-machine-learning-models-with-privacy-by-design-in-mind/ |
| An Update on Security Playbook Standardization | https://www.concordia-h2020.eu/blog-post/an-update-on-security-playbook-standardization/ |
| US elections 2020: a retrospective analysis of the Twitter corpus | https://www.concordia-h2020.eu/blog-post/us-elections-2020-a-retrospective-analysis-of-the-twitter-corpus/ |
| Beyond COVID-19 in Threat Intelligence | https://www.concordia-h2020.eu/blog-post/beyond-covid-19-in-threat-intelligence/ |
| Cloud Security: Paving the Way to Smarter Security Automation! | https://www.concordia-h2020.eu/blog-post/cloud-security-paving-the-way-to-smarter-security-automation/ |
| CONCORDIA's Sector-specific Pilots – the basics | https://www.concordia-h2020.eu/blog-post/concordias-sector-specific-pilots-the-basics/ |
| Faith-based security, the case of the fax | https://www.concordia-h2020.eu/blog-post/faith-based-security-the-case-of-the-fax/ |
| Federated Machine Learning (FML) for Financial Sector Threat Intelligence and Fraud Prevention | https://www.concordia-h2020.eu/blog-post/federated-machine-learning-fml-for-financial-sector-threat-intelligence-and-fraud-prevention/ |
| The CODE 2021: Secure supply chains for digital sovereignty? | https://www.concordia-h2020.eu/blog-post/the-code-2021-secure-supply-chains-for-digital-sovereignty/ |
| Threat Intelligence sharing: What kind of intelligence to share? | https://www.concordia-h2020.eu/blog-post/threat-intelligence-sharing/ |
| Universal Adversarial Perturbations for Malware | https://www.concordia-h2020.eu/blog-post/universal-adversarial-perturbations-for-malware/ |
| The endless identity problem | https://www.concordia-h2020.eu/blog-post/the-endless-identity-problem/ |
| Creating trust through blockchain? | https://www.concordia-h2020.eu/blog-post/creating-trust-through-blockchain/ |
| CONCORDIA's Cyber Security Ecosystem: Virtual Lab, Services and Training | https://www.concordia-h2020.eu/blog-post/concordias-cyber-security-ecosystem-virtual-lab-services-and-training/ |
| On Customer Side Cloud Security | https://www.concordia-h2020.eu/blog-post/on-customer-side-cloud-security/ |
| QUIC protocol from the monitoring perspective | https://www.concordia-h2020.eu/blog-post/quic-protocol-from-the-monitoring-perspective/ |
| Cybersecurity Roadmap for Europe by CONCORDIA | https://www.concordia-h2020.eu/blog-post/cybersecurity-roadmap-for-europe-by-concordia/ |
| Developing and running a testbed for the DdoS Clearing House | https://www.concordia-h2020.eu/blog-post/developing-and-running-a-testbed-for-the-ddos-clearing-house/ |

**Videos:**

We continued with video production during the third year of the project on CONCORDIA YouTube channel. We produced 27 videos this year and the overall number of views is 4 823. Most of the videos are from "CONCORDIA stories" series. Stories are short and simple videos in which CONCORDIANS describe their work and their results.


Figure 6: CONCORDIA Stories Example
(https://www.youtube.com/watch?v=HYDUon6VEFI)

**Infographics:**

We created 39 infographics during the last year. They cover various topics which are relevant for CONCORDIA project. This year we focused especially on CONCORDIA Industrial Pilots, Economic Perspectives of Cybersecurity, Education, Women in Cyber and Cybersecurity Threat Map.

The infographics can be found on CONCORDIA website (https://www.concordia-h2020.eu/dissemination-material/).


Figure 11: CONCORDIA infographics example

**CONCORDIA women:**

In cooperation with task 4.5 (Women in Cybersecurity) we regularly promote women in CONCORDIA. We have published 35 content posts focus on the women in cyber topic since the last review.


Figure 12: Example of women in cyber content

**Promotional content:**

We support CONCORDIA outputs by the production of promotional content. We regularly promote CONCORDIA research papers produced by Work Package 1. We also focus on other outputs (e.g., CONCORDIA courses, Service catalogue and our newsletters).


Figure 13: Examples of CONCORDIA promotional content

We have continued promoting CONCORDIA experts. We want to show how diverse are our experts and also support networking since the project is after all about building a network. This content is then connected with the database of our experts on CONCORDIA website (https://www.concordia-h2020.eu/concordia-service-cybersecurity-experts/).


Figure 14: Example of CONCORDIA experts' activity

**Ad hoc content:**

Finally, we produced various types of ad hoc content in order to raise awareness about relevant events (international days, surveys, competitions etc.). We have 16 outputs of this type during the last year.


Figure 15: Example of ad hoc content output

### 3.3.3. Social media

CONCORDIA's presence is established in Twitter, LinkedIn and Facebook. Initial information can be found in the deliverable named "D5.1: Website and Social Media presences". In this section we will provide only the report on the social media activity for the third year of the project (2021). KPI-DC-10 for total views and likes in social media is defined as the sum of total likes on LinkedIn, reactions on Facebook and engagements on Twitter. Communication group does not have access to any type of social media

management software. Therefore, we are limited in reporting and analysis only to very basic tools which are offed by social media platforms for free.

**LinkedIn:**

Our LinkedIn network grew during the second year of the project. It enlarged from 1 371 connected accounts to 2 221. We have also 2 303 followers on LinkedIn. We published 316 posts on our LinkedIn channel and they in total achieved 2 543 likes and 118 300 views. The data were obtained using the LinkedIn site for posts and activity management.

Table 8: LinkedIn activity

| Months | Posts | Likes | Views |
|---|---|---|---|
| M24-M36 | 316 | 2543 | 118 300 |

**Twitter:**

Currently, we have 1544 followers on our profile. There were 284 original posts published, which had in total 11 699 engagements and 437 768 impressions. The data were obtained via Twitter Analytics.

Table 9: Twitter activity

| Months | Posts | Engagements | Impressions |
|---|---|---|---|
| M24-M36 | 284 | 11 699 | 437 768 |

**Facebook:**

Currently, we have 339 followers on our project profile. There were 260 posts published which, in total, achieved 3 807 reactions and achieved a reach of 29 403. The data were obtained via Facebook Insights.

Table 10: Facebook activity

| Months | Posts | Reactions | Reach |
|---|---|---|---|
| M24-M36 | 260 | 3 807 | 29 403 |

### 3.3.4. Campaigns

We started with the concentrated communication activities on different topics during the second year and we continued in this activity also in the third year of the project. In every campaign, we use our website, social media channels and content marketing. We also use direct mails, internal communications, media relations and cooperation with other subjects if it is relevant. The following table contains a list of our communication campaigns.

Table 11: CONCORDIA Campaigns 2021

| Name | Date | Goal |
|---|---|---|
| CONCORDIA Start-ups | 1. 2. – 28. 2. | To increase awareness about our activities for Start-ups |
| Cybersecurity and high schools | 8. 2. – 28. 2. | To introduce our activities and motivate people to participate in the survey |
| Cybersecurity & Diversity – campaign | 3. 3. – 10. 3. | To increase awareness about this topic |
| Infographics campaign (topic: Threats) | March | To support dissemination of CONCORDIA Threat Map activity |
| Cyber Range workshop | April | To motivate people to participate |
| Cybersecurity and Economy (SEConomy framework) | May | To motivate people to participate |
| CONCORDIA pilots | Summer | To increase awareness of CONCORDIA services |
| CONCORDIA course map | September | To attract as many relevant people as possible to contribute to CONCORDIA Courses Map |
| CONCORDIA Open Door campaign | September/October | To motivate people to participate |
| CONCORDIA Road map | October/November/December | To increase awareness about the CONCORDIA Road map |

### 3.3.5. Events

The following table includes a list of 37 events – conferences, presentations, workshops and other events where CONCORDIA was present through participation of its partners. The events are of different types and the table presents the title, type of event, date it was performed and location in the world. The number of events is impacted by the ongoing COVID-19 situation. Scientific events for representation of research papers are listed in Deliverable D1.3. Communication group also cooperated on preparation of CONCORDIA Open Door event 2021. More information about this event can be found in deliverable D4.9.

Table 12: CONCORDIA Events 2021

| Title | Event | Date | Place |
|---|---|---|---|
| EU Cybersecurity Skills Gap: Situation and way forward. | 17th Student Conference DET | May 18, 2021 | Athens |
| Mesa Redonda: Desde la Educación, pasando por la I+D, hacia la Empresa Inteligente | JNIC 2021 | June 10th 2021 | Online |
| Security threats, trends challenges and gaps | PhD Course | February-March 2021 | Milan |
| Governance, Risk and Compliance in Distributed Architectures | PhD Course | May-June 2021 | Milan |
| Project Presentation | Presentation | May 19, 2021 | Athens |
| Linking Standardization and Certification Plans for the future | Cyberwatching event | July 13, 2021 | Online |
| The Future of Cybersecurity in Slovenia and Europe | Presentation of CONCORDIA | October 4, 2021 | Ljubljana & Online |
| Demonstrating the DdoS Clearing House distributed testbed | La Fabrique Défense | December 9, 2021 | Nancy & online |
| Project presentation | CyberHOT Summer School | September, 2021 | Chania |
| Developing and Evaluating a DdoS Clearing House for Europe | Euritas Summit | September, 2021 | Brussels, Online |
| DdoS Clearing House for Europe | NBIP@20 | July, 2021 | Utrecht, NL, and online |
| DdoS Clearing House for Europe | ICANN71 vTechDay | June, 2021 | Online |

| | | | |
|---|---|---|---|
| DdoS Clearing House for Europe | ABNAMRO Bank online meetup | May, 2021 | Online |
| DdoS Clearing House Update | Plenary meeting if Dutch anti-DdoS Coaltiion | February, 2021 | Online |
| No More DdoS – Anti-DdoS Coalition | Inter-ISAC meeting NL | January, 2021 | Online |
| SIDN Labs activities (including a discussion on the DdoS Clearing House) | NGI talks (Next Generation Internet) | January, 2021 | Online |
| Cybersecurity Competence Centre Pilot Projects: SME Impact and Opportunities | DIGITAL SME Working Group Cybersecurity and Data Protection & Cyberwatching.eu | July 2021 | Online |
| Fast Kernel Error Propagation Analysis in Virtualized Environments | IEEE ICST | April 2021 | Online |
| Failure Diagnosis for Cluster Systems using Partial Correlations | IEEE ISPA | Sept 2021 | Online |
| IFIP WG10.4 Meeting on Intelligent Vehicles Dependability and Security | Conference | Jan 2021 | Online |
| Project Presentation | Presentation BAE Systems | Feb 2021 | Online |
| Roadmap Presentation: | Presentation Philips | Mar 2021 | Online |
| Roadmap Presentation: NEC & SAP | Presentation NEC & SAP | Mar 2021 | Online |
| T1.3 Presentation: EPSRC | TAS-S Workshop | Mar 2021 | Online |
| Roadmap Presentation: EC SANCUS Project | Presentation | Jun 2021 | Online |
| T1.3 Presentation | IFIP WG10.4 Mtg | Jun 2021 | Online |
| T1.3 Presentation | Presentation/Discussions: Microsoft Research + Amazon | Jul 2021 | Cambridge, UK |
| Roadmap Presentation | Presentation at NSF | Jul 2021 | US |
| Roadmap Presentation | Presentation at Finnish ICT Unit | Sep 2021 | EU |
| T1.3 Presentation & Discussions | VW, Continental and HPI | Nov 2021 | EU |

| | | | |
|---|---|---|---|
| T1.3 Presentation & Discussions | TU Munich, LMU and Bosch | Nov 2021 | EU |
| Career Path towards Cybersecurity | ECSM 2021 Campaign | 18 OCT 2021 | ONLINE |
| Career Path towards Cybersecurity | ECSM 2021 Campaign | 18 NOV 2021 | ONLINE |
| Career Path towards Cybersecurity | ECSM 2021 Campaign | 14 DEC 2021 | ONLINE |
| Securing Runtime Memory via MMU manipulation | SECURWARE | 14-18 November | Online/Athens |
| CONCORDIA-Cybersecurity for mobile communication systems | OPTICS2 Dissemination Event 'Security' | 28th of September | Online |
| Security challenges for collaborative autonomous aircraft systems | Security Lancaster Lecture Series | 12th of November | Online |
| Presentation of CONCORDIA | La Fabrique Défense | December 9, 2021 | Nancy, France & online |
| Malware: a Patrol to detect dormant variants | FIC (International Cybersecurity Forum) | September,8th2021 | Lille, France |
| Malware hunting patrol | Hack'IT'N conference | May, 27th 2021 | Online |
| General presentation | European Cyber Week | November, 16th-18th 2021 | Rennes, France |
| Morphological analysis solution to characterize unknown or obfuscated malware | Cercle de l'Arbalète | November, 18th 2021 | Military School, Paris, FR |

### 3.3.6. Publicity

This section describes publicity results and activities during the third year of the project. Even though that publicity is not the main goal during the dissemination phase of the project, it is still important part of project communication activities.

**Publicity outputs:**

These communication activities helped to increase the publicity of the project. We had 19 publicity outputs in the third year of the project, as summarized in the next table. Publicity outputs were influenced by the ongoing COVID-19 situation – there is lower number of opportunities to promote the project. Especially face to face networking that is a natural part of every physical event is missed in the COVID-19 era.

Table 13: Publicity outputs

| Publicity date | Publicity info | Type |
|---|---|---|
| 21-10-2021 | CONCORDIA Women Awards success article | News item |
| 14-10-2021 | Developing and running a testbed for the DdoS Clearing House Demonstrating the DdoS Clearing House in a representative simulated environment | Blog |
| 13-10-2021 | Event with industry at the Faculty of Electrical Engineering and Computer Science where CONCORDIA was presented in the lab of UM team | News item |
| 04-10-2021 | Gabi Dreo Rodosek participated in the event "The Future of Cybersecurity in Slovenia and Europe" presenting CONCORDIA project as well as participating in the Round Table – Establishment of Cybersecurity Competence Network in EU. | Presentation |
| 30-09-2021 | Cristian Hesselman presenting "Developing and Piloting a DdoS Clearing House for Europe" at the Euritas Summit / Cyber Security Panel | Presentation |
| 28-09-2021 | Cora Lisa Perner presented CONCORDIA in OPTICS2 Final Dissemination Event | Presentation |
| 23-09-2021 | CONCORDIA Open Door Virtual Event -Cybersecurity 20th and 21st of October – Arthur Strategies & Systems | Blog |
| 07-09-2021 | Sotiris Ioannidis, Despoina Antonakaki and Jean-Yves Marion with the four Cybersecurity Pilots at the EU Commission stand at International Cybersecurity Forum FIC2021, 7-9 September 2021 | Booth |
| 19-07-2021 | CONCORDIA in CODE's Annual report 2020 | Annual Report |
| 22-06-2021 | Gabi Dreo Rodosek in 36th International Conference on ICT Systems Security and Privacy Protection – IFIP SEC 2021, 22–24 June 2021 | Conference |
| 14-06-2021 | Meet the CXO with Gabi Dreo,Folge 10 – Thomas Tschersich und Gabi Dreo Rodosek | Podcast |
| 03-06-2021 | Three more things you need to know about the Responsible Internet, University of Twente and University of Amsterdam | Blog |
| 18-05-2021 | H2020 Concordia : un réseau européen de cybercompétences | Interview |
| 01-04-2021 | CONCORDIA in an article of AG Connect, IT magazine in the Netherlands | Article |
| 23-02-2021 | Interview on cybersecurity | TV news |
| 18-02-2021 | Interview on cybersecurity | TV news |
| 12-02-2021 | News feed on the Faculty's homepage University of Maribor | News item |
| 11-02-2021 | Interview regarding International Day of Women and Girls in Science | TV news |
| 04-02-2021 | Assist. Prof. Dr. Lili Nemec Zlatolas on local TV, interview | TV news |

**Cooperation activities:**

The project and its activities gained publicity also thanks to the support of other entities during the third year of the project. Within social media, there is regular cooperation of entities dealing with cybersecurity in Europe (especially ENISA, ECSO, Sparta, ECHO, CyberSec4Europe, C4IioT and SPIDER H2020). CONCORDIA also supports the communication activities of these entities.

It is essential to emphasize our cooperation with the EC communication team. In addition to supporting social media and coordinating communication activities within the Cyber Competence communication group, it is a particularly important to mention our contributions to the Cybersecurity and Digital Privacy newsletter. The EC newsletter has a large audience which is very relevant for CONCORDIA. We send inputs for this newsletter regularly.

CONCORDIA also regularly cooperates with Cyberwatching platform – a European observatory of research and innovation in the field of cybersecurity and privacy. The two projects cooperate on social media level by promoting each other and CONCORDIA has also its profile on the platform and use it to promote project activities – https://cyberwatching.eu/projects/1484/concordia.

CONCORDIA also applied to the Horizon Booster – Horizon Results Booster (https://www.horizonresultsbooster.eu), a new package of 49 organized services with a goal to maximise the impact of R&I public investment and further amplify the added value of H2020 projects. CONCORDIA is currently engaged in the module A of Portfolio Dissemination & Exploitation Strategy. The module is focused on identifying and creating the portfolio of R&I project results.

Finally, CONCORDIA also cooperated with the EC Innovation Radar (https://www.innoradar.eu/methodology). Two of CONCORDIA innovations were designated as a high potential innovation. The DdoS Clearing House and the KYPO Cyber Range Platform were included into the radar. In addition, the later was then nominated into the Innovation Radar Prize 2021. The KYPO Cyber Range platform then won in Disruptive Tech category.

**Announcements:**

This section summarizes CONCORDIA announcements (website news items, press releases etc.) that we have published since the last review.

Table 14: CONCORDIA announcements

| Topic | Link |
|---|---|
| CONCORDIA – Strategic EU Cybersecurity Competence Network Project Based in Munich | https://www.concordia-h2020.eu/news/concordia-strategic-eu-cybersecurity-competence-network-project-based-in-munich/ |
| Becoming Cybersecurity Consultant | https://www.concordia-h2020.eu/news/becoming-cybersecurity-consultant/ |
| Cybersecurity in High-school – a Survey | https://www.concordia-h2020.eu/news/cybersecurity-in-high-school-a-survey/ |
| #4 Stakeholders' Newsletter | https://www.concordia-h2020.eu/news/3-stakeholders-newletter/ |
| Vacancy: Coordinating Research Engineer trusted future internet infrastructures at SIDN Labs | https://www.concordia-h2020.eu/news/vacancy-coordinating-research-engineer-trusted-future-internet-infrastructures-at-sidn-labs/ |
| Cybersecurity in high-school survey from CONCORDIA available now in 7 languages! | https://www.concordia-h2020.eu/news/cybersecurity-in-high-school-survey-from-concordia-available-now-in-7-languages/ |

| | |
|---|---|
| Virtual opening of the Twente University Centre for Cybersecurity Research | https://www.concordia-h2020.eu/news/virtual-opening-of-the-twente-university-centre-for-cybersecurity-research/ |
| Become a part of the CONCORDIA Observer Stakeholders Group! | https://www.concordia-h2020.eu/news/become-a-part-of-the-concordia-observer-stakeholders-group/ |
| EUROSEC 2021 – 14th EUROPEAN WORKSHOP ON SYSTEMS SECURITY | https://www.concordia-h2020.eu/news/eurosec-2021-14th-european-workshop-on-systems-security/ |
| 1st Workshop on Secure and Reliable Communication and Navigation in the Aerospace Domain (SRCNAS 2021) | https://www.concordia-h2020.eu/news/1st-workshop-on-secure-and-reliable-communication-and-navigation-in-the-aerospace-domain-srcnas-2021/ |
| #1 PECT-UP Newsletter 2021 (Pan-European Cybersecurity Start-Up Community) | https://www.concordia-h2020.eu/news/4-pect-up-newsletter-2021-pan-european-cybersecurity-start-up-community/ |
| #4 Stakeholders' Newsletter | https://www.concordia-h2020.eu/news/4-stakeholders-newletter/ |
| HiPEAC Spring 21 | https://www.concordia-h2020.eu/news/hipeac-csw-spring-2021/ |
| KYPO Cyber Range Platform 101 | https://www.concordia-h2020.eu/news/kypo-cyber-range-platform-101-webinar/ |
| CONCORDIA WOMEN's AWARDS | https://www.concordia-h2020.eu/news/concordia-womens-awards/ |
| PRESS RELEASE: DdoS Clearing House designated high potential innovation by European Commission | https://www.concordia-h2020.eu/news/press-release-ddos-clearing-house-designated-high-potential-innovation-by-european-commission/ |
| Annual Conference CODE 2021: Supply Chain Sovereignty: Reality or Illusion? | https://www.concordia-h2020.eu/news/annual-conference-code-2021-supply-chain-sovereignty-reality-or-illusion/ |
| New release of KYPO Cyber Range Platform brings support for Windows machines | https://www.concordia-h2020.eu/news/new-release-of-kypo-crp-brings-support-for-windows-machines/ |
| CONCORDIA Open Door Event 2021 is an opportunity! Are you keen to exploit it? | https://www.concordia-h2020.eu/news/concordia-open-door-cod2021-save-the-date/ |
| The pilot Course "Becoming a Cybersecurity Consultant" just closed – What's next? | https://www.concordia-h2020.eu/news/the-pilot-course-becoming-a-cybersecurity-consultant-just-closed-whats-next/ |
| CALL FOR APPLICATIONS ERCIM STM WG 2021 Award for the Best Ph.D. Thesis on Security and Trust Management | https://www.concordia-h2020.eu/news/call-for-applications-ercim-stm-wg-2021-award-for-the-best-ph-d-thesis-on-security-and-trust-management/ |
| Diversity & Cybersecurity: Women in Research | https://www.concordia-h2020.eu/news/diversity-cybersecurity-women-in-research/ |
| CONCORDIA WOMEN's AWARDS | https://www.concordia-h2020.eu/news/concordia-womens-awards-2/ |
| CONCORDIA map 2.0<br>Courses for cybersecurity professionals new look, new fields, new content | https://www.concordia-h2020.eu/news/concordia-map-2-0/ |
| Research category winners in CONCORDIA WOMEN's AWARDS | https://www.concordia-h2020.eu/news/research-category-winners-in-concordia-womens-awards/ |
| CONCORDIA Open Door 2021 | https://www.concordia-h2020.eu/news/concordia-open-door-2021/ |
| CyberHOT Summer School | https://www.concordia-h2020.eu/news/cyberhot-summer-school/ |
| The Future of Cybersecurity in Slovenia and Europe | https://www.concordia-h2020.eu/news/the-future-of-cybersecurity-in-slovenia-and-europe/ |
| Press Release: KYPO Cyber Range Platform is the European Commission's Innovation Radar Prize Winner | https://www.concordia-h2020.eu/news/press-release-kypo-cyber-range-platform-is-the-european-commissions-innovation-radar-prize-winner/ |

### 3.3.7. CCN communication activities

CONCORDIA participated in coordinated activities of the CCN communication group (consists of CONCORDIA, ECHO, SPARTA and CyberSec4Europe). That means in particular realization of CCN communication plan which includes usage of shared social media, websites and events. We also collaborated with Directorate-General for Communications Networks, Content and Technology (DG CNECT) on the monthly newsletters. We met regularly (at least once a month) during whole year.

More specifically, CONCORDIA contributed to the CCN communication activities by assuming the leadership of the group for the first six months of 2021. CONCORDIA communication team focused on the implementation of the CCN communication plan. The team initiated and led the campaign about CCN Education focus group outputs (Figure 16). The campaign promoted the results via social media and the CCN website, and it was 51 organized with the cooperation of ENISA. Another coordinated activity was the update of the joint presentation about the four pilots. Finally, in collaboration with ECHO, we coordinated the participation of four pilots at the International Cybersecurity Forum (FIC) 2021 event. Representatives of the four pilots were part of the EC DG-CNECT booth. CONCORDIA was represented by three project members who were available in the booth during the event. They used roll ups, flyers and presentations focused on CONCORDIA and CCN.
EC DG-CNECT considered the event successful.

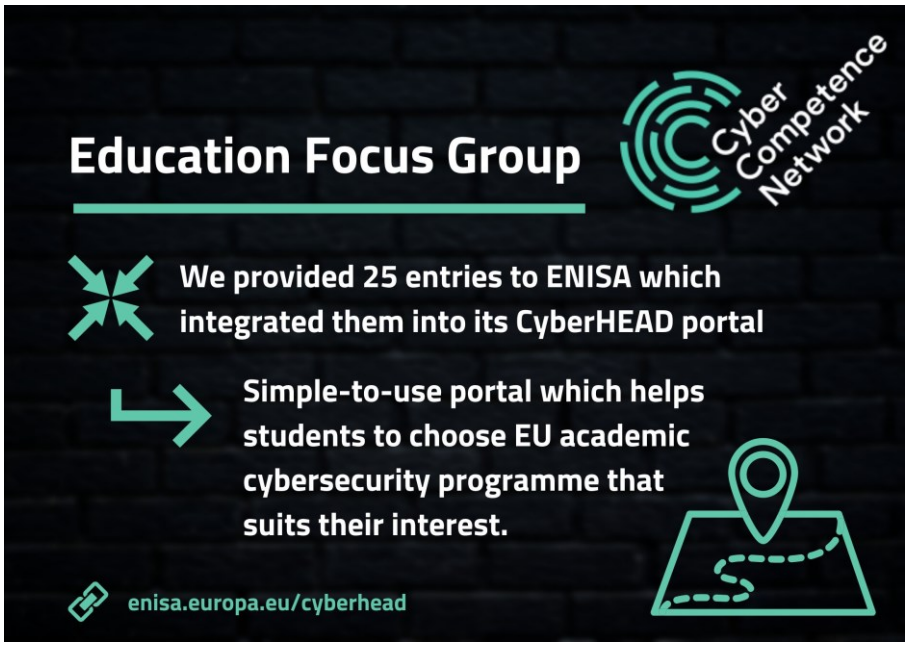



Figure 16 Visual example from CCN Education focus group campaign

### 3.3.8. Visual identity

CONCORDIA significantly refreshed visual communication via social media and other channels during the third year of the project. This was in relation to the negotiation about the logo usage – the CONCORDIA team managed to obtain consent with the single-color usage of our logo. Thanks to this it was possible to create many ‘new visual

implementations. The goal is to vary the visual forms in order to still catch the attention of our target audiences. Currently, basically every campaign has its unique visual form.

We also created many new visual outputs in order to support CONCORDIA activities during the third year of the project. Usually we prepare pictures, headers, apply our logo, icons, etc. – these are small, but necessary applications. Specifically, we would like to mention the creation of visuals for “Becoming Cybersecurity Consultant” course which simplified the communications about the course and its content.

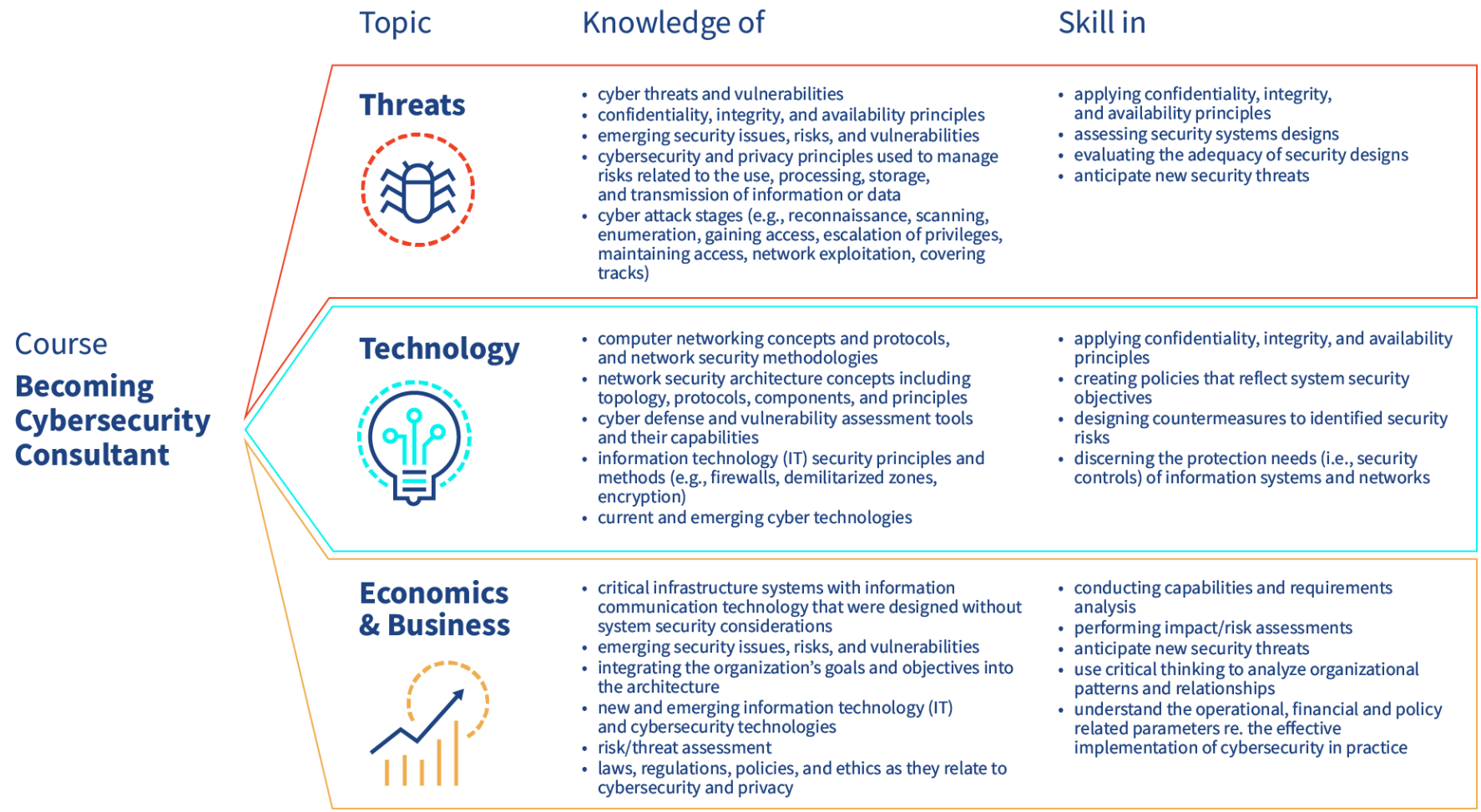



Figure 17: Example of Becoming Cybersecurity Consultant visual

### 3.3.9. Offline activities

Offline activities are influenced by COVID-19 situation since usage of printed materials is usually connected with the events participation. CONCORDIA communication team prepared the flyers and banner for the FIC 2021 event. Also, most of our infographics are prepared in the PDF form for possible printing.

### 3.3.10. Internal communication

Communication group was also focused on internal communication during the third year of the project. We regularly shared any important news with the consortium and we also maintain dedicated website in Confluence in order to provide centralized source information about our communication activities. We also provided instructions to make our communication consistent. We also updated a manual for preparing CONCORDIA blog posts. Internal communication activities are also performed in cooperation with task 6.1 (more information is available in deliverable D6.6 3rd year management report).

### 3.3.11. Dissemination and communication activities performed by other tasks

It is important to highlight those activities which were reported in previous paragraphs are not the only communication and dissemination activities performed by the CONCORDIA project. Communication group (T5.2) leads the communication and dissemination and it is responsible for its coordination and planning. The below table (Table **15**) provides an overview of the dissemination and communication activities of other project tasks that are directly involved in communication activities.

Table 15: Dissemination and communication in consortium

| Task | Activity |
|---|---|
| WP1 tasks | Produce scientific papers and deal with dissemination to the scientific community. More information is available in Work Package 1 in Deliverable D1.3. |
| T3.5 | Deals with communication activities targeted to start-ups. It creates a community mailing list, produces its own newsletter. |
| T4.5 | Focuses on communication activities related to workforce diversity. It produces various types of content, including webinars. Communication group closely cooperates with the task 4.5. More information is available in Deliverable D4.6. |
| T4.6 | Deals with communication activities targeted to CONCORDIA stakeholders. Among other things, it creates a community mailing list, produces his own newsletter and organizes the CONCORDIA Open Door Event. More information is available in Deliverable D4.9. |
| T6.1 | Deals with governance of the project which is connected with the internal communication activities. More information is available in Deliverable D6.6. |

## 3.4. Impact from Covid-19 pandemic crisis

The pandemic has a long-term effect on the dissemination and communication of the CONCORDIA project.

Firstly, the pandemic affected or even interrupted the work of several CONCORDIA teams, either academic or industrial, and reduced or even stopped their technical progress. The technical and scientific achievements of the project are essential inputs for the communication group (see Table 6 – CONCORDIA content). On the other hand, a sufficient number of CONCORDIA assets were produced and were used for dissemination and communication activities. To sum the first point up, pandemic influenced the selection of topics. However, CONCORDIA was still able to implement its communication and dissemination plan for this year.

Secondly, the pandemic still influences the usage of our communication tactics. The opportunities to attend events have been significantly reduced during this year. This also has a negative impact on CONCORDIA's publicity outputs because there is lower number of opportunities to promote the project. Especially, face to face networking that is a natural part of every physical event is missed in the COVID-19 era.

The reduced number of events also means that there was almost no demand for offline communication materials (except the FIC 2021 event). The CONCORDIA communication group focused more on digital activities. We had to move the CONCORDIA Open Door event to digital again (more information can be found in the deliverable D4.9).

Finally, the pandemic situation is still an opportunity for discussing the importance of cybersecurity. In Year 3, we have supported communication activities performed by ENISA and the European Commission, that deal with pandemics and cybersecurity. In addition, we also produced several blog posts (see the Table **7**) which were focused on this topic.

## 3.5. Next Steps on Dissemination and Communication

CONCORDIA communication and dissemination activities during the project are divided into five distinctive phases (see the Table **4**). We will start with the Closing phase in 2021. During this phase, we will still perform regular communication and dissemination activities. In addition, we will start with the activities specific to this phase. This particularly means providing a summarization of our results and focusing on what was delivered in the project. We plan to realize a long-term campaign that is currently called #CONCORDIADelivers.

Another important campaign will be focused on the CONCORDIA Roadmap which is one of the most important results of the project.

We would also like to continue in our cooperation with the Horizon Results Booster as was described in the Publicity section of this document (Publicity). Especially we plan to engage in media relations with the formed group. Another important activity for the next year is the use of paid advertising on Twitter. The permission to use this tool was granted by EC. We will use it to support our most important posts on Twitter. We will also regularly evaluate their success and optimize the advertising.

We also plan to strongly cooperate with the EC communication team, the CCN pilots, and other cybersecurity initiatives.

# 4. Efforts on Certification & Standardization

## 4.1. Objectives of Task (T5.3)

This task focuses on the certification and standardization activities of the project. The objective of the task is to ensure alignment with the technologies to be developed (WP1), as well as the pilots (WP2). To this end, the project monitors continuously the evolving certification, standardization and best practices landscape, in order to timely identify other initiatives that may be linked to the CONCORDIA areas of interest. It will also develop the initial engagements/liaisons with the respective governing organizations and will actively engage with external stakeholders aiming at promoting the achievements resulting from the technical WPs in the appropriate fora.

## 4.2. Strategy to achieve Task Objectives

CONCORDIA is a project where different organizations come together to:

- Devise a cybersecurity roadmap to identify powerful research paradigms, to do hands-on experimental validation, prototype and solution development in an agile way to quickly identify successful but also unsuccessful potential product development.
- Develop next-generation cybersecurity solutions by taking a holistic end-to-end data-driven approach from data acquisition, data transport and data usage, and addressing device-centric, network-centric, software- and system-centric, data- and application-centric and user-centric security.
- Develop sector-specific (vertical) and cross-sector (horizontal) industrial pilots with building incubators.

Also, in terms of focus areas, the CONCORDIA project deals with a variety of subjects related to security in devices, network, software, data and users covering various sectors (Telecom, Finance, Transport, E-Health, Aerospace) and services.

Certification is not a one–fits–all practice. For each of the objectives and focus areas, the need for certification must be identified and individually addressed. Moreover, to find the way that Certification fits the needs of the task and solution, the outcomes of this task and solution should have reached a certain level of maturity (such that a certification scheme could have a positive value and recognition to the interested parties).

In order to achieve all the above, the following strategy was devised:

- Map the standardization needs (explained in further details in Section 4.3.2 on Standardization)
- Identify the certification needs per task
- Design and implement the certification activities per task
- Collaborate internally and externally to promote the certification task results to stakeholders.

In Section 4.2.1**Fehler! Verweisquelle konnte nicht gefunden werden.**, the actions performed regarding the Certification activities are described, in Section 4.2.2, the actions performed regarding the Standardization activities are described, and in Sections 4.3.1 and Section 4.3.2 the results of these actions up to this point, respectively, are described.

Section 4.4 contains information regarding the effects of the COVID-19 pandemic crisis and of the imposed restriction had on the activities of the project. Finally, Section 4.5. contains information regarding the next steps that will be undertaken for the Certification and Standardization task of the project.

### 4.2.1. Certification

Certification is the third-party attestation related to products, processes, systems, persons or bodies. Whereas attestation, is issue of a statement, based on a decision following review, that fulfilment of specified requirements has been demonstrated.[16] Depending on the subject of certification, different international standards provide the related best practices (e.g., ISO 17021[17], ISO 17024[18], ISO 17025[19], etc.).

**Identification of the certification needs per task**

As mentioned in the beginning of Section 4.2, the CONCORDIA project addresses a variety of topics and industry sectors. In order to identify the certification needs, an individual approach had to be adopted. This approach consists of the following four activities:

- Individual discussions with different task leaders, in order to identify the certification potential.
- The project team reviews all related deliverables expected to be finished by the end of the year.
- Discussions with relevant stakeholders (either within the relevant Observer Group or outside).
- Participation in Cybersecurity Certification Events and Conferences.

From the combination of the collected information from the activities mentioned above, ideas and areas (related to certification) were identified and put forward for discussion with the relevant WP / Task Leaders and Partners of the project.

More information regarding the activities and results of these efforts can be found in Section 4.3.

### 4.2.2. Standardization

Before introducing the subject of standardization, it is deemed necessary to provide two simple definitions regarding the terms *Standard* and *Standards Developing Organizations* (SDO) in the context of the CONCORDIA project:

- **Standard:** "A standard (French: Norme, German: Norm) is a technical document designed to be used as a rule, guideline or definition. It is a consensus-built, repeatable way of doing something."[20]

[16] ISO/IEC 17000:2004(en) Conformity assessment — Vocabulary and general principles.
[17] ISO/IEC 17021-1:2015. Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements. https://www.iso.org/standard/61651.html
[18] ISO/IEC 17024:2012. Conformity assessment — General requirements for bodies operating certification of persons. https://www.iso.org/standard/52993.html
[19] ISO/IEC 17025:2017. General requirements for the competence of testing and calibration laboratories. https://www.iso.org/standard/66912.html
[20] CEN, the European Committee for Standardization, is an association that brings together the National Standardization Bodies of 34 European countries, retrieved from the official website

- **SDO:** "An SDO is an organization that facilitates the development of standards and publication of standards. SDOs include: National Association of Standardization and Certification (ANCE), ASTM International (ASTM), International Society of Automation (ISA), National Fire Protection Association (NFPA), Underwriters Laboratories (UL), ULC Standards" and various others [21].

Considering the above definitions, for the CONCORDIA project, some of the types of documents referred to as Standards are [22]:

- **International Standards:** An International Standard provides rules, guidelines or characteristics for activities or for their results, aimed at achieving the optimum degree of order in a given context. It can take many forms. Apart from product standards, other examples include test methods, codes of practice, guideline standards and management systems standards. In the results of the Standardization subtask described below, such standards are identified from various Standards Development Organizations like International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), Institute of Electrical and Electronics Engineers (IEEE) and others.
- **Standards:** Documents issued by Standards Development Organizations following their individual procedures. In the results of the Standardization subtask described below, such standards are identified from Standards Development Organizations like Underwriters Laboratories (UL), Society of Automobile Engineers (SAE), ASTM International (ASTM), National Aeronautics and Space Administration (NASA) and others.
- **Technical Specifications:** A Technical Specification addresses work still under technical development, or where it is believed that there will be a future, but not immediate, possibility of agreement on an International Standard. A Technical Specification is published for immediate use, but it also provides a means to obtain feedback. The aim is that it will eventually be transformed and republished as an International Standard. In the results of the Standardization subtask described below, such specifications are identified from Standards Development Organizations like ISO and IEC.
- **Technical Reports:** A Technical Report contains information of a different kind from that of the previous publications. It may include data obtained from a survey, for example, or from an informative report, or information of the perceived "state of the art". In the results of the Standardization subtask described below, such reports are identified from Standards Development Organizations like ISO, IEC and American National Standards Institute (ANSI).
- **Guides:** Guides give rules, orientation, advice or recommendations relating to international standardization and conformity assessment. [23] In the results of the Standardization subtask described below, such guides are identified from Standards Development Organizations like IEC and the International Association of Drilling Contractors.
- **Special Publications:** A type of publication issued by National Institute of Standards and Technology (NIST). Specifically, the SP 800-series reports on the Information Technology Laboratory's research, guidelines, and outreach efforts in

[21] https://ulstandards.ul.com/about/glossary/

[22] CEN, the European Committee for Standardization, is an association that brings together the National Standardization Bodies of 34 European countries, retrieved from the official website

[23] Information retrieved from the website of IEC: https://www.iec.ch/standardsdev/publications/guide.htm

computer security, and its collaborative activities with industry, government, and academic organizations. [24]

- **Recommendations:** The International Telecommunication Union (ITU) - Radiocommunication Sector (ITU-R) Recommendations constitute a set of international technical standards developed by the Radiocommunication Sector (formerly CCIR) of the ITU. They are the result of studies undertaken by Radiocommunication Study Groups on various subjects. The ITU-R Recommendations are approved by ITU Member States. Their implementation is not mandatory; however, as they are developed by experts from administrations, operators, the industry and other organizations dealing with radiocommunication matters from all over the world, they enjoy a high reputation and are implemented worldwide. [25]

**Data Collection:**

The effort regarding the collection of data on standardization efforts relevant to the CONCORDIA project has started from the first year of the project and is still in progress. Specifically, as described in the 1st year report on exploitation, dissemination, certification and standardization, a survey was conducted involving all partners in order to collect the following information, per Work Package, per Task and per Partner:

- The key topics that each partner will be involved in during their participation in the project, per Task.
- The standards each Partner is already using for the performance of each Task.
- The standards each Partner is planning on using for the performance of each Task.
- The standardization activities that each Task member is part of.

This year, and since the activities of the project have matured and several channels of communication have been created and are being maintained by the project partners, an additional approach was added.

Specifically:

- Each partner was asked to identify whether some of their outputs and activities could contribute to standardization efforts under development, or where likely candidates to be included in such efforts.
- Specific standardization efforts were highlighted and input was requested by the project partners.

The results related to standardization related activities are included in Section 4.3.2.

## 4.3. Results on Certification and Standardization

### 4.3.1. Certification

#### 4.3.1.1. Certification of Cybersecurity Skills under Task 3.4

One of the aims of Task T3.4 is to "provide a certification framework for professional courses; going beyond professionals and industry to address the wider society by engaging new generations and "teaching the teacher". To facilitate the above goals, the need arose for the development of a framework in the context of Cybersecurity to ease the process of

[24] NIST SP 800-63-3 under Special Publication (SP)

[25] Information retrieved from the website of ITU: https://www.itu.int/pub/R-REC

delivering, obtaining, securing and verifying of certificates for well-defined Cybersecurity skills.
As part of a pilot operation of the Cybersecurity Skills Certification Framework, a Certification Scheme for Cybersecurity Skills was designed and implemented over the first three years of the project.
The overall activities that are implemented within this context are depicted below:

- **Create a Feasibility study**: The purpose of this study is to describe the need that the Certification Scheme is going to fill, to identify existing efforts and to define the exact profile of the proposed certification. The document contains an analysis of the market situation, of the available skills frameworks and concludes with the identification of possible gaps in Cybersecurity Skills Certification Schemes. The document of the feasibility study has been published in the CONCORDIA website: https://www.concordia-h2020.eu/wp-content/uploads/2020/06/CONCORDIA-SkillsFeasibilityStudy-forpublication.pdf. (Completed during the previous years.)
- **Select a Cybersecurity Skills Certification Scheme for implementation**: The feasibility study mentioned above revealed gaps in Cybersecurity Skills Certification Schemes. Moreover, the project team conducted an online survey, to retrieve the opinion of the CONCORDIA partners regarding their implementation preference. The results of these two actions led the project team to select the role of the Cybersecurity Consultant. The Role Profile of the Cybersecurity Consultant had not been formulated before. To create the role profile, an analysis of existing guidance and a specialized workshop was conducted (https://www.concordia-h2020.eu/news/participate-in-the-definition-of-the-european-cybersecurity-consultant-profile/). The combined results of these actions produced a document called "Cybersecurity Consultant Role Profile" which is currently in its final stages of implementation. (Completed during the previous years.)
- **Create a Certification Framework**: The purpose of the Certification Framework is to define the rules under which the Certification Scheme will operate. The Certification Framework contains the best practices regarding certification in the area of Cybersecurity based on the knowledge and experience of the CONCORDIA partners. The final version of the Certification Framework will be issued after the evaluation of the results of the pilot certification scheme (Cybersecurity Consultant). (In process - currently in process of being finalized).
- **Create Supporting material for the implementation of the Scheme**: A certification scheme for skills, based on the international best practices of ISO 17024, comprises of the following documents: The certification scheme, the examination databank, a declaration of honour for the certified professionals and various templates of required documents e.g., certificate, etc. At the point that this report is being drafted, the certification scheme, the exam databank for the theoretical exam, the activities for the practical exam, the templates for the grading and the certification have been completed. The Certification Scheme for the $C^3$ by CONCORDIA can be found at https://www.concordia-h2020.eu/wp-content/uploads/2021/11/Concordia_Certification_SchemeC3_v1.pdf. Since the databank is used actively to support the Certification Scheme no screenshot or other evidence of existence is included in this deliverable. (Completed within Year 3 of the project).
- **Piloting the Certification scheme**: The scheme was piloted twice within 2021. The objectives of the pilots were to validate the scheme, the operational methods, perform a quality evaluation of the databank, establish the appropriateness of the tools used for the assessment, identify opportunities for improvement and shortcomings. The fist pilot was

implemented during May and June of 2021. This first pilot of the certification scheme was carried out after the completion of the relevant training course (https://www.concordia-h2020.eu/becoming-a-cybersecurity-consultant/). The results of the pilot are included in a Report, which is attached to this document as Annex B. While this report is being drafted the second pilot is being implemented. The objectives for piloting the certification scheme remain the same, with the addition that in this iteration, and in order to test the affinity and validity of the certification scheme and process, a limited number of professionals will be allowed to participate without having completed the relevant CONCORDIA Cybersecurity Consultant Course. Results regarding these activities will be reported in due course. (In process).

- **Issuing Certificates**: The Certification Scheme for the $C^3$ by CONCORDIA describes the principles and the method through which the relevant Certificates will be issued. The contents of the Certificates are aligned with the minimum requirements as set by international standards (e.g., ISO 17024). For the $C^3$ by CONCORDIA Certificates it was decided to store the information of the certificate in the EduCTX[26] based on blockchain technology. EduCTX is a platform for managing students' micro-credentials (i.e., certificates), which is a solution already proven in pilot based-environment established among multiple academic institutions (e.g., University of Maribor, University of Applied Sciences Bielefeld, University of Sarajevo and soon Brno University of Technology). This system allows for the easy and reliable validation and storage of a given certificate. The responsible partner for this implementation in the context of the CONCORDIA project is the University of Maribor. (In process).
- **Improvement:** After each pilot, a quality review is implemented by the relevant committee described in the Certification Scheme, taking into consideration the results of the participant, the feedback of the organizing partners during the implementation of the pilot and the feedback of the participants during the various phases. (More information is included in the Report of the 1st pilot of the certification scheme included on Annex B of this document). From this review opportunities for improvement and corrective actions are identified and implemented. At the end of the pilots, the collected information will be used for the improvement and finalization of the Cybersecurity Skills Certification Framework. (In process).

#### 4.3.1.2. Cross-pilot activities in the Area of Certification

The following activities have been carried out in collaboration with other pilots:

**Activity 1: Certification of Cybersecurity MOOCs**

As a result of the CCN group in education, collaboration potential was identified in the field of certification in education. Specifically, after the initial exploratory discussions within the activities of the Cyber Competence network Group for Education, a cooperation potential was identified between two pilots: CONCORDIA and CyberSec4Europe. CyberSec4Europe has created a list of quality assurance criteria for MOOCs with an emphasis on Cybersecurity whereas CONCORDIA has already implemented a certification scheme for Cybersecurity Skills and has created a draft Cybersecurity Certification

[26] https://eductx.org/

Framework. Taking these into consideration, the two projects have decided to collaborate in order to implement the following actions:

- Action 1: Conduct Survey on refined requirements for a Certification Scheme for the MOOC and Cyber ranges needed in Education and Training
- Action 2: Based on the results of the surveys, decisions regarding the implementation of a joined scheme certification will be taken.
- Action 3: Design and implement advanced Certification Scheme (if practicable).

The above-mentioned activities have yielded the following results:

- A survey was designed to collect responses regarding the value of a possible certification scheme for Cybersecurity MOOCs and the relevant criteria that could be included. The survey was launched at the beginning of 2021 and collected responses until the end of May 2021.
- The provided responses were analysed and initial results and conclusions were drawn.
- The results and preliminary conclusions were presented in a joint presentation and subsequent publication in the 6th IEEE European Symposium on Security and Privacy, Cybersecurity Certification Workshop[27].
- The next steps of the cooperation include individual interviews with volunteers to clarify some of the issues discovered during the analysis of the responses and then the formulation of an initial certification scheme.

Conclusions drawn, from the survey, to the point that this deliverable is being drafted:

Based on the responses of the participants, it is derived that the majority of the MOOC stakeholders (both educators and non-educators) value a MOOC certificate showing that a MOOC was independently reviewed and fulfils specific acknowledged criteria, and agreed using it as a factor for selecting a MOOC.

The majority of the respondents agree that they have experienced a variety of challenges when using a MOOC including privacy, accessibility and openness issues as well as problems with the qualifications and competence of the instructors, the definition of learning objectives, and others.

Within the survey a number of quality criteria were proposed, as possible inclusions to such a certification scheme, and the respondents (educators and non-educators) generally agreed that the proposed criteria were suitable and desirable for such a scheme.

The next steps to be implemented include interviews and further analysis in order to select and weight the final set of criteria against the best practices and decide on the final set.

[27] M. Beckerle, A. Chatzopoulou and S. Fischer-Hübner, "Towards Cybersecurity MOOC Certification," 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2021, pp. 1-11, doi: 10.1109/EuroSPW54576.2021.00008.

Annex C of this document contains more information and extracts regarding the relevant effort.

### Activity 2: 6th IEEE European Symposium on Security and Privacy, Cybersecurity Certification Workshop

The 6th IEEE European Symposium on Security and Privacy, Cybersecurity Certification Workshop[28] was co-organised by the following four H2020 pilot projects SPARTA, CyberSec4Europe, CONCORDIA and ECHO for establishing a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap.

Two members of the CONCORDIA project participated in the Program committee and actively assisted in the review of the submitted papers.

Program chairs: Philippe Massonet (CETIC, Belgium), Tobias Fiebig (TU Delft, Netherlands).

| Name | Organisation |
|---|---|
| Thibaud Antignac | CEA, France |
| Volkmar Lotz | SAP, France |
| Artsiom Yautsiukhin | CNR, Italy |
| Nicolò Maunero | CINI/Politecnico di Torino, Italy |
| Kai Rannenberg | Chair of Mobile Business & Multilateral Security, Goethe University Frankfurt, Germany |
| Chatzopoulou Argyro | TÜV TRUST IT GmbH, TÜV Austria Group, Germany |
| Liina Kamm | Cybernetica AS, Estonia |
| Vashek Matyas | Masaryk University, Czechia |
| Douglas Wiemer | Rhea Group, Belgium |
| Barbara Carminati | University of Insubria, Italy |

Figure 18. Members of the program committee. Blue boxes mark the CONCORDIA partners

### Activity 3: CONCORDIA Open Door Event – 2021, Cybersecurity Product Certification Panel

During the CONCORDIA Open Door Event – 2021[29], a panel discussion was provided on the subject of Cybersecurity Product Certification.

The panel was coordinated by Chatzopoulou Argyro, TÜV TRUST IT GmbH and the panellists contributed with their knowledge and experience in the identification of the current status, the challenges and the next steps regarding Cybersecurity Product Certification.

One of the members of the panel was Mr. Philippe Massonet, Scientific Coordinator, Business Research Alignment of CETIC, leading the Certification activities of the SPARTA Project.

[28] https://www.cetic.be/cybercert2021
[29] https://opendoor.concordia-h2020.eu/2021/

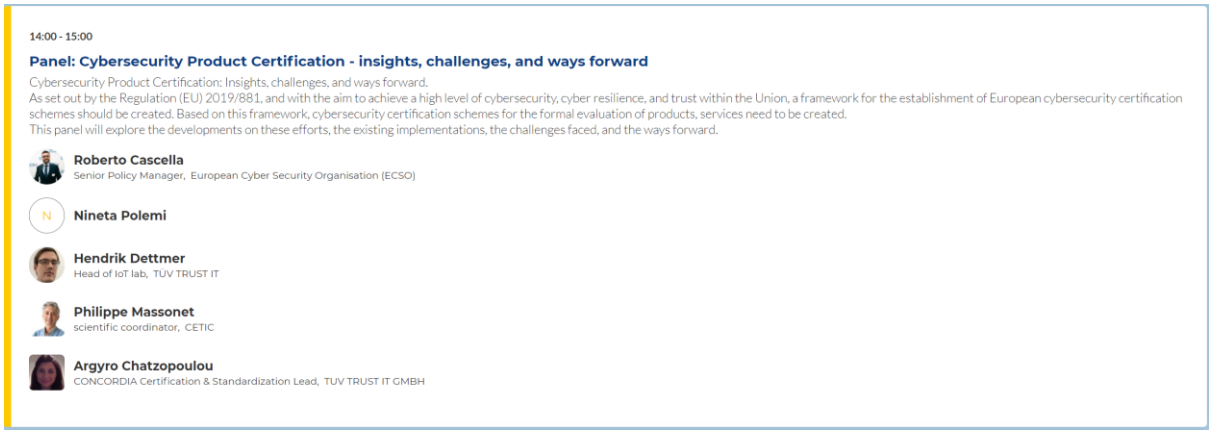



Figure 19: Screen shot of the panel on Cybersecurity Product Certification of COD 2021[30]

The key points and take-aways from the panel discussion, are included in Deliverable D4.9 3rd year report on Liaison with Stakeholders.

**Activity 4: The REWIRE project**

The Cybersecurity Skills Alliance – New Vision for Europe – REWIRE[31] project develops a Blueprint for the Cybersecurity industry and a concrete European Cybersecurity Skills Strategy. It brings together 25 partners from academia and VET, cybersecurity industry, non-cyber industries, certification partners and umbrella organizations. Its work builds upon four pilot projects: CONCORDIA, SPARTA, ECHO, CyberSec4Europe implemented with the support of the European Union's Horizon 2020 research and innovation programme.

The project includes areas related to certification of skills and will built upon the results of all projects.

Specifically, WP4 Blueprint Toolbox – Tools directly connected to education, training and certification includes the creation of a Cybersecurity Skills Certification Scheme Core, relevant qualification standards and for a sample of Roles, it will provide the piloting of the Schemes and Standards. Finally, the project will provide a Cybersecurity Skills Assessment Recommendation (in relation to the theoretical and practical assessment of cybersecurity skills within a certification activity)[32].

### 4.3.1.3. CONCORDIA's Cybersecurity Roadmap for Europe

The activities of Task 4.4 include the realization of the "Cybersecurity Roadmap for Europe by CONCORDIA". The document was originally presented in its first draft form in 2020. It was agreed that the document will be updated annually based on the current state of play. The final version will be delivered in month 48. More information regarding the roadmap can be found in 2021's version of D4.4.Y3 deliverable.

[30] https://cod2021.w.tame.events/

[31] REWIRE is co-funded by the ERASMUS+ programme of the European Union (Agreement Number – 621701-EPP-1-2020-1-LT-EPPKA2-SSA-B) for a duration of four years (01.11.2020 to 31.10.2024).

[32] More information can be found at: https://rewireproject.eu/

The roadmap amongst others, identifies six holistic dimensions of observation, namely (i) Research and Innovation, (ii) Education and Skills, (iii) Legal and Policy, (iv) Economics and Investments, (v) Certification and Standardization and (vi) Community Building.

Especially in the area of Certification, Chapter 8.2., within the year 2021, the roadmap has been updated based on the current information derived from:

- Discussions with relevant stakeholders
- Participation in events and conferences
- Review of new publications
- Discussions within the project team.

The relevant chapter of the Roadmap includes:

- An introduction to certification
- A description of challenges faced by Certification
- Short term aims
- Mid term aims
- Long term aims.

Since the information included in the previous version of the document was gathered until November 2020, the update to the relevant entries was important since a series of developments transpired within 2021.Some of the relevant events and publications are shown in the following list.[33] :

- ENISA has initiated the following ad-hoc Working Groups: Ad-Hoc Working Group on Awareness Raising; Ad Hoc Working Group on EU Cybersecurity Market; Ad-Hoc Working Group on Security Operation Centres (SOCs); Ad-Hoc Working Group on Enterprise Security; Ad-Hoc Working Group on Cyber Threat Landscapes; Ad-Hoc Working Group on Artificial Intelligence Cybersecurity
- On Jan 11th, 2021 ENISA, the European Agency for Cybersecurity, held a webinar presentation of the draft EUCS scheme[34].
- The draft version of the EUCS candidate scheme (European Cybersecurity Certification Scheme for Cloud Services), which looks into the certification of the cybersecurity of cloud services, was issued on December 22, 2020
- The ENISA Cybersecurity Certification Conference 2020[35] was held on December 18, 2020
- Publication of a study which proposes a set of initial methodological steps to work towards a market analysis on cybersecurity certification of ICT products, ICT services and ICT processes. The performance of a market analysis on cybersecurity certification aims to contribute to the EU cybersecurity certification framework and the planning activities of the European Commission, the ECCG and the SCCG by identifying future areas for cybersecurity certification. The study was published on April 09th , 2021 under the title Cybersecurity Certification Market Study
- Version -V.1.1.1- of EUCC scheme has been updated based on the comments received through the public consultation and from the ECCG, May 25, 2021
- A report has been published that presents the outcome of the public consultation on the first draft of the cybersecurity certification candidate EUCC scheme. May 26, 2021

[33] https://www.enisa.europa.eu/news
[34] https://www.enisa.europa.eu/events/webinar-certification-of-cloud-services-in-europe
[35] https://www.enisa.europa.eu/events/ENISA-CCC/enisa-ccc

- Following a request by the European Commission, ENISA will proceed with the preparation of the new candidate cybersecurity certification scheme on 5G. This step follows on from the EU toolbox for 5G security and it is expected to further enhance the cybersecurity of 5G networks as it contributes to addressing certain risks, as part of a broader risk mitigation strategy. February 03, 2021

Also, developments have taken place also in the area of Standardization (which is closely linked to Certification) which also helped in shaping the information contained in the Roadmap. (More information on the inputs to standardization can be found in Section 4.3.2.).

#### 4.3.1.4. Designing new certification related activities

During this year, in an attempt to discover certification related areas of contribution of the CONCORDIA project, the project team discussed with relevant stakeholders, held individual discussions with the members of the relevant Observers Group[36], liaised with other related projects and discussed with partners on their work.

The above resulted in the following:

- The project decided not to create another Certification Scheme, since the relevant processes (especially for products and services) are currently in progress by ENISA.
- Instead, the project decided to work in the direction of the Cybersecurity Certification Framework (an umbrella document that provides principles and processes regarding Cybersecurity Certification). To this effect the following activities are being undertaken
    - A collaboration has started with the following two European funded projects:
        - CYRENE project: [37]
          The CYRENE project focuses in certifying the security and supply chain of supply chain services. they have created a model scheme based on the EUCS and have planned for the execution of two pilots.
        - A4CEF project: [38]
          The A4CEF project focuses on the development of a comprehensive framework model for all stakeholders, interactions and flows that will facilitate businesses that are active in the area of ICT to certify their products globally with the aim of elevating trust, technology and security and by extension the national economies. A team within CONCORDIA is being formulated[39]. The team will undertake the following tasks:

[36] Due to the limited number of the members of the group, there was no official meeting of the Group within 2021. Individual discussions were held with the members in order to get their feedback on possible new actions.

[37] This project has received funding from the European Union's Horizon 2020 Research and Innovation program under grant agreement No 952690. (https://www.cyrene.eu/)

[38] This project has been designed to directly meet the relevant requirements for the deployment of the Digital Service Infrastructure (DSI) defined in section 3.9 of the 2019-2020 Connecting Europe Facility (CEF) Telecom Work Programme. "Support to cooperation and capacity building for cybersecurity certification in line with the Cybersecurity Act". https://www.a4cef.eu/about

[39] The call for volunteers is expected to end at the end of November 2021.

        - Propose on the formulation of a Cybersecurity Certification Framework (that will include skills, products, processes and services).
        - Provide feedback on work implemented to the above mentioned two projects.
        - Undertake other actions, as they may arise.
- New efforts related to certification are being investigated for implementation until the end of the project:
    - Collaboration with T.4.3 for a potential determination of viable aspects relevant for standardization and certification approaches/proposals, such as usage of the methodology and solutions as part of the "Cybersecurity Label"[40].
    - Collaboration with WP4 on the subject of the approach to continuous (dynamic) vs static certification.

### 4.3.2. Standardization

#### 4.3.2.1. Standardization efforts from within the project

As mentioned in the Section 4.2.2. the project team researched the different existing public and proprietary standards (in their various stages of development) and documented the results in the Sheet Index_Standards of the relevant file[41] that is available on the project's repository. The objective was to identify standards related to cybersecurity covering various different aspects and inform accordingly the partners of the CONCORDIA project. This activity was carried out in the beginning of the project (and the results were included in the previous yearly report) and was repeated this year (and the results are included within this report).

Number of identified:

- Standards Developing Organizations (SDOs): 36
- Standards: 565
- Standards in preparatory stages (Draft, Pending, etc.): 101

The identified standards during this preliminary research covered the area of cybersecurity from various aspects:

- Technical (e.g., Guidelines for Securing Wireless Local Area Networks (WLANs))
- Introductory (e.g., Ships and marine technology--Cyber safety)
- Sector Specific (e.g., Road Vehicles -- Cybersecurity engineering)
- Technology specific (e.g., Securing Manufacturing Industrial Control Systems: Behavioural Anomaly Detection NISTIR 8219), etc.

[40] https://www.cyberwatching.eu/news-events/news/new-cybersecurity-label-creating-clearer-path-better-cybersecurity-european-smes and the latest version of the label can be found at http://gtt.cyberwatching.eu/Pages/Home.aspx

[41] The file Information Re_Standards was firstly introduced during the first year of the project as a means to depict and collect information regarding standards and standardization efforts. The structure and content of the file was described in the 1st year report.

The inputs of the partners regarding Standardization as described above were consolidated, and one document was created.

Table 16 summarizes the contribution of the partners in various standardization efforts. The table includes the following fields:
**Partner**: The CONCORDIA partner participating in the identified standardization effort.
**SDO**: Standards Developing Organization under which the standardization activity is taking place.
**Title of committee or standard**: The title of the committee or the standard where the partner is involved. It could be a working group, a specific committee or a specific document.
**Type of participation**: There are different types of participation e.g..,. contributor, follower, editor, co-editor, convener, observer etc. The type of participation depends on the SDO and its relevant processes.

Table 16: Standardization efforts where CONCORDIA partners are participating

| Partner | SDO | Title of committee or standard | Type of participation |
|---|---|---|---|
| CAIXA | Cloud Security Alliance (CSA) | Financial Sector WG | Contributor |
| CAIXA | ENISA | ENISA's Financial experts Working Group | Member |
| CAIXA | European Savings and Retail Banking Group | ESBG Cloud Certification Working Group | Member |
| CAIXA | Financial Services Information Sharing and Analysis Center (FS-ISAC) | | Member |
| CAIXA | Payment Security Support Group and Card Fraud Prevention (EPC) | | Member |
| Industrial Systems Institute/Research Center ATHENA | Internet Engineering Task Force (IETF) | 6TISCH Working Group RFC draft Zero - Touch Secure Join Connect, 6TiSCH secure minimal architecture | Observer - Provide Possible implementation of the protocol |
| Jacobs University Bremen | IETF | TEEP | Following WG progress |
| Jacobs University Bremen | IETF | NETMOD - specification draft-ietf-netmod-rfc6991-bis | Editor |
| Jacobs University Bremen | IETF | RATS | contribution to WG discussions |

| Partner | SDO | Title of committee or standard | Type of participation |
|---|---|---|---|
| Jacobs University Bremen | IETF | SUIT | following WG progress |
| Jacobs University Bremen | IETF | NETCONF/YANG | contributing to WG documents |
| Jacobs University Bremen | IETF | TEEP | following WG progress |
| Jacobs University Bremen | IETF | RATS | contribution to WG discussions |
| Jacobs University Bremen | IETF | SUIT | following WG progress |
| Jacobs University Bremen | IETF | NETCONF /YANG various revisions (e.g. ipsecme-yang-iptfs, sfc-nsh-integrity, avtcore-multi-party-rtt-mix etc) | contributing to WG documents |
| Jozef Stefan Institute | IEEE | P2933 | Co-chair Clinical IoT |
| Jozef Stefan Institute | RISC-V International | Security Horizontal Committee (security) | Following the relevant activities |
| Jozef Stefan Institute | RISC-V International | Trusted Execution Environment Task Group (tech-tee) | Following the relevant activities |
| RISE Research Institutes of Sweden AB | IETF | RFC 7744 | Author |
| RISE Research Institutes of Sweden AB | IETF | CoRE WG - Object Security for Constrained RESTful Environments (OSCORE) | Author |
| RISE Research Institutes of Sweden AB | IETF | CoRE WG - Group OSCORE - Secure Group Communication for CoAP | Author |
| RISE Research Institutes of Sweden AB | IETF | CoRE WG - Group Communication for the Constrained Application Protocol (CoAP) | Author |

| Partner | SDO | Title of committee or standard | Type of participation |
|---|---|---|---|
| RISE Research Institutes of Sweden AB | IETF | CoRE WG - Discovery of OSCORE Groups with the CoRE Resource Directory | Author |
| RISE Research Institutes of Sweden AB | IETF | ACE WG - Key Provisioning for Group Communication using ACE | Author |
| RISE Research Institutes of Sweden AB | IETF | ACE WG - Key Management for OSCORE Groups in ACE | Author |
| RISE Research Institutes of Sweden AB | IETF | ACE WG - EST over secure COaP (EST-coaps) | Author |
| RISE Research Institutes of Sweden AB | IETF | ACE WG - Authentication and Authorization for Constrained Environments (ACE) using Oauth 2.0 Framework (ACE-OAuth) | Author |
| RISE Research Institutes of Sweden AB | IETF | ACE WG - Additional OAuth Parameters for Authorization in Constrained Environments (ACE) | Author |
| RISE Research Institutes of Sweden AB | IETF | ACE WG - OSCORE profile of the Authentication and Authorization for Constrained Environments Framework | Author |
| RISE Research Institutes of Sweden AB | IETF | ACE WG - Datagram Transport Layer Security(DTLS) Profile for Authentication and Authorization for Constrained Environments (ACE) | Author |

| Partner | SDO | Title of committee or standard | Type of participation |
|---|---|---|---|
| RISE Research Institutes of Sweden AB | IETF | ACE WG - Proof-of-Prossession Key Semantics for CBOR Web Tokens (CWTs) | Author |
| RISE Research Institutes of Sweden AB | IETF | ACE WG - CBOR Profile of X.509 Certificates | Author |
| RISE Research Institutes of Sweden AB | IETF | Network Working Group - ACE Clients in Disadvantaged Networks | Author |
| RISE Research Institutes of Sweden AB | IETF | ACE WG - Protecting EST payloads with OSCORE | Author |
| RISE Research Institutes of Sweden AB | IETF | 6TiSCH WG - Robust Scheduling against Selective Jamming in 6TiSCH Networks | Author |
| SIDN | IETF | DNSOP WG | Contributor |
| SIDN | IRTF | MAPRG | Contributor |
| Siemens | OASIS | STIX | Member |
| Siemens | OASIS | OpenC2 TC | Member |
| Siemens | OASIS | CACAO TC | Member |
| Telecom Italia (TI) | ETSI | TC CYBER | Observer |
| Telecom Italia (TI) | GSMA | Fraud and security Architecture Group | Contributor |
| Telecom Italia (TI) | NGMN | Security Competence Team | Observer |
| Telefonica I+D | 3GPP | SA3 (architecture, management and security aspects related to Release 18 and beyond) | Participation |
| Telefonica I+D | 3GPP | RAN Plenary Contributing to several Rel-18 proposals | Participation |

| Partner | SDO | Title of committee or standard | Type of participation |
|---|---|---|---|
| Telefonica I+D | CORD | OpenCORD | Member of the Technical Steering Team for CORD |
| Telefonica I+D | ETSI | NFV ISG | Chair of the Network Operator Council |
| Telefonica I+D | ETSI | NFV SEC | Founding member Contributor |
| Telefonica I+D | ETSI | TC CYBER | Contributor |
| Telefonica I+D | ETSI | SAI | Founding member Contributor |
| Telefonica I+D | ETSI | RIS ISG Radio Intelligent Surfaces | Contributor |
| Telefonica I+D | IETF | WG: TEEP, RATS, ACME, I2NSF | Participation |
| Telefonica I+D | IETF | MODEL-T | Part of the proposer team and participant |
| Telefonica I+D | ODL | Open Daylight | Member of the Advisory Board Contributor |
| Telefonica I+D | O-RAN | TSC/EB/WGs | Members of TSC and EB Following activities in WG3, WG4, WG6, WG9 and WG10. |

| Partner | SDO | Title of committee or standard | Type of participation |
|---|---|---|---|
| Telefonica I+D | OSM | Open Source MANO | Leading the initiative Main contributor |
| TÜV TRUST IT | CEN - CENELEC | CEN/CLC/JTC 13 "Cybersecurity and Data Protection" prEN 17640 | Expert |
| TÜV TRUST IT | ISO | - ISO/IEC JTC 1/SC 27 "Information security, cybersecurity and privacy protection" ISO 27017 | Co-editor |
| TÜV TRUST IT | ISO | - ISO/IEC JTC 1/SC 27 "Information security, cybersecurity and privacy protection" ISO 27109 | Expert |
| Università degli Studi di Milano (UMIL) | CEN/CENELEC CWA | Workshop on "Requirements and Recommendations for Assurance in Cloud Security (RACS)". | Contributor |
| Università degli Studi di Milano (UMIL) | ETSI | Cloud Standard Coordination | Contributor |
| Università degli Studi di Milano (UMIL) | OASIS | eXtensible Access Control Markup Language (XACML) | Contributor |
| University of Oslo | OASIS (oasis-open.org) | Open Command and Control (OpenC2) TC | Member |
| University of Oslo | OASIS (oasis-open.org) | Collaborative Automated Course of Action Operations (CACAO) for Cyber Security TC | Secretary |
| University of Passau | DKE AK 351.3.7 | Security Anforderungen an signaltechnische Einrichtungen | Member |
| University of Patras | International Telecommunication Union-T | X.series | Observer, possible contribution |

#### 4.3.2.2. Individual calls for contribution

Through the identification of the key topics that each partner is involved or interested in, monitoring of various standardization efforts was performed by the project team. Having the key topics in mind, individual calls for contributions were sent to targeted partners in those cases where an opportunity for contribution was identified.

e.g., PWI ISO 27109 (where information from Task 3.4. and the CONCORDIA education map was provided).
BS EN 17640[42] Fixed time cybersecurity evaluation methodology for ICT products (where comments were provided as part of Task 5.3.)
BS EN IEC 62351-14[18] Power systems management and associated information exchange – Data and communications security – Part14: Cyber security event logging

#### 4.3.2.3. CONCORDIA's Cybersecurity Roadmap for Europe

As mentioned already in Section 4.3.1.3. one of the six dimensions of "Cybersecurity Roadmap for Europe by CONCORDIA" in related to Certification and Standardization. Information about the contributions to Certification is included in section 4.3.1.3. and in the following paragraphs, information regarding the contributions to Standardization is provided.

Especially in the area of Standardization, within the year 2021, the roadmap has been updated based on the current information derived from:

- Discussions with relevant stakeholders
- Participation in events and conferences
- Review of new publications
- Discussions within the project team

The relevant chapter of the Roadmap includes

- An introduction to standardization
- A description of challenges faced by standardization
- Short term aims
- Midterm aims
- Long term aims

Since the information included in the previous version of the document was gathered until November 2020, the update to the relevant entries was important since a series of developments transpired within 2021.Some of the relevant events and publications are shown in the following list:

- ICT Security Standards Roadmap, published by ITU[43]
- Joint Communication The EU's Cybersecurity Strategy for the Digital Decade, JOIN/2020/18 final – 16/12/2021
- The Rolling plan for ICT Standardization[44]
- Cybersecurity Standardization Conference 2021, 02 February 2021[45]

[42] Standards in public consultation
[43] https://www.itu.int/en/ITU-T/studygroups/com17/ict/Pages/default.aspx
[44] http://ec.europa.eu/growth/industry/policy/ict-standardisation_en
[45] https://www.enisa.europa.eu/events/cybersecurity_standardisation_2021

## 4.4. Impact from Covid-19 pandemic crisis

As discussed already in the other parts of this deliverable as well as in other deliverables of this project, the pandemic affected or even interrupted the work of several CONCORDIA teams, either academic or industrial, and reduced or even stopped their technical progress. This was the case last year, and also this year (Y3).
In relation to the Certification activities, as mentioned in section 4.3.1. two pilots of the $C^3$ by CONCORDIA were implemented using remote means. Based on the feedback from the participants, the use of fully online means for participating in the exams was not identified as a negative. The activities in relation to the Cybersecurity MOOC Certification were delayed from the original planning proposed during the end of the previous year, but the delays cannot be attributed to the COVID-19 restrictions (mainly due to the extension of the survey duration to collect a greater number of responses and the decision of the team to participate in an international workshop with a relevant presentation and publication). The activities regarding the interviews and the validation of the results have already started and will be completed within Y4.
The project team participated in various conferences, workshops and meetings within this project, with other projects, organized by ENISA and other parties. None of these interactions were face to face, that had a somewhat adverse effect in terms of networking and exploration of cooperation potential. In spite of this limitation, the project team was able to receive feedback regarding future needs and create cooperations that will be further explored in Y4.
Finally, it is the project team\s opinion, that the standardization efforts were not significantly affected by the COVID-19 restrictions.

## 4.5. Next Steps in Certification and Standardization

During the next period of the CONCORDIA project, the project team aims to do the following:

In the area of Certification, as already described in the above sections, the following activities are planned:

- Initiation of the new team on Certification (more information in Section 4.3.1.4.)
- Realization of the cooperation between CONCORDIA and the two projects (CYRENE & A4CEF) (more information in Section 4.3.1.4.)
- Provision of feedback regarding certification schemes and initiatives (more information in Section 4.3.1.4.)
- Provide recommendations regarding the Cybersecurity Certification Framework (more information in Section 4.3.1.4.)
- Implement a new pilot to the Certification scheme of the Cybersecurity Consultant (more information in Section 4.3.1.1.)
- Collect feedback and improve the Certification scheme of the Cybersecurity Consultant (more information in Section 4.3.1.1.)
- Finalize the Cybersecurity Skills Certification Framework (more information in Section 4.3.1.1.)
- Provide feedback and finalize the input regarding Certification in CONCORDIA's Cybersecurity Roadmap (more information in Section 4.3.1.3.)
- Evolve activities regarding MOOC certification (more information in Section 4.3.1.2. Activity 1)

- Collaborate with T.4.3 in relation to the Cybersecurity Label (more information in Section 4.3.1.4.)
- Collaborate with WP4 in relation to dynamic certification (more information in Section 4.3.1.4.)
- Pursue other opportunities in relation to certification (more information in Section 4.3.1.4.)
- Continue the cooperation with the REWIRE project (more information in Section 4.3.1.2. Activity 4.)

In the area of Standardization, as already described in the above sections, the following activities are planned:

- Support the CONCORDIA partners in their needs regarding standardization
- Investigate further actions and synergies regarding standardization
- Provide feedback and finalize the input regarding Standardization in CONCORDIA's Cybersecurity Roadmap
- Provide CONCORDIA's input in relation to specific standardization efforts (where possible). The project team plans to employ the same methodology and target specific standardization efforts based on the key topics each partner / WP / Task is involved in. (more information in Section 4.3.2.2.)

# 5. Conclusions

In view of achieving the overarching project Objectives, Work Package 5 (WP5), aims at, enhancing the impact of CONCORDIA's outcomes through strategic exploitation, dissemination, and standardization activities. From an exploitation perspective, WP5 has developed and executes a comprehensive exploitation plan, in alignment with the project's objectives and the partners' commercial and research interests. Furthermore, the standardization activities in WP5 aim to enhance the impact of CONCORDIA by transferring project results to relevant industry standardization and best practice working groups.

This document split into three parts: Exploitation, Dissemination & Communication and Certification & Standardization. In each part, it presents the objectives, the strategy to achieve them, the activities carried out and the results achieved during the 3rd year of the project, the impact from the COVID-19 pandemic crisis and the next steps to be carried out during the next year (Y4) of the project.

In Year 3, CONCORDIA project engaged in dissemination and communication activities with a focus on the demonstration of the value that is delivered by the project during the last year. In this respect, it is important to mention three facts. Firstly, the consortium is able to produce regular quality content about its work; note that all partners all involved. in the generation of this content. Secondly, CONCORDIA regularly cooperates with external stakeholders, including the DG CNECT communication team. Thirdly, the performed communication activities have been primarily focused on digital channels due to COVID-19. The growing communities on social media platforms (Twitter and LinkedIn) show that CONCORDIA is able to build its audience even without face-to-face meetings. Some changes and delays have been identified due to the COVID-19 pandemic crisis imposed restrictions. More information regarding this impact is contained in the relevant subsections of each part (namely the 2.7, 3.4 and 4.4 subsections). By the moment of the drafting of this document, specific plans have been created and activities have been identified to be implemented from now until the end of the project. More information is contained in the relevant subsections of each part (namely the 2.8, 3.5 and 4.5 subsections).

As a general conclusion regarding all parts and topics presented in this document, all relevant objectives have been achieved or exceeded. This is reflected by the key achievements reported through this document and are further demonstrated by the level of completion of the KPIs, outlined in the Introduction of this deliverable.

# Annex A: Meeting minutes for June and November 2021 meetings of ISC

Meeting date: 17.06.2021
Meeting occasion: Internal Strategy Committee Semi-annual meeting (T5.1)
Meeting location: online
Meeting Agenda:

1. Introduction
2. Discussion on data collected up to mid 2021
3. Certification scheme for cybersecurity skills
4. Cross pilot collaborations
5. Future directions / steps

| **Participants** |
|---|
| **Partner organisation** |
| TÜV TRUST IT |
| SIDN |
| DFN-CERT |
| IFAG |
| Airbus |
| Bitdefender |
| CAIXABANK |
| Telenor |
| RUAG |
| ATOS (T5.1 co-leader) |
| TID (T5.1 co-leader) |
| Eesy-inno |
| Flowmon |
| ERICSSON |
| CRF |

**1. Introduction:**

- Primary intention of the meeting is to jointly discuss Key Exportable Results (KER)
- The T5.1 leader presented the structure of the new T5.1 (objectives and strategy) and repeated the reasons why ISC exists and what are its roles
    1. At the end of 2020, the tasks T3.5 (start-up community building) and T5.1 (exploitation) were merged. In addition, some elements of innovation from WP6 (T6.3) were also introduced. Also, two communities of email lists were merged for efficiency purposes
    2. This new task redefined the strategy to align exploitation and innovation.
    3. Also, by the end of 2020 (December) there was the first assessment of ERs that was in fact presented to the project review meeting, early 2021
- Each industrial partner has one representative in ISC, currently 23 members. ISC at the same time serves as innovation and exploitation board, established within CONCORDIA. Roles are to find ERs, provide feedback on business model, help with incubators and supporting start-ups, etc.

**2. Data collection on Exploitable Results:**

- In the last meeting (12/2020), there was a definition of 4 criteria on how to judge ERs across different dimensions:
    1. market demand (based on the knowledge of ISC members)
    2. innovation potential
    3. technical maturity (TRL level)
    4. network/community effect (CONCORDIA specific)
- The ISC members shared feedback on possible integration within ERs, e.g., such as in T2.1 and its sub-pilots ERs. The goal would be to accelerate ERs, since industrial partners can give a boost to an ER given their contacts in respective communities and eco-systems/markets.
- The ISC members also provided feedback on synergies or complementarities across Work Packages.
- In Y3 there is a need to accelerate ERs, concretely for pilots to find market uptake, more visibility and find potential users/buyers (which was one of review comments). For that reason, ISC should focus on market readiness level and market desirability.
- The T5.1 leader shared a list of actions for 2021, including new yearly call for ER (as defined methodology in past deliverable) and review of old ERs. Final ranking for 2021 to be done in December at the next meeting of ISC.
- In final year Y4, CONCORDIA should make events to boost ER uptake. This has already been done for the financial pilot / sector: An event was organized in 04/2021 and another one is planned for 12/2021.
- The new ER collection for mid 2021 was performed via email communication and survey collection, following similar process as in Y1 and Y2, but with richer and more detailed features requested per ER.
- Strategies mentioned for promotion of KERs: a) innovation radar and visibility at EC web, b) use of COD 2021 for promoting Concordia results.
- Strategy ideas for community-depended ERs:
    1. Scale visibility, CONCORDIA community to promote its results of all partners. Also, consider current market fragmentation in Europe. Organise targeted events for specific regions, or sectors.
    2. Link ER initiatives, e.g., with the certification activities.
    3. Different national communities (for ECCC) are already created with their own specificities. There should be alignment and CONCORDIA's help of community management at EU level. This effort may also be related to governance. Community as in a call is ERs, those processes and procedures can be replicated. As example this ISC could be a pilot for what in the future could be some kind of board (advisory) in ECCC.

**3. Certification scheme for cybersecurity skills**

- An idea for what the industrial community could do for the exploitation of this certification scheme would be, along with T4.6, to create a stakeholder group on certification and promote it in certification bodies.
- As certification has been part of training, there has been already a lot of promotion on the topic.
- It was also promoted in the CCN group and to the other pilots. Maybe industrial

partners can also promote it internally, and review the set of skills included in this schema.
- Also, for national authorities, a framework on cybersecurity consultants might be interesting, in cooperation with the EU project REWIRE (https://rewireproject.eu/) which is working on the idea of "cybersecurity officer".

**4. Cross-pilot collaboration:**
- There was a contact with SPARTA, who created a platform to manage research assets called RAMP[46] , managed by the University of Luxembourg. This is similar to CONCORDIA's table for collecting ERs.
- One idea discussed was that in the next version of RAMP, CONCORDIA will get access to this platform to include ERs as assets, with different visibility options: 1) only CONCORDIA partners, 2) across the 4 pilots, 3) outside the pilots.
- CONCORDIA proposed to SPARTA delegates to include in the workflow further steps such as security assessments as a precondition for getting certification or cybersecurity labelling, and also allow search in the platform for partners that will carry out the specific ER or asset.
- SPARTA was open for further ideas and proposals to extend the RAMP platform to be more than just a marketplace. Also, since SPARTA finishes at the end of 2021, a 2nd version of the platform will be available by then (in that 2nd version, RAMP will move away from the initial MISP-based solution, and instead will be more customised for the specific task at hand).
- Overall, it would be good to use the tool for collection and structure of ERs till the end of the year and/or project, and to give the tool a chance within CONCORDIA, since no resources will be needed, and also does not make sense to put effort in building an additional tool. It would also be important for transitioning of the 4 pilot projects' ERs/assets into international communities. Therefore, it will be an advantage to have one prominent tool for the management of all pilots' ERs. There was a question of further operational support after SPARTA projects ends. The ISC hopes there will be an opportunity to have a local operational CONCORDIA version, in 2022.

**5. Future Directions:**
- The ISC discussed the idea of building a future series of seminars, e.g., on how to build a business plan, and how to pitch or demo an ER to investors, how to protect the IP of an ER, maybe summarize some successful ER stories, etc. Some options would be to organize: 1) a 1-day event with several sessions, or 2) a series of sessions (bi-weekly, monthly, etc.). Maybe the ISC could launch a call for seminars within the incubators/accelerators community to get feedback, ideas and interest for participation. Then, the ISC can select suitable proposals.
- The ISC to-dos for next meeting:
    1. Raise awareness on ER importance across CONCORDIA partners
    2. Push CONCORDIA partners for ER collection
    3. Help inexperienced partners (SMEs/start-ups) with the process
    4. Consider options for KERs to be demoed in session with 4 pilots

Meeting date: 24.11.2021
Meeting occasion: Internal Strategy Committee Semi-annual meeting (T5.1)
Meeting location: online
Meeting Agenda:

[46] https://ramp.c3.lu/

1. Intro on ISC for new members
2. Update on ECCC CC strategy for Innovation and Exploitation
3. Assessment of ER ranking
4. Next steps / ideas for strategic direction contributions

| **Participants** |
|---|
| **Partner organisation** |
| SIDN |
| DFN-CERT |
| IFAG |
| Airbus |
| Telenor |
| RUAG |
| ATOS (T5.1 co-leader) |
| TID (T5.1 co-leader) |
| Eesy-inno |
| Flowmon |
| CRF |
| TI |

**1. Introduction:**

- There was a short introduction on ISC for new members, as they may have lately joined, to get a better overview on ISC function and tasks: ISC meets twice a year, discusses project outputs from the point of view technology, CONCORDIA pilots and their progress with respect of ERs. Performs assessments of ERs, once per year (via surveys) to identify novel ideas, does KER selection, support and promotes top ER candidates, gives guidance in e.g., patentability, business plans, etc.
- Main goals for the new meeting: ECCC-CC updates, ER assessment and raking, key ER identification, and next steps.

**2. Updates on ECCC – CC:**

| Strategy element | Challenges | Benefit | Risk |
|---|---|---|---|
| Yearly ER assessment | Single framework for disparate ER (in terms of TRL, type etc) | Continuous feedback helps ER owners, but also in project orientation (synergies, complementarities, priorities) | Another overhead for partners and decision making body (ISC) |
| ISC role as an expert committee | Move from subjective to objective ER assessment | Selects and highlights KER according to desirability, feasibility and sustainability criteria | Motivational issues, feasibility and sustainability of ISC |
| Start-ups as an exploitation path | Conciliation with the other paths | Support in definition of value, access to funding, partnership and market propositions… | Needs to be balanced with the other initiatives and paths |
| Highlights for "community role" | Network effects, economy of scale, partnerships, education, certification… | Identifies increase of ER potential through community support | Community exploitation path is not mature yet |

Figure 7: CONCORDIA Strategy on Innovation and Exploitation

- CONCORDIA strategy and its main elements (see Figure 7): ISC foresees yearly ER assessment, single framework for exploitation and innovation. It is important for community to have such priorities in terms of where research and where more market-oriented studies should go.
- Innovation radar or JRC as methodology applied, KYPO won prize in 2021. But still method of Innovation Radar is subjective and based on self-assessment.
- CONCORDIA is the only pilot having this exploitation path for start-ups, and this should be included in ECCC as one of possible exploitation paths for future EU project results.
- CONCORDIA's community role differs from the other pilots, giving special importance for network effects. It was acknowledged in the last paper of ENISA about ECCC, explicitly mentioning assessment of network effects as issues for future strategic directions of ECCC. In fact, ENISA received more than 400 feedbacks and proposals from the 4 pilots and ECSO, and in fact reduced the 11 strategic directions of ECCC to 8 in its last document draft.
- During a meeting of ENISA, ECCC, ECSO and the 4 pilots, CONCORDIA was represented with members in CCN focus groups on roadmaps, governance and strategy, respectively. Feedback received from the meeting could be included in CONCORDIA's roadmap, a responsibility that lies within T4.4.
- The ISC also discussed the transition of research to development. That is, in what extend will the ECCC interact in similar initiatives in member states, or structure of organisations existing at universities around Europe for transfer of research. Will the centre duplicate that effort at an EU level?

**3. Assessment of ERs / Ranking:**

- The ISC discussed the ERs that were collected using the process from last year, i.e., via surveys. The same process was applied for the collection of accelerators and incubators.
- ERs could be tangible or intangible. Partners were asked to submit or resubmit ERs giving the relation to specific defined dimensions. This information was used to do the ranking by the ISC.
- Details of all ERs collected was presented, including summaries on type, technical readiness levels, market focus, etc. (please check Section 2 for these results).
- Current ERs classified in context of technical maturity and envisioned technical maturity (something not done in 2020). Most ERs plan to increase TRL level, which is an encouraging sign. Industry sectors for applications of ERs include telco, finance, operators of digital services, e-health, automotive, any industry sector. (please check Section 2 for these results).
- Next step was to perform selection of ERs, ranking and selection of Key ERs for 2021. Thus, first there was a preselection of ERs, focusing on tangible ERs (software, services) according to a) market readiness, innovation potential, technical maturity and community orientation.
- Then, there was a survey circulated within ISC to perform ER assessment and valuation for ranking.
- Finally, the current ranking of ERs based on the surveys collected was shown and discussed (please check Section 2 for these results).

## 4. Next steps / ideas for strategic direction contributions

- The ISC needs to analyse the current CONCORDIA roadmap and give feedback related to the ERs and ISC activities.
- Other process activities for last year of the project will include the promotion of Key ERs, definition/collection of business models, their ranking and promotion of suitable business models to accelerators and incubators.
- The ISC needs to remind CONCORDIA partners that it can offer guidance and advice to those partners that are not skilled in handling IPR. Also, CONCORDIA is here to pilot processes for ECCC and should listen to typical problems/requests of partners. Based on these declarations and the experience in this process, the ISC should give future competence centre advice/list of typical issues, e.g., that centres should have contact point for conflict resolution, should have templates for exploitation agreements, legal contact point for patents, etc.
- The ISC will work more intensely on PR actions in 2022, and take advantage of the *CONCORDIA Delivers* campaign. The ISC should also engage the incubators and accelerators that CONCORDIA partners have a reach, in order to organize workshops and seminars. The ISC should also facilitate the pitching of Key ERs to the next ISC meeting.
- The ISC also brainstormed on what else can be done with respect to ERs and T5.1. An idea was to perform clustering of ERs based on some dimension. Several directions of possible clustering were discussed such as:
    a) Clustering ERs that are ground-breaking
    b) Clustering ERs that are just incremental changes of existing technology
    c) Mapping ERs to target groups that will be addressed with said ERs, such as consumers (citizens), special industries (business users), public bodies, or cybersecurity professions
    d) Clustering ERs together if they support EU main target of Digital Sovereignty or other high-level EC priorities
    e) Clustering ERs based in respect to horizontal and vertical industries
- The ISC also discussed the appropriate use of Technological Readiness Level (TRL) and Market Readiness Level (MRL), as used in other EU projects such as Cyberwatching.eu, to assess readiness of ERs to be used in the market. In fact, the ISC may propose to establish Exploitation Readiness Levels (ERL) (See Figure 8) as indicator to assess market maturity. This ERL adaption preliminary idea is to keep levels 6-9 from MRL list, and adapt the first five 1-5 levels. KPIs to have an ERL proven are different, but we need to check if there are any existing indicators to reuse.

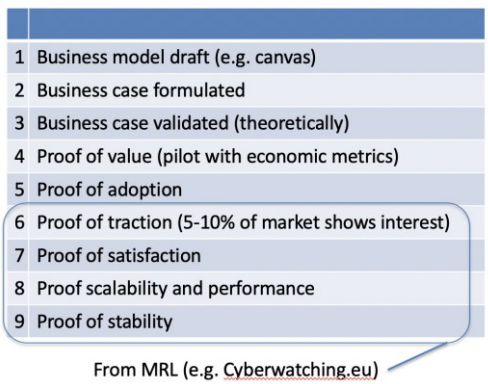



Figure 8: Proposal for Exploitation Readiness Levels (ERLs)

# Annex B. Report on Piloting the C³ by CONCORDIA certification scheme – structure and deployment

## Table of Contents



## Introduction

The key component to any certification program is its scheme. The scheme consists of the standards and systems that certification programs use to determine what the requirements are for initial certification, maintenance of certification and re-certification and how individuals are to be assessed against these requirements[47].
As part of the CONCORDIA Education activities, the need for developing a framework in the context of CONCORDIA Cybersecurity certification was identified. The goal of the Certification Framework is to ease the process of delivering, obtaining, securing and verifying certificates for Cybersecurity skills. This certification Framework defines the principles and requirements of CONCORDIA for Cybersecurity certification.
The certification scheme "C³ by CONCORDIA" [Link] was developed based on the best practices described in the CONCORDIA Certification Framework for Cybersecurity skills. (Please note that the CONCORDIA Certification Framework for Cybersecurity skills has been in preparation and is planned to be published soon, after the completion of the pilot runs of the certification scheme).

[47] GUIDELINES ON CONFORMITY ASSESSMENT – ISO/IEC 17024:2012. United Nations Industrial Development Organization.

The current document presents the model followed for the pilot of the certification scheme "$C^3$ by CONCORDIA"

**The components of the certification scheme "$C^3$ by CONCORDIA"**

This certification scheme "$C^3$ by CONCORDIA" aims to validate the knowledge, skills and abilities, in other words the relevant competencies, of a Professional acting (or wanting to act as a Cybersecurity Consultant).

The process of defining and validating the profile for the Cybersecurity Consultant is documented in the CONCORDIA Workshop on Education for cybersecurity professionals - post workshop report – [Link]. The implemented profile was expressed in a manner compatible to both the NICE Cybersecurity Workforce Framework taxonomy [Link] and the European e-Competency framework [Link].

The certification scheme "$C^3$ by CONCORDIA" builds upon the information of the Cybersecurity Consultant Role Profile and defines the mechanisms for its validation.

The information contained in the certification scheme "$C^3$ by CONCORDIA" is:

- Scope of certification
- Job and task description
- Required competence
- Abilities
- Prerequisites
- Declaration of Honour
- Criteria for initial certification and recertification
- Examination Committee/ Examiners
- Requirements
- Assessment methods for initial certification and recertification
    - Section A.: Assessment method Theoretical method, written.
    - Section B.: Assessment method Practical method, simulation
- Surveillance methods and criteria
- Criteria for suspending and withdrawing certification
- Storing and Validating certificate information

**The pilot of the certification scheme "$C^3$ by CONCORDIA"**

In order to test the best practices proposed by the CONCORDIA certification framework and the processes defined in the certification scheme "$C^3$ by CONCORDIA", a pilot examination was designed and implemented.

For the implementation of this pilot, the following assumptions were made.

**The knowledge, skills and abilities**

Due to the maturity of the framework, the project team selected to construct the curriculum based on the NICE Cybersecurity Workforce Framework taxonomy[48], although it identified 73 Knowledge and 38 Skills requirements.

Since Role Profile was identified at a medium level and keeping in mind the constraints of the examination mechanisms, the knowledge and skills requirements were prioritized based on their importance during the relevant workshop [Link].

[48] https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework

The remaining, most important, knowledge, skills and abilities were aggregated and grouped under three main learning objectives:

1. Threats – Get updated on the existing and emerging cybersecurity threats, the assets possible to be impacted, and the latest models of attacks.
2. Technology – Become knowledgeable about specific technological threats, learn how to anticipate and prevent them, while developing proactive management skills.
3. Economics – Get an understanding of the economics behind cybersecurity activities within your organization. Learn about risk management and information security to protect the corporate reputation and preserve customer loyalty.

The following Figure B1, depicts the knowledge and skills covered by the Cybersecurity Consultant role profile to be covered by the relevant certification scheme.

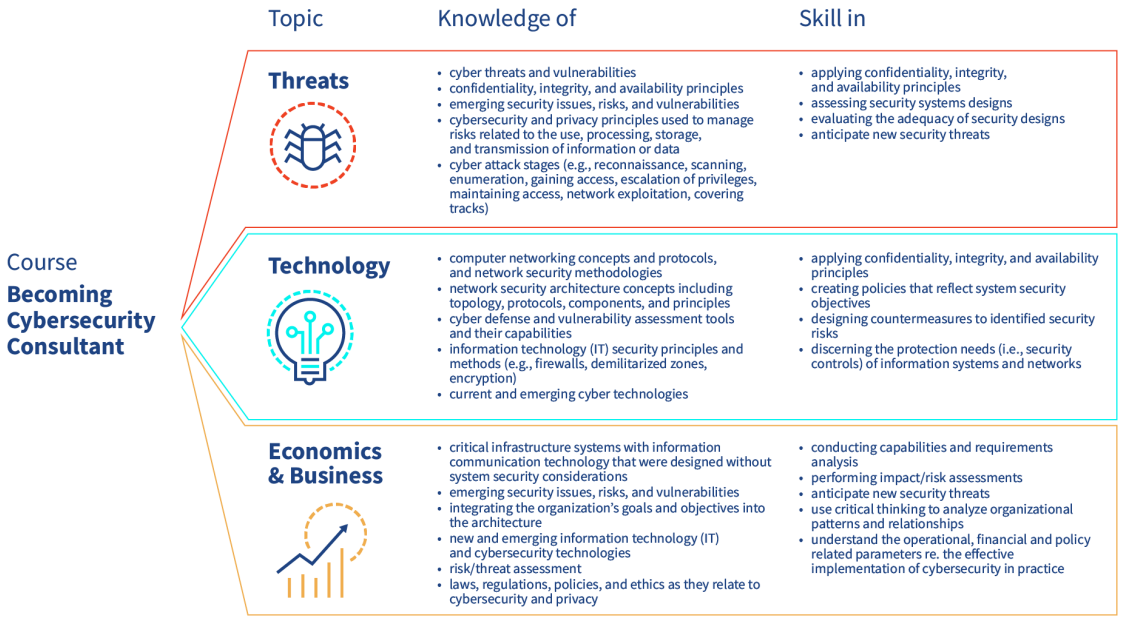



Figure B1: List of Knowledge and Skills addressed under the 3 main learning Objectives.

To make sure that the produced certificate correctly reflects the level of knowledge, skills and abilities of the Cybersecurity Consultant, a set of prerequisites has been defined. Specifically, candidates for the "C$^3$ by CONCORDIA" certificate, should already have a basic knowledge on several of the areas mentioned above. The analysis of the pre-requisites is provided in the certification scheme "C$^3$ by CONCORDIA" [Link].

## Preparation for the Exam

As mentioned in the "C$^3$ by CONCORDIA" certification scheme, the examination is split into two sections. Section A is a theoretical multiple-choice exam, run through a specialized platform and Section B is a practical simulation like exam, ran through two separate specialized platforms.

Prior to the implementation of the pilot exam, and in order to facilitate the two sections of the exam the following steps were implemented:

***Section A.1: Assessment method Theoretical method, written.***

A databank of multiple-choice questions was created. The partners involved in the effort to create the databank are presented at the end of the section. The databank contains 170 questions covering content from learning objectives and formulated as to reflect all three levels of difficulty.

The level easy represents questions that are related to theoretical knowledge on basic concepts and principles of the related subject. The level medium represents questions that build on the theoretical knowledge of the previous questions a deeper understanding of the subject in question. Finally, the level high represents questions that exercise critical thinking and require deep understanding of the subject in question.

The following table B1, depicts the distribution of the questions based on their learning objective and difficulty.

Table B1: Distribution of the questions based on their learning objective and difficulty

| Categories | Number of Questions | Questions per LO | Questions per Dif. Level |
|---|---|---|---|
| **LO1** | **60** | **35,29%** | |
| Easy | 19 | | 31,67% |
| Medium | 26 | | 43,33% |
| High | 15 | | 25,00% |
| **LO2** | **54** | **31,76%** | |
| Easy | 18 | | 33,33% |
| Medium | 24 | | 44,44% |
| High | 12 | | 22,22% |
| **LO3** | **56** | **32,94%** | |
| Easy | 20 | | 35,71% |
| Medium | 24 | | 42,86% |
| High | 12 | | 21,43% |
| **Total** | **170** | **100,00%** | **100,00%** |

Based on the decision of the project team, all multiple answer questions followed the same format, meaning that in every case, for each question, 4 possible answers were proposed, only one of which was correct (single choice).

The activity was coordinated by EIT Digital and TÜV Trust IT GmbH, member of the TÜV Austria Group, and received substantial support in all its phases, from design to implementation, from CONCORDIA academic and industry partners: University of Milan, Italy; University of Loraine, France; University of Zurich, Switzerland; The Industrial System Institute Greece, University of Insubria, Italy; BITDEFENDER, Romania; Arthur's Legal, The Netherlands.

***Section A.2: The assessment platform.***

For the implementation of the theoretical exam, the project partners performed a market survey and selected the company (and platform) ISOGRAD[49].

[49] https://www.isograd-testingservices.com/EN/index

The criteria that needed to be met for the selection of the platform were the following, as derived from the principles of the relevant CONCORDIA certification framework and scheme:

- **Online**. The platform has to be available 24x7 for the period that the examination is active for the participants.
- **Proctored**. The platform or the system should have the ability either automatically or manually to monitor the activity of the participant, in order to identify and prohibit foul play.
- **Random**. The platform should have the ability to construct the examination by selecting questions randomly from the databank. Each participant should not undertake the same (100%) exam. The selection of the questions from the databank should be governed by a specific algorithm related to the LO and the difficulty level.
- **Interactive**. The platform should provide interactive messages to the participant, in case that a problem or an issue has been identified during the session.
- **Results**. Provisional results should be shown at the end of the examination attempt.
- **Timed**. The platform should have the ability to monitor the time spent per question and overall, for each attempt. Each examination attempt will only be allowed to be taken once and will only have a specific – predetermined – duration.
- **Confidentiality**. The information and performance of the candidates should remain confidential. Specific measures to guarantee confidentiality should be implemented throughout the entire process.
- **Privacy**. The personal information of all subjects should be protected in accordance with current European regulation and legislation.

***Section A.3: Preparing the exam***

Followingly, the ISOGRAD system was customized based on the specifications of the certification scheme "$C^3$ by CONCORDIA".
Specifically, all 170 questions and possible answers were inserted, and the following rules were implemented:

- The total number of questions per examination should be 50.
- The questions shall be selected from each learning objective identified the databank and from all difficulty levels following at least the percentage of selection (30% Low - 50% Medium- 20% High).
- All learning objectives will be equally covered.
- A candidate will need to score of 70% or more in order to pass this section of the exam.
- A candidate will need to score of 60% or more per Learning Objective in order to pass this section of the exam.
- Each question is awarded one mark. No negative marking is applicable.

After the questions were inserted and the rules implemented, tests were carried out by four members (EIT Digital, TÜV TRUST IT, University of Insubria and University of Zurich), of the CONCORDIA project team between the 6$^{th}$ of May to the 13$^{th}$ of May 2021.
Identified issues or improvements were communicated to the ISOGRAD team and corrections and corrective actions were implemented.
Specific texts for the introduction to the exam and the environment and for the announcement of the results were created and implemented in the system.

***Section B.1: Assessment method Practical method, interactive simulation.***

*The practical exam involved the creation of a scenario implemented through two different platforms:*

- *KYPO* - https://www.concordia-h2020.eu/kypo-cyber-range/
- *Mooncloud* - https://www.moon-cloud.eu/en/

*The implemented scenario aimed to assess and validate skills and abilities of the participants within the following domains:*

- *Risk assessment*
- *Threat identification*
- *Vulnerabilities*
- *Source code analysis*
- *Penetration testing*
- *Cybersecurity Economics*

*These topics were selected by the project team taking into consideration the Learning Objectives presented above, the available resources, the restrictions of current solutions and the restrictions imposed by the current COVID-19 pandemic crisis.*

***Section B.2: The assessment platforms.***

The criteria that needed to be met for the selection of the platforms for the practical part of the exam were the following, as derived from the principles of the relevant CONCORDIA certification framework and scheme:

- **Online**. The platform has to be available 24x7 for the period that the examination is active for the participants.
- **Hands-on.** The platform should provide the ability for the candidates to exercise and validate their skills and abilities in a practical manner.
- **Interactive**. The platform should provide interactive messages to the participant, in case that a problem or an issue has been identified during the session. Moreover, the platform should allow where possible the provision of hints, so that the process could continue. Each hint should have a specific penalty when used.
- **Results**. The results should be shown at the end of the examination attempt.
- **Timed**. The platform should have the ability to monitor the time spent per question and overall, for each attempt. Each examination attempt will only be allowed to be taken once and will only have a specific – predetermined – duration.
- **Confidentiality**. The information and performance of the candidates should remain confidential. Specific measures to guarantee confidentiality should be implemented throughout the entire process.
- **Privacy**. The personal information of all subjects should be protected in accordance with current European regulation and legislation.

***Section B.3: Preparing the exam.***

The project team decided to incorporate all topics to be exercised and validated in one comprehensive scenario. The scenario contained a number of virtual appliances which were implemented in the platforms. Tasks were created in each platform and a system for grading the attempts was created. Due to the nature of the platforms, no automatic grading was

possible. Each attempt was manually reviewed and graded after completion. (The reasoning for the manual grading was the following: The attempt included the creation of zones and targets, executing evaluations and registering targets. Since the effort consists of multiple steps and not just an end result, the grading had to be performed manually, taking into consideration the implementation of all the correct steps).
A document containing instructions for the participants was created.

The activity was coordinated by EIT Digital and TÜV Trust IT GmbH, member of the TÜV Austria Group, and received substantial support in all its phases, from design to implementation, from CONCORDIA academic and industry partners: University of Milan, Italy; University of Loraine, France; University of Zurich, Switzerland; The Industrial System Institute Greece, University of Insubria, Italy; BITDEFENDER, Romania; Arthur's Legal, The Netherlands.

## The application process

An application for the $C^3$ by CONCORDIA certification exam was created and dispatched on the 25th of May 2021 to all participants of the Cybersecurity Consultant course which successfully attended both the online and live webinar modules of the course.
The Application is contained within Annex A of this document.
The received applications were reviewed by the project team in relation to the certification scheme acceptance criteria.
An acceptance email was sent to the relevant participants, providing information on the timeline of the examination.

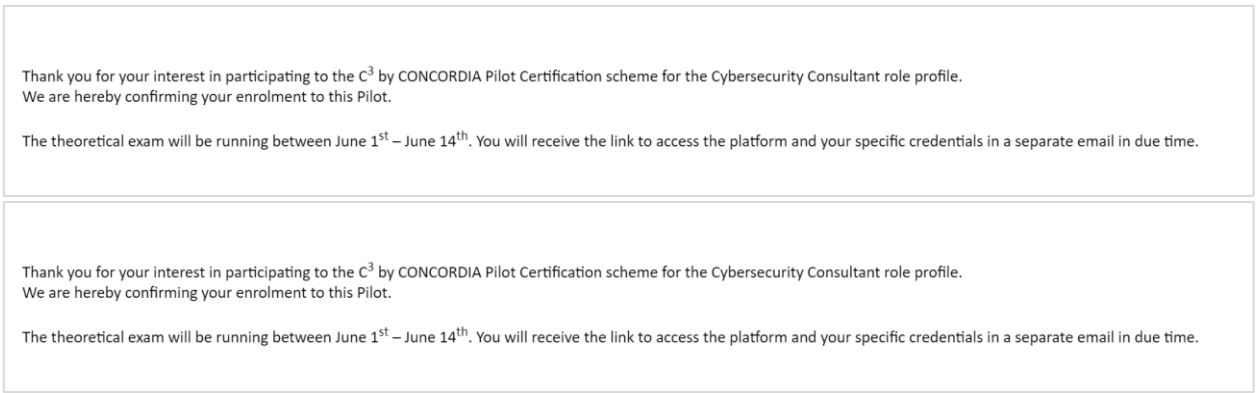


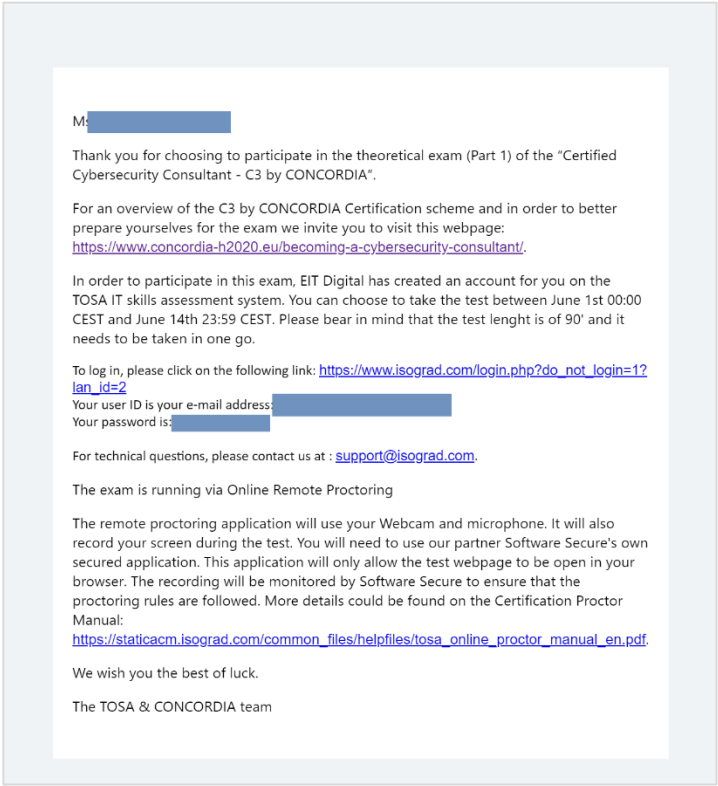

Figure B2: Acceptance email was sent to the relevant participants, providing information on the timeline of the examination

## The implementation of the exam

### Exam participants and results

The number of submitted and accepted applications was ten (10).
The candidates were invited via email to participate in the **theoretical part of the exam**.
The period that the exam could be undertaken through the ISOGRAD platform was June 1st – June 14th 2021.
Each participant had the opportunity to select the desired timeslot to undertake the exam, based on her/his preference.

All participants were given access to the ISOGRAD platform and manual.
All ten candidates participated in the theoretical exam.



M[redacted]

Thank you for choosing to participate in the theoretical exam (Part 1) of the "Certified Cybersecurity Consultant - C3 by CONCORDIA".

For an overview of the C3 by CONCORDIA Certification scheme and in order to better prepare yourselves for the exam we invite you to visit this webpage: https://www.concordia-h2020.eu/becoming-a-cybersecurity-consultant/.

In order to participate in this exam, EIT Digital has created an account for you on the TOSA IT skills assessment system. You can choose to take the test between June 1st 00:00 CEST and June 14th 23:59 CEST. Please bear in mind that the test lenght is of 90' and it needs to be taken in one go.

To log in, please click on the following link: https://www.isograd.com/login.php?do_not_login=1?lan_id=2
Your user ID is your e-mail address: [redacted]
Your password is: [redacted]

For technical questions, please contact us at : support@isograd.com.

The exam is running via Online Remote Proctoring

The remote proctoring application will use your Webcam and microphone. It will also record your screen during the test. You will need to use our partner Software Secure's own secured application. This application will only allow the test webpage to be open in your browser. The recording will be monitored by Software Secure to ensure that the proctoring rules are followed. More details could be found on the Certification Proctor Manual:
https://staticacm.isograd.com/common_files/helpfiles/tosa_online_proctor_manual_en.pdf.

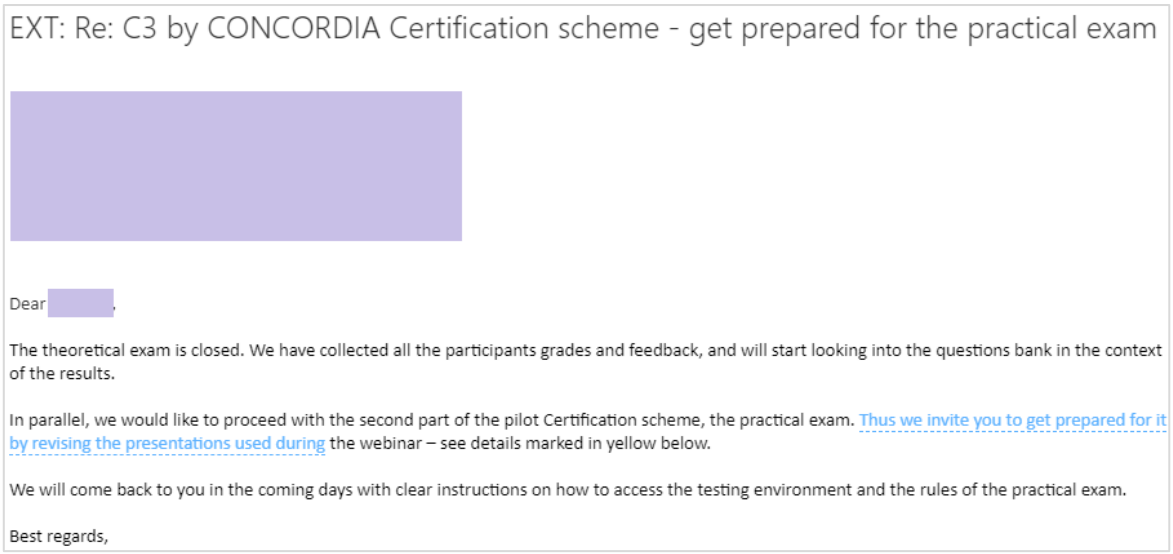
We wish you the best of luck.

The TOSA & CONCORDIA team

Figure B3: Invitation for the participation in the theoretical exam though the ISOGRAD system

The ISOGRAD platform utilizes an AI assisted proctoring system. The recordings and issues identified during the exam are reviewed within a period of 10 days after the implementation of the exam.
An analysis of the result is displayed to the candidate after the completion of the test, but a specific text was crafted to inform them that this would not be the final results as the review and quality review is pending.
The average score for people that passed the theoretical exam was 79.5% and the Average score for people that failed the theoretical exam was 70.5% (this is above 70% which is the threshold but, in these cases, the candidates did not achieve the minimum 60% in all sections).

For the **practical part of the exam**, the candidates were informed via email about the time that the platform will remain open. The period that the exam could be undertaken through the Moon Cloud and KYPO Cyber Range platform was June 1$^{st}$ – June 14$^{th}$ 2021. Attached to the informative email were relevant instructions for conducting the exams.



EXT: Re: C3 by CONCORDIA Certification scheme - get prepared for the practical exam

[redacted]

Dear [redacted],

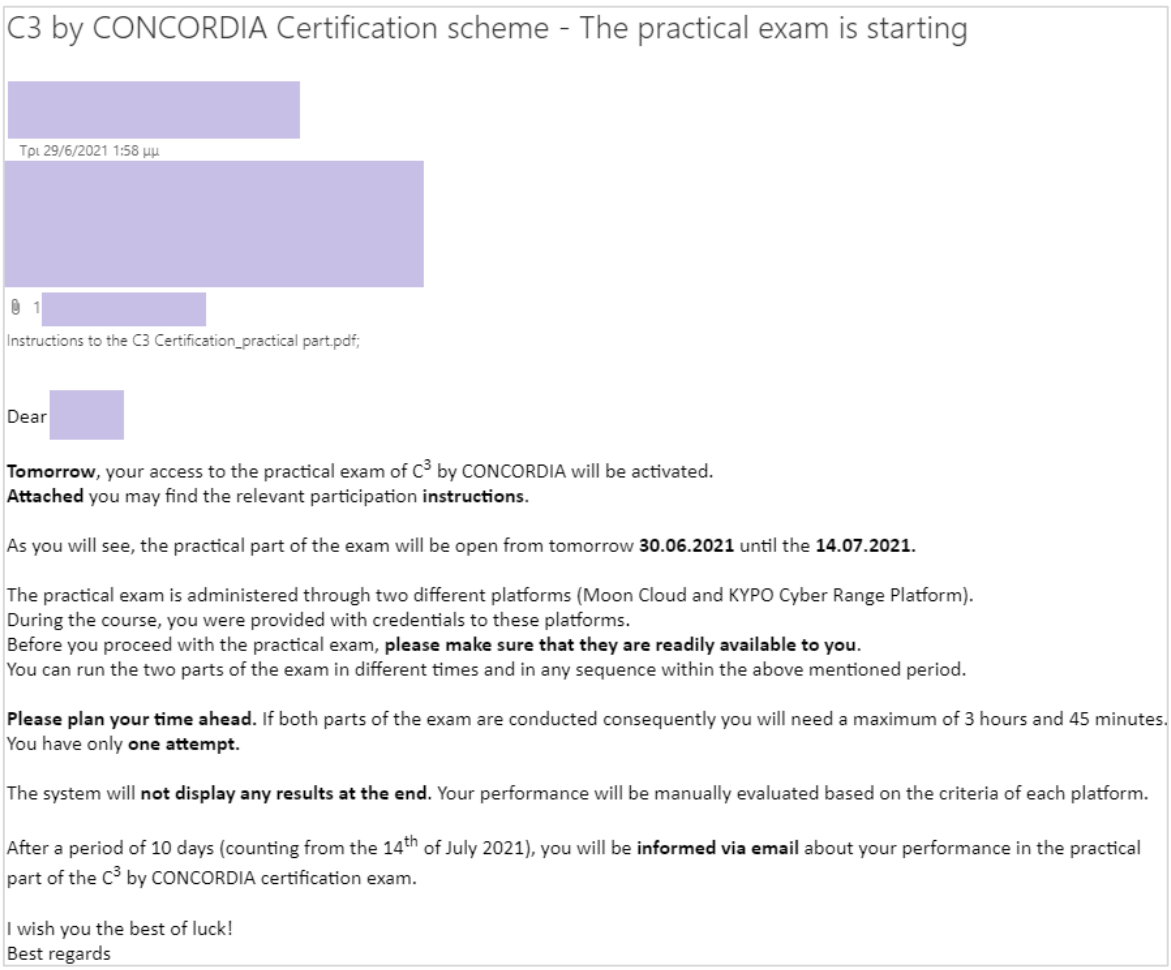
The theoretical exam is closed. We have collected all the participants grades and feedback, and will start looking into the questions bank in the context of the results.

In parallel, we would like to proceed with the second part of the pilot Certification scheme, the practical exam. Thus we invite you to get prepared for it by revising the presentations used during the webinar – see details marked in yellow below.

We will come back to you in the coming days with clear instructions on how to access the testing environment and the rules of the practical exam.

Best regards,

Figure B4: Invitation to participate in the practical exam part 1



C3 by CONCORDIA Certification scheme - The practical exam is starting

[redacted]

Τρι 29/6/2021 1:58 μμ

[redacted]

1 [redacted]

Instructions to the C3 Certification_practical part.pdf;

Dear [redacted]

**Tomorrow**, your access to the practical exam of $C^3$ by CONCORDIA will be activated.
**Attached** you may find the relevant participation **instructions**.

As you will see, the practical part of the exam will be open from tomorrow **30.06.2021** until the **14.07.2021.**

The practical exam is administered through two different platforms (Moon Cloud and KYPO Cyber Range Platform).
During the course, you were provided with credentials to these platforms.
Before you proceed with the practical exam, **please make sure that they are readily available to you**.
You can run the two parts of the exam in different times and in any sequence within the above mentioned period.

**Please plan your time ahead.** If both parts of the exam are conducted consequently you will need a maximum of 3 hours and 45 minutes.
You have only **one attempt**.

The system will **not display any results at the end**. Your performance will be manually evaluated based on the criteria of each platform.

After a period of 10 days (counting from the 14th of July 2021), you will be **informed via email** about your performance in the practical part of the $C^3$ by CONCORDIA certification exam.

I wish you the best of luck!
Best regards

Figure B5: Invitation to participate in the practical exam part 2

The number of participants in the practical exams was 7 (out of a total of 10 applications). KYPO CRP uses a level-based approach combining hands-on exercises with tests (single/multiple choice).

The relevant tests were evaluated with no negative points. The hands-on exercise allows 5 attempts for the correct answer. After that solution is displayed and candidate gets 0 points for the exercise.
The scoring of the activities on the Moon Cloud platform, were based on the implementation of specific tasks and on the provision of the relevant responses to questions posed in an online document.

**Quality review**
A quality review was performed on the questions that participated in the theoretical exam based on the performance of the candidates and their comments in the feedback section. The quality review was carried out by TÜV TRUST IT GmbH and EIT Digital.
As it can be seen in the Table A2 below, a number of questions were not answered correctly by any of the candidates, indicating in most cases that the questions should at least be revisited and if needed be corrected / improved or replaced.

| ID | QUESTION | OCCURANCE | SUCCESS | DIFFICULTY |
|---|---|---|---|---|
| CYBEN0010 | Question 10 | 1 | 0% | High |
| CYBEN0012 | Question 12 | 1 | 0% | High |
| CYBEN0051 | Question 51 | 1 | 0% | High |
| CYBEN0080 | Question 80 | 1 | 0% | Easy |
| CYBEN0133 | Question 133 | 1 | 0% | High |
| CYBEN0167 | Question 167 | 1 | 0% | Medium |
| CYBEN0040 | Question 40 | 2 | 0% | High |
| CYBEN0113 | Question 113 | 2 | 0% | High |
| CYBEN0106 | Question 106 | 3 | 0% | Easy |
| CYBEN0163 | Question 163 | 3 | 0% | Easy |
| CYBEN0059 | Question 59 | 4 | 0% | High |
| CYBEN0123 | Question 123 | 4 | 0% | Medium |
| CYBEN0154 | Question 154 | 4 | 0% | Easy |
| CYBEN0019 | Question 19 | 5 | 0% | Medium |
| CYBEN0121 | Question 121 | 5 | 0% | Medium |
| CYBEN0168 | Question 168 | 5 | 0% | Medium |
| CYBEN0107 | Question 107 | 6 | 0% | Easy |
| CYBEN0155 | Question 155 | 6 | 0% | Easy |

Table B2: Questions rejected as a result of the quality review

The questions with the worst performance (e.g., 0% success in multiple occurrences) were not taken into consideration in the overall score of the participants and are now reviewed by the applicable parties.
The provisional results of the theoretical exams were re-evaluated after the completion of the quality review and the final score for this part of the exam was derived per candidate. The number of candidates that passed the theoretical exam after the quality review was eight (8).

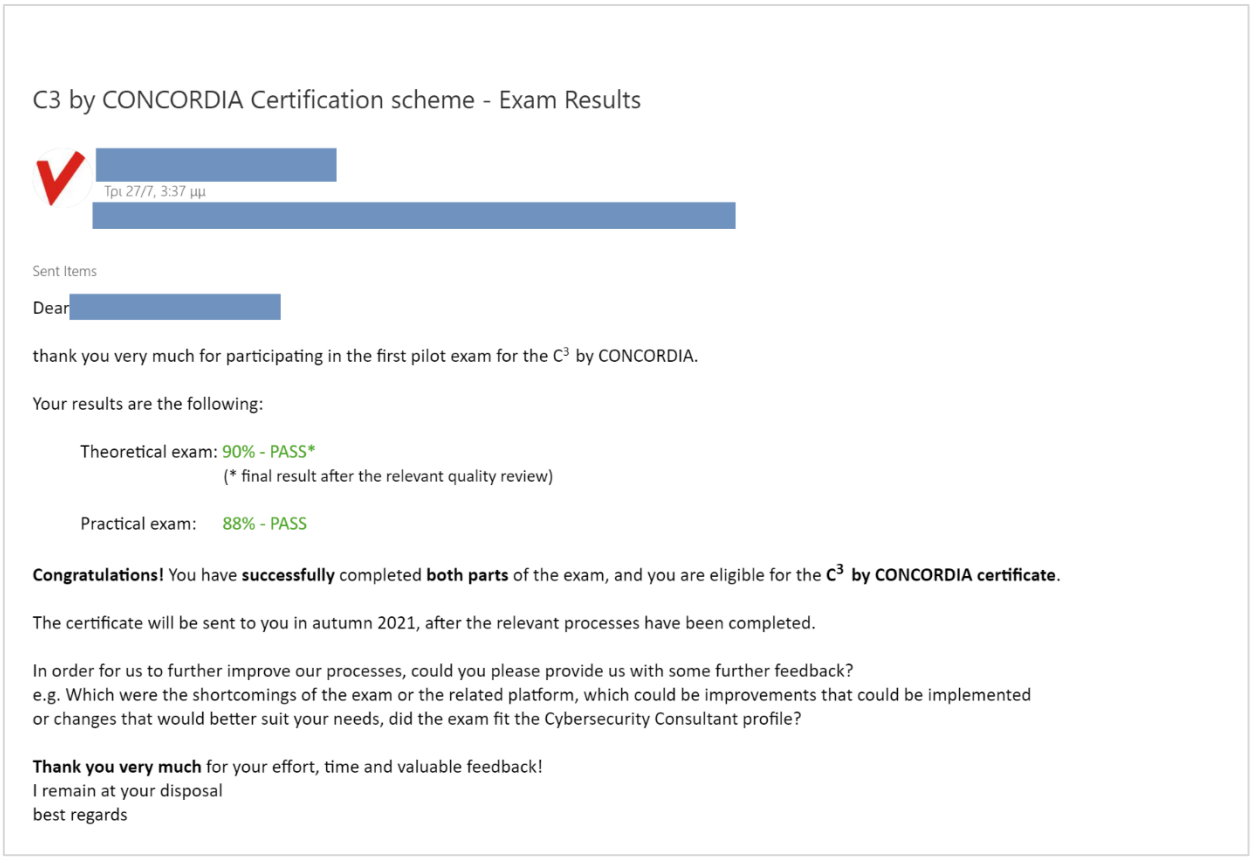
**Practical exam evaluation**
After the time period of the practical exam had elapsed, the evaluation process started. The evaluation responsible for each platform (KYPO and MoonCloud) was contacted and carried out the appropriate evaluation and scoring of the respective attempts taking into consideration the following:

- The correct completion of each prescribed action and
- The duration of each attempt.

All of the participants passed the practical exams. The Average score for people that passed the practical exam was 90%.

**Final results**
After the completion of the theoretical and practical exams, the participants were informed via email about their performance in the exams.

Six (6) of the participants successfully passed the $C^3$ by CONCORDIA PILOT certification exam.



C3 by CONCORDIA Certification scheme - Exam Results

[redacted]
Τρι 27/7, 3:37 μμ
[redacted]

Sent Items

Dear [redacted]

thank you very much for participating in the first pilot exam for the C³ by CONCORDIA.

Your results are the following:

Theoretical exam: 90% - PASS*
(* final result after the relevant quality review)

Practical exam: 88% - PASS

**Congratulations!** You have **successfully** completed **both parts** of the exam, and you are eligible for the **C³ by CONCORDIA certificate**.

The certificate will be sent to you in autumn 2021, after the relevant processes have been completed.

In order for us to further improve our processes, could you please provide us with some further feedback?
e.g. Which were the shortcomings of the exam or the related platform, which could be improvements that could be implemented or changes that would better suit your needs, did the exam fit the Cybersecurity Consultant profile?

**Thank you very much** for your effort, time and valuable feedback!
I remain at your disposal
best regards

C3 by CONCORDIA Certification scheme - Exam Results

[redacted]
Τρι 27/7, 3:37 μμ
[redacted]

Sent Items

Dear [redacted]

thank you very much for participating in the first pilot exam for the C³ by CONCORDIA.

Your results are the following:

Theoretical exam: 90% - PASS*
(* final result after the relevant quality review)

Practical exam: 88% - PASS

**Congratulations!** You have **successfully** completed **both parts** of the exam, and you are eligible for the **C³ by CONCORDIA certificate**.

The certificate will be sent to you in autumn 2021, after the relevant processes have been completed.

In order for us to further improve our processes, could you please provide us with some further feedback?
e.g. Which were the shortcomings of the exam or the related platform, which could be improvements that could be implemented or changes that would better suit your needs, did the exam fit the Cybersecurity Consultant profile?

**Thank you very much** for your effort, time and valuable feedback!
I remain at your disposal
best regards

Figure B6: Communication of the results to the participants

**Feedback**

At the end of the exam, all participants were given the opportunity to send their comments and observations via email. All comments were collected and recorded.
The received comments can be split in the following categories:

- General comments – 3 comments
- Theoretical Exams comments – 2 comments
- Practical Exams comments – 8 comments
- Questions Related comments – 2 comments

The comments and other feedback will be reviewed by the applicable partners and improvements will be implemented prior to the next iteration of the $C^3$ by CONCORDIA Certification exam.

# Annex BA. The C³ by CONCORDIA certification application

CONCORDIA
Cyber security cOmpeteNce fOr Research anD Innovation

## Cyber Security Consultant Certification Application Form

| Applicant's Information<br>*Fields with an asterisk (*) are mandatory* | |
|---|---|
| Last Name* | |
| First Name* | |
| Mobile Number* | |
| Email Address* | |
| Company | |
| Position | |

## Information for the Applicant

*By filling in this application (for the participation in the examination of the certification scheme C³ by CONCORDIA) you are informed and agree to the following:*

- The applicant recognizes that the Certification provided by *CONCORDIA* does not substitute in any case any professional license required by the applicable legislation.
- The applicant possesses the following minimum pre-requisites as stipulated by the Certification Scheme of *C³ by CONCORDIA*:
  1. Successful attendance of the CONCORDIA online module for the Cybersecurity Consultant (more information regarding the Course "Becoming a Cybersecurity Consultant" at https://www.concordia-h2020.eu/becoming-a-cybersecurity-consultant/ ).
  2. Attendance of the CONCORDIA Face-to-Face/webinar part for the Cybersecurity Consultant (more information regarding the Course "Becoming a Cybersecurity Consultant" at https://www.concordia-h2020.eu/becoming-a-cybersecurity-consultant/ ).
  3. 3 years of practical experience in the subject of Cybersecurity (Including but not limited to Cybersecurity Consulting, Cybersecurity Management etc) or a relevant Post-graduate Academic Degree.*
- The applicant will be invited to sit two subsequent exams: one theoretical exam and one practical exam, both ran on specialized platforms.
- The applicant will abide to the rules of the platforms utilized during the two parts of the examination.
- After the successful completion of the examinations, the applicant will be asked to agree to the Declaration of Honor of the Cybersecurity Consultant, in order to complete the certification process. (more information about the certification scheme can be found at https://www.concordia-h2020.eu/becoming-a-cybersecurity-consultant/.

*Note: The relevant information stated here will not be collected by the CONCORDIA project, for the first pilot run of the examination. (see relevant dates below). If you do not fulfil all requirements, please refrain from filling in the application.

CONCORDIA project (https://www.concordia-h2020.eu/) receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 830927.

# Cyber Security Consultant Certification Application Form

## Instructions for the Applicant

*For the participation in the examination of the certification scheme C³ by CONCORDIA, the following instructions must be considered by the applicants, prior to submitting their application.*

- The personal data of applicants and certified professionals remain confidential throughout the whole Certification process (from receiving the application until the issue of the certificate and its maintenance). For any further explanation, you may contact the Data Protection Officer (DPO) of FORTH by sending an e-mail at **dpo@admin.forth.gr**.
- In order to participate in the next examination of the C³ by CONCORDIA certification scheme, the applicant must submit the signed application 5 working days before the date of the examination at the latest.
- *CONCORDIA* processes the applications and informs the applicants on time (3 working days before the examination at the latest), about their eligibility to participate to the examination and about the time and place of the examination.
- *CONCORDIA* holds the right to change the date of examination. In this case, the interested parties will be informed by telephone or e-mail.
- The Certification Proctor Manual for the theoretical exam can be found at https://www.concordia-h2020.eu/wp-content/uploads/2021/04/TOSA-Online-Proctor-Manual.pdf
- General instruction to access the platform for the practical exam can be found at:
- https://docs.crp.kypo.muni.cz/user-guide-basic/training-agenda/training-run/linear-training-run/#training-runs-overview

| Full Name | Signature | Date |
|---|---|---|
| | | |

CONCORDIA project (https://www.concordia-h2020.eu/) receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 830927.

# Annex BB. Instructions to the practical exam

CONCORDIA

## Cyber Security Consultant Certification
## C³ by CONCORDIA Pilot Certification
## Instructions to the Practical Exam

Dear Participant!

Congratulations for completing the theoretical part of the C³ by CONCORDIA pilot certification exam.

Below you may find instructions regarding the practical part of the C³ by CONCORDIA pilot certification exam.

The objective of the practical exam is to evaluate that you possess the necessary skills and abilities introduced and practiced during the relevant course and deemed as necessary to successfully carry out the role of the Cybersecurity Consultant.
(Details on the most important skills can be found at the dedicated CONCORDIA page https://www.concordia-h2020.eu/becoming-a-cybersecurity-consultant/).

The practical exam is administered through two different platforms (KYPO Cyber Range Platform and Moon Cloud).
During the webinar held on 11-13 of May, you were provided with credentials to these platforms.
Before you proceed with the practical exam you need to make sure that they are readily available to you.

The practical exam can be completed between the following time period:
30/06/2021 – 14/07/2021
The two parts require a maximum of 3 hours and 45 minutes to complete if taken consequently. Please read the following instructions and plan your time accordingly. Keep in mind that only one attempt per exam platform is allowed.

Part A. KYPO Cyber Range Platform

Part A, contains a number of Practical Exercises on Penetration testing and Source Code Auditing implemented through the KYPO Cyber Range Platform.
After logging into the platform, you will be required complete 15 tasks/questions on penetration testing and 5 questions on source code auditing.
When you are ready to begin, please log in to KYPO CRP at
with your credentials and put toke to the form. Your exam will start right away after submitting the form.
You will have a maximum of 105 minutes (1 hour and 45 minutes) to complete this part of the exam. You have only one attempt. Although the platform will not discontinue your session, the duration of the attempt is recorded and will be evaluated afterwards for compliance to the 1 hour and 45 minutes limit. Only actions within this limit will be evaluated.

For any issues with the KYPO platform, please, contact
The evaluation of your performance will be implemented through the KYPO CRP.

Part B. Moon Cloud

CONCORDIA project (https://www.concordia-h2020.eu/) receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 830927.

# Cyber Security Consultant Certification
# C³ by CONCORDIA Pilot Certification
# Instructions to the Practical Exam

Part B, contains a number of Practical Exercises and questions implemented through the use of the Moon Cloud platform (the questions and their answers are facilitated through Google Forms.
When you are ready to begin, please log in to Moon Cloud at [redacted] with your credentials. Your timer will start after this log on.
Open the google form at [redacted]
Please follow the instructions listed at the top of the google form regarding the scenario to be implemented in Moon Cloud.
Some best practices for the work implemented in Moon Cloud:

- Work in a new, blank, project.
- Create the zones and the targets before executing any evaluation. You might need to register the same target multiple times but of different types.
- Execute only the evaluations which are strictly required by the exam.
- If you do not immediately see the output of something you have done (e.g., target creation), just refresh the page may solve the problem. For what concerns evaluations, you may have to wait a little to see results.

The scenario used resembles the one introduced during the course (ACME company) for your convenience.

You will have a maximum of 120 minutes (2 hours) to complete this part of the exam. You have only one attempt. Although the platform will not discontinue your session, the duration of the attempt is recorded and will be evaluated afterwards for compliance to the 2 hour limit. Only actions within this limit will be evaluated.
For any issues with the Moon Cloud platform, please, contact [redacted]
After you finish your attempt, log off from Moon Cloud and submit your answers on Google Forms.

You may implement the parts at any order you wish and is convenient to you. Please be aware that you have only one continuous attempt for each part. You may choose to take each part on the same day or on different days, consequently or at different time.

The system will not display any results at the end. Your performance will be manually evaluated based on the criteria of each platform.

After a period of 10 days, you will be informed via email about your performance in the practical part of the C³ by CONCORDIA pilot certification exam.

Thank you very much for participating!
Good luck!

CONCORDIA project (https://www.concordia-h2020.eu/) receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 830927.

# Annex C. Cybersecurity MOOC Certification Information

CONCORDIA and CyberSec4Europe projects collaborated in order to provide initial answers to the following questions:

RQ1: How do (cybersecurity) MOOC stakeholders value a certificate as a selection criteria and what should such a certificate convey?
RQ2: What challenges have current (cybersecurity) MOOC stakeholders experienced?
RQ3: What quality criteria do stakeholders want to be included in a certification scheme for addressing such challenges?

For answering the above mentioned questions an online survey was conducted. Approval for this study was provided by one of the Ethical Advisors at Karlstad University. Survey participation was voluntary. The survey was announced in January and February 2021 via various cybersecurity mailing lists, and was thus addressing cybersecurity experts.

3.1. Study design
The online survey questions are based on a selection of MOOC quality criteria, which were published in a relevant publication[50], structured in categories and further processed in order to better address the objectives / questions.
The survey consisted of 72 Questions in total structured as shown in the following table[51]:

TABLE 1: Categories of questions

| Part | n | Scale | Topic |
|---|---|---|---|
| Demographics | 8 | Mixed | Demographic information |
| Part A | 11 | Quantitative | Former experiences with MOOCs |
| Part B | 5 | Likert | Criteria that factor in the selection of a specific MOOC |
| Part C | 6 | Likert | Which are the statements or properties that should be conveyed by a MOOC Certificate? |
| Part D1 | 20 | Quantitative | Challenges encountered by the participants during their MOOC experience. Five of the questions are specific for Cybersecurity MOOCs and only appear when such a participation is confirmed |
| Part D2 | 20 | Likert | Quality aspects that should be included in a (Cybersecurity) MOOC Certification for addressing these challenges? |
| Part E1 | 1 | Text | Other challenges (optional); What other challenges could be addressed by a relevant certification scheme? |
| Part E2 | 1 | Text | Email address (optional - for being contacted for further feedback) |

The results and conclusions drawn from the survey are included in the relevant publication[16], and are also mentioned in section 4.3.1.2. Activity 1.

[50] S. Fischer-Hubner, M. Beckerle, A. L. Lafuente, A. R. Mart ¨ ´ınez, K. Saharinen, A. Skarmeta, and P. Sterlini, “Quality criteria for cyber security moocs,” in IFIP World Conference on Information Security Education. Springer, 2020, pp. 46–60
[51] M. Beckerle, A. Chatzopoulou and S. Fischer-Hübner, "Towards Cybersecurity MOOC Certification," 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2021, pp. 1-11, doi: 10.1109/EuroSPW54576.2021.00008.

MOOC Certification Survey

jointly organized by

CONCORDIA

Cyber Security for Europe

**Introduction**

The acronym MOOC stands for Massive Open Online Course. What is hidden behind these words are frameworks that provide online, accessible, collaboration and learning spaces were learners can participate in a training course, can interact with other students, can complete assignments etc. MOOCs courses still contain the basic characteristics of the traditional courses (e.g. training material, instructor, participants etc) without having to obey to the traditional constraints (e.g. location, participation etc).

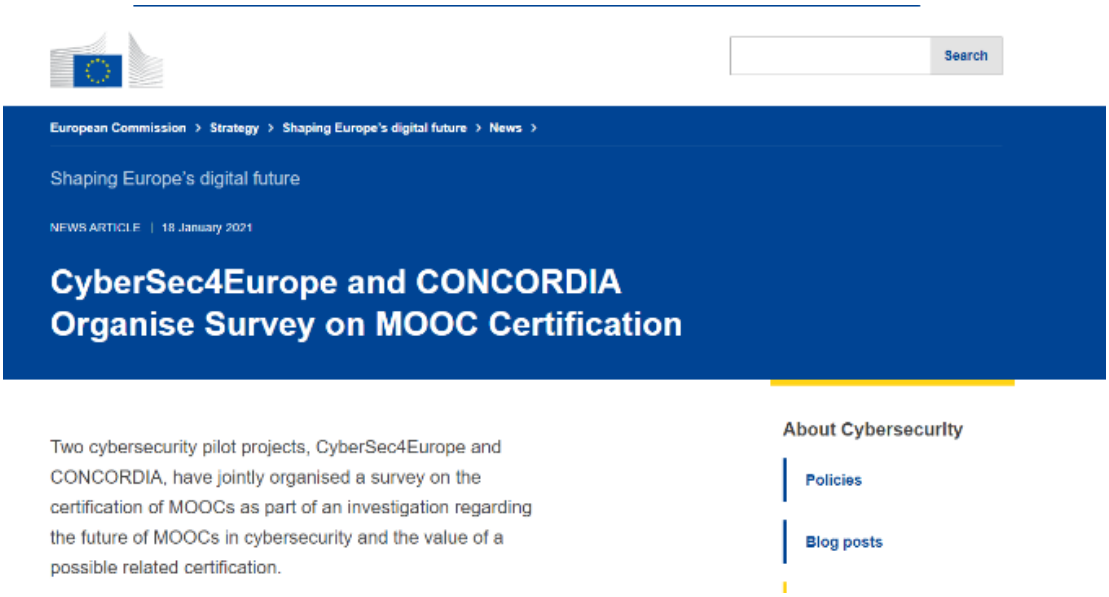
Although 2012 was named "The Year of the MOOC" (https://www.classcentral.com/report/mooc-hype-year-1/), the year 2020 and the COVID-19 crisis, have given an unprecedented rise to MOOC participation. It is worth mentioning that "three MOOC providers (Coursera, edX, and FutureLearn) registered **as many new** users in **April 2020** as in the **whole of 2019**. [To give you an idea of the sheer volume: The new users registered (in four platforms) within 2020 amounted to 32.7 Millions representing an increase of more than 120% from the relevant number of 2019]. (https://www.classcentral.com/report/mooc-stats-pandemic/)

To this moment there are hundreds of MOOCs and the industry is expected to grow at a rate of at least 40% within the next seven years (https://www.databridgemarketresearch.com/reports/global-mooc-market#).

MOOCs have been implemented for a variety of subjects, one of which is Cybersecurity. With the cybersecurity skills gap in Europe still existing, such implementations are increasingly interesting.

With MOOC utilization undergoing such a hype and the provided solutions being numerous, this survey aims to identify whether there is a need for further standardization of (Cybersecurity) MOOC implementations and whether a possible certification scheme would have an added value to the learner, the offering institution or any other interested party.

Figure C1: Screenshot of the first page / introduction of the survey



Search

European Commission > Strategy > Shaping Europe's digital future > News >

Shaping Europe's digital future

NEWS ARTICLE | 18 January 2021

**CyberSec4Europe and CONCORDIA Organise Survey on MOOC Certification**

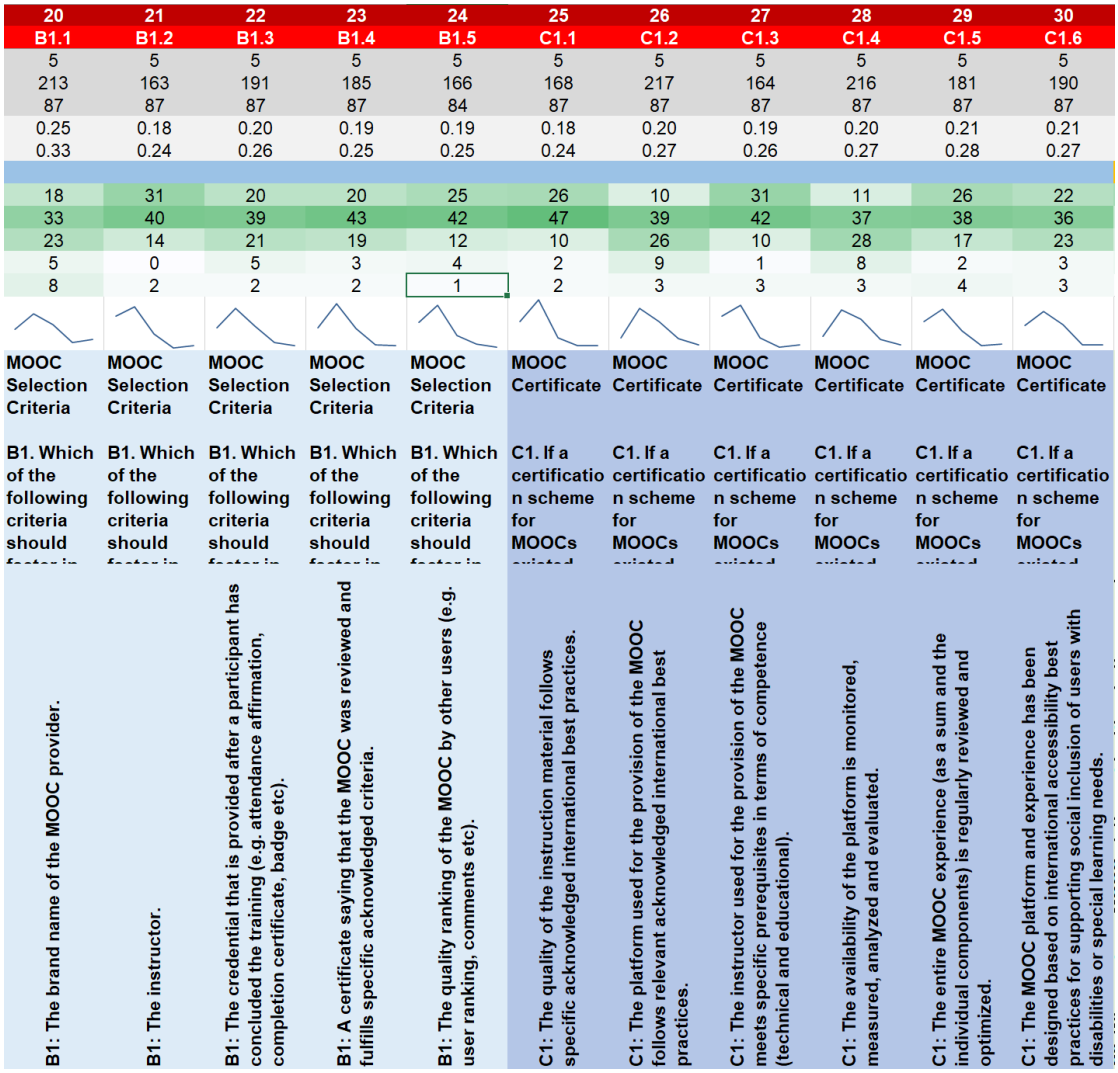
Two cybersecurity pilot projects, CyberSec4Europe and CONCORDIA, have jointly organised a survey on the certification of MOOCs as part of an investigation regarding the future of MOOCs in cybersecurity and the value of a possible related certification.

About Cybersecurity

Policies

Blog posts

Figure C2: Screenshot of the announcement of the Survey outside the projects



| 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
|---|---|---|---|---|---|---|---|---|---|---|
| B1.1 | B1.2 | B1.3 | B1.4 | B1.5 | C1.1 | C1.2 | C1.3 | C1.4 | C1.5 | C1.6 |
| 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| 213 | 163 | 191 | 185 | 166 | 168 | 217 | 164 | 216 | 181 | 190 |
| 87 | 87 | 87 | 87 | 84 | 87 | 87 | 87 | 87 | 87 | 87 |
| 0.25 | 0.18 | 0.20 | 0.19 | 0.19 | 0.18 | 0.20 | 0.19 | 0.20 | 0.21 | 0.21 |
| 0.33 | 0.24 | 0.26 | 0.25 | 0.25 | 0.24 | 0.27 | 0.26 | 0.27 | 0.28 | 0.27 |
| | | | | | | | | | | |
| 18 | 31 | 20 | 20 | 25 | 26 | 10 | 31 | 11 | 26 | 22 |
| 33 | 40 | 39 | 43 | 42 | 47 | 39 | 42 | 37 | 38 | 36 |
| 23 | 14 | 21 | 19 | 12 | 10 | 26 | 10 | 28 | 17 | 23 |
| 5 | 0 | 5 | 3 | 4 | 2 | 9 | 1 | 8 | 2 | 3 |
| 8 | 2 | 2 | 2 | 1 | 2 | 3 | 3 | 3 | 4 | 3 |
| MOOC Selection Criteria | MOOC Selection Criteria | MOOC Selection Criteria | MOOC Selection Criteria | MOOC Selection Criteria | MOOC Certificate | MOOC Certificate | MOOC Certificate | MOOC Certificate | MOOC Certificate | MOOC Certificate |
| B1. Which of the following criteria should | B1. Which of the following criteria should | B1. Which of the following criteria should | B1. Which of the following criteria should | B1. Which of the following criteria should | C1. If a certification scheme for MOOCs | C1. If a certification scheme for MOOCs | C1. If a certification scheme for MOOCs | C1. If a certification scheme for MOOCs | C1. If a certification scheme for MOOCs | C1. If a certification scheme for MOOCs |
| B1: The brand name of the MOOC provider. | B1: The instructor. | B1: The credential that is provided after a participant has concluded the training (e.g. attendance affirmation, completion certificate, badge etc). | B1: A certificate saying that the MOOC was reviewed and fulfills specific acknowledged criteria. | B1: The quality ranking of the MOOC by other users (e.g. user ranking, comments etc). | C1: The quality of the instruction material follows specific acknowledged international best practices. | C1: The platform used for the provision of the MOOC follows relevant acknowledged international best practices. | C1: The instructor used for the provision of the MOOC meets specific prerequisites in terms of competence (technical and educational). | C1: The availability of the platform is monitored, measured, analyzed and evaluated. | C1: The entire MOOC experience (as a sum and the individual components) is regularly reviewed and optimized. | C1: The MOOC platform and experience has been designed based on international accessibility best practices for supporting social inclusion of users with disabilities or special learning needs. |

Figure C3: Screenshot of the analysis of raw data of the Survey


Figure C4: Screenshot of the page of the Second International Workshop On Cybersecurity Certification, 6th IEEE European Symposium on Security and Privacy

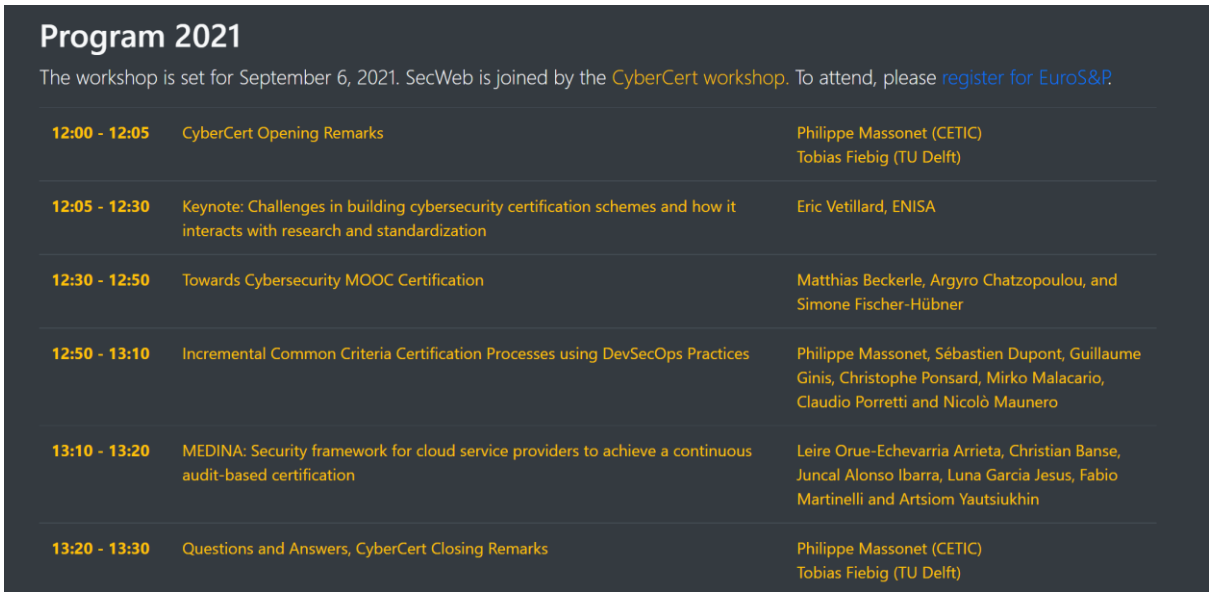



Figure C5: Screenshot of the workshop program

# List of Acronyms

| | |
|---|---|
| **ANCE** | National Association of Standardization and Certification |
| **ANSI** | American National Standards Institute |
| **ASTM** | American Society for Testing and Materials |
| **CA** | Consortium Agreement |
| **CSA** | Cloud Security Alliance |
| **CSRC** | Computer Security Resource Center |
| **DIN** | Deutsches Institut für Normung |
| **DoA** | Description of Action |
| **EC** | European Commission |
| **ECCC** | European Cybersecurity Competence Centre |
| **ER** | Exploitable Result |
| **ETSI** | European Telecommunications Standards Institute |
| **EU** | European Union |
| **FDA** | Food And Drug Administration |
| **GA** | Grant Agreement |
| **GSMA** | Groupe Speciale Mobile Association |
| **IEC** | International Electrotechnical Commission |
| **IEEE** | Institute of Electrical and Electronics Engineers |
| **IETF** | Internet Engineering Task Force |
| **IoC** | Indicator of Compromise |
| **ISA** | International Society of Automation |
| **ISO** | International Organization for Standardization |
| **ITU** | International Telecommunication Union |
| **NASA** | National Aeronautics and Space Administration |
| **NATO** | North Atlantic Treaty Organization |
| **NCCOE** | National Cybersecurity Center of Excellence |
| **NEMA** | National Electrical Manufacturers Association |
| **NERC** | North America Electric Reliability Center |
| **NFPA** | National Fire Protection Association |
| **NIST** | National Institute of Standards and Technology |
| **oasis-open** | Organization for the Advancement of Structured Information Standards |
| **SAE** | Society of Automotive Engineers |
| **TRL** | Technology Readiness Level |
| **UL** | Underwriters Laboratories |
| **WP** | Work Package |

(The above list contains the most frequently used acronyms. More acronyms are included in line with their description as needed.)