R5.5.2
Cybersecurity SSA Network building/Campaign Assessment Report

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Title	R5.5.2 Cybersecurity SSA Network building/Campaign Assessment Report
Document description	This document identifies, documents and promotes best and good practices aiming at addressing cybersecurity skills and shortages as well as fostering multi-stakeholder partnerships.
Nature	Public
Task	T5.5 Cybersecurity SSA Network building/Campaign
Status	Final
WP	WP5
Lead Partner	EfVET
Partners Involved	All
Date	26/08/2024

Revision history	Author(s)	Delivery date	Summary of changes and comments
Version 01	Paolo Nardi (EfVET) Ibon Rejas (EfVET)	25/08/2024	Draft for partners' comments
QA Review	Simas Grigonis (MRU) and Daiva Banaitė (EKT)	06/09/2024	REWIRE Quality Assurance Review
Final Version	Paolo Nardi (EfVET) and Enrique Blanco (EfVET	16/09/24	Final adjustments based on QA review

Disclaimer:

CONTENTS

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

1. INTRODUCTION

The REWIRE project, among its several tasks and expected results, has implemented a campaign aimed to build awareness and to augment the SSA (Sector Skills Alliance) Network on cybersecurity over the last 24 months. This task (T5.5. Cybersecurity SSA Network building/Campaign), under EfVET's coordination, consisted of 3 rounds of 11 national events, starting in the Autumn 2023 and concluding at the beginning of the Summer 2024.

The SSA bears a unique advantage of having already an increased circle of influence, since it is supported by the four pilots (CONCORDIA, ECHO, SPARTA, CYBERSEC4EUROPE). Despite this advantage, the project team planned to create campaigns targeting stakeholders representing different viewpoints (e. g: business, trade unions, research institutions, education and training institutions, public authorities, professional bodies, certification bodies, accreditation councils, and others). Beside the partners of the REWIRE project, the impact and reach of these campaigns was further enhanced by several stakeholders and organizations that have explicitly declared their support to the project and interest in the results, since the beginning. The REWIRE partners have been collaborating with Cyberwatching.eu, the European observatory of research and innovation in cybersecurity and privacy. Through the network and actions of Cyberwatching.eu, the project was further promoted since its start. In the second half of the project, REWIRE joined the Pact for Skills and the Digital Large-Scale Partnership (DLSP), becoming a reference point for Cybersecurity in most of their events (cfr. DLSP matchmaking events, R5.6.1 National Cybersecurity Events List).
The results of these events aimed at campaigning the Cybersecurity SSA and building/reinforcing its network of stakeholders have been collected, documented, reported and, when the case, contributed to the improvement of the project thanks to experts' feedback or emerging needs for improvement.
EFVET, as task leader, had 30+ reports, one for each event, collected and summarized in a final report (R5.5.2) to document the impact of this activity.
The following sections aim at disseminating the purpose of these events/meetings (section 2); introducing the reader to the template distributed to collect those essential elements about every single event (section 3); providing an overview on the 3 rounds of National events (section 4-6). A final section will offer a summary and potential implications.

2. CYBERSECURITY SSA NETWORK BUILDING/ CAMPAIGN: GOAL AND METHOD

The focus of the task T5.5 Cybersecurity SSA Network Building and Campaigns consists of a series of national initiatives led by REWIRE partners (associated per country) to advocate for the project and its results and to promote its tools, namely the four online courses dedicated to the training on relevant skills in the cybersecurity sector.
Most relevant targets for these events have been Education and Training providers; Higher Education Institutions; VET Networks; Umbrella Associations; Policymakers; Industrial Companies and their Associations; Research Institutes; Certification and Standardization Bodies; End Users; ICT Professionals.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

The importance of campaigns for raising awareness has been clear to the partners since the beginning of the project: mapping and analysis of Cybersecurity Awareness Campaigns was already conducted via specific databases (please, also cfr. REWIRE, R3.4.1), bringing to highlight a total of 37 practices (in 23 countries). An overview on these practices (43, after being integrated with some examples based on further desk research) has been proposed to the list of stakeholders of the REWIRE project who have been requested to provide feedback in terms of relevance and transferability. The results of this analysis have been published in the R5.3.5 REWIRE Fiche V.
The events have been carried out according to a specific methodology and a clear roadmap:

- One Info Day organized in each partner country in M25, one month after the Blueprint development;
- One Info-day organised in each partner country in M36, one month before the official launch of the 1st round of the REWIRE courses, with the aim of attracting as many participants to the REWIRE MOOCs as possible.
- One Info-day will be organised in each partner country in M42, one month before the official launch of the 2nd round of the REWIRE courses, with aim to attract as many participants to the REWIRE MOOCs as possible and launching this product to the community of cybersecurity experts and stakeholders.

For each round of events, a calendar was also created on an excel file to collect the most essential info related to the country, partners involved, date and venue of the event, main goals, expected number and type of participants.

3. METHODOLOGY AND STRUCTURE OF THE REPORT

As previously mentioned, EfVET has been in charge of coordinating and monitoring the organization of the National events (or Info Days). Part of its responsibility was then to invite every partner to fill in a post-event report and check the information.
Making reports after these events has been crucial to the overall effectiveness, accountability, and continuous improvement of the project itself and its deliverables. The aims of the reports include:

- Evaluating Success and Measuring Impact
    - Assessment of Goals: Post-event reports should help determine whether the event met its initial objectives and goals, such as attendance numbers, participant engagement, or knowledge dissemination.
    - Impact Measurement: They had to provide data on the impact of the event on participants and stakeholders, such as increased awareness, knowledge gained, or the formation of new partnerships.
    - Data Collection: Reports aimed at collecting quantitative and qualitative data that can help measure the success and effectiveness of the event.

- Gathering Feedback and Insights

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

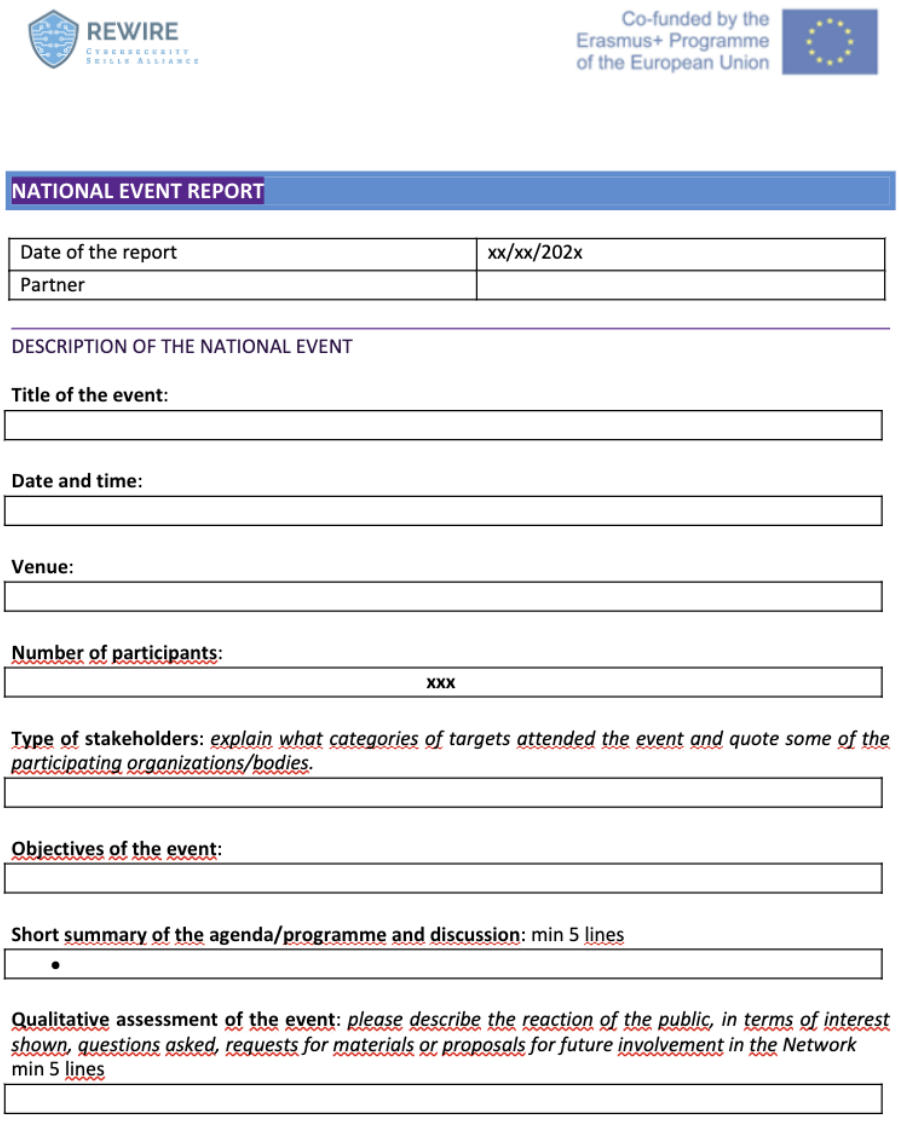
- Understanding Audience Reaction: Reports were asked to include feedback from participants, which can provide insights into what was well received and what needs improvement.
- Identifying Strengths and Weaknesses: By analyzing feedback, organizers were helped to identify which aspects of the event were most effective and which were less successful or could be improved.

Above all, these reports were essential for:

- Enhancing Accountability and Transparency:
  Event reports served as official documentation of what transpired, providing a detailed account of the event for stakeholders and partners, helping EfVET in its monitoring work.
- Facilitating Communication and Follow-Up:
  EfVET and EVTA could widely use information emerging from reports to produce dissemination and communication materials to facilitate follow-up, further engagement with participants, or addressing any issues raised, contributing to the network building with participants, stakeholders, and partners.

To fulfill those expectations, REWIRE partners realized a template (fig. 1) which every National coordinator partner would have to fill after the event and share in a common folder on Teams.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE Cybersecurity Skills Alliance
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union



REWIRE Cybersecurity Skills Alliance

Co-funded by the Erasmus+ Programme of the European Union

NATIONAL EVENT REPORT

Date of the report	xx/xx/202x
Partner	

DESCRIPTION OF THE NATIONAL EVENT

Title of the event:

Date and time:

Venue:

Number of participants:

xxx

Type of stakeholders: *explain what categories of targets attended the event and quote some of the participating organizations/bodies.*

Objectives of the event:

Short summary of the agenda/programme and discussion: min 5 lines

•

Qualitative assessment of the event: *please describe the reaction of the public, in terms of interest shown, questions asked, requests for materials or proposals for future involvement in the Network* min 5 lines

Potential impact of the event on your organisation or at the local/national level: min 3 lines

Other info (if applicable):

Figure 1: template for the post-event report

In summary, making these reports after the events has been important for a comprehensive evaluation of the events' success, facilitating continuous improvement, ensuring accountability, and helping EfVET in the strategic planning and monitoring, including the realization of this final report.

4. FIRST ROUND

The first round of the Cybersecurity SSA Network building/Campaign events were focused on the European Cybersecurity Blueprint elaborated in the WP3.

4.1. CONTENT

Events gave the partners first the possibility to offer participants a framework of what the Blueprint is, namely a key initiative to create new strategic approaches and cooperation for concrete skills development solutions in the industrial ecosystems as introduced by the updated EU industrial policy. Like each Blueprint project, REWIRE developed a sectoral skills strategy to support the overall growth strategy for the industrial ecosystem and skills needs, with a focus on cybersecurity.
Following this strategy, the partners could identify priorities and milestones for action and develop concrete solutions, such as creating and updating curricula and qualifications based on changing or new occupational profiles (as in WP4).
In most of the events, REWIRE partners shared the activity of the first 24 months of the project, namely the analysis of the already existing cybersecurity skills frameworks from various sources (national, international, public, private) and documented in the Deliverable R2.2.2. Cybersecurity Skills Needs Analysis and the R5.4.1 Policy Recommendations.
The events also documented the dramatic lack of skilled and qualified personnel in the labor market to work in cybersecurity roles, and their relevance for many fields. Based on this emergency, REWIRE partners made clear to the audience of the events:

- the R.2.2.3. Methodology to anticipate future needs where the REWIRE project partners proposed a methodology to facilitate the identification of future needs based also on inputs from specific stakeholders and the market. (fig. 2)
- The tool Cybersecurity Job Ads Analyzer to help in the processing of information form Job ads and the extraction of information on current and emerging skills needs.

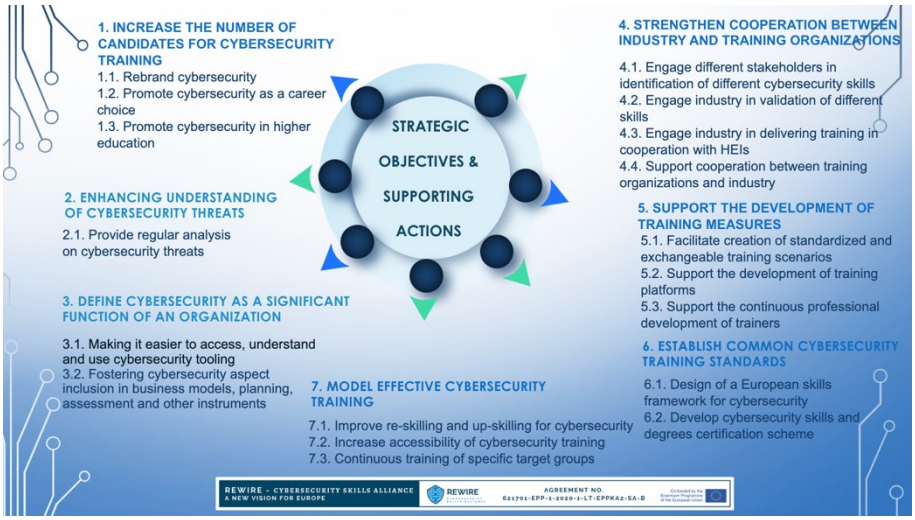


Figure 2: Main objectives for anticipating future needs

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Based on the shared analysis, the events introduced the PESTLE analysis as an essential step toward the Blueprint strategy.

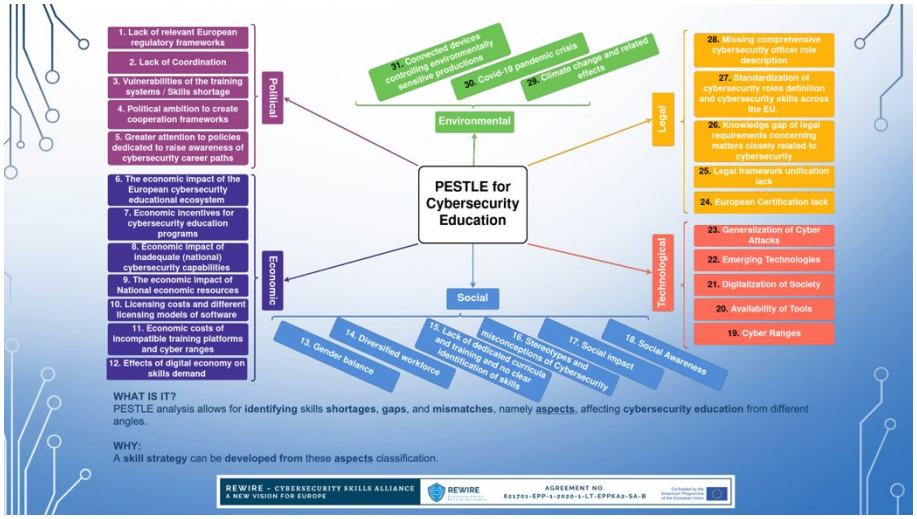


Figure 3: PESTLE analysis

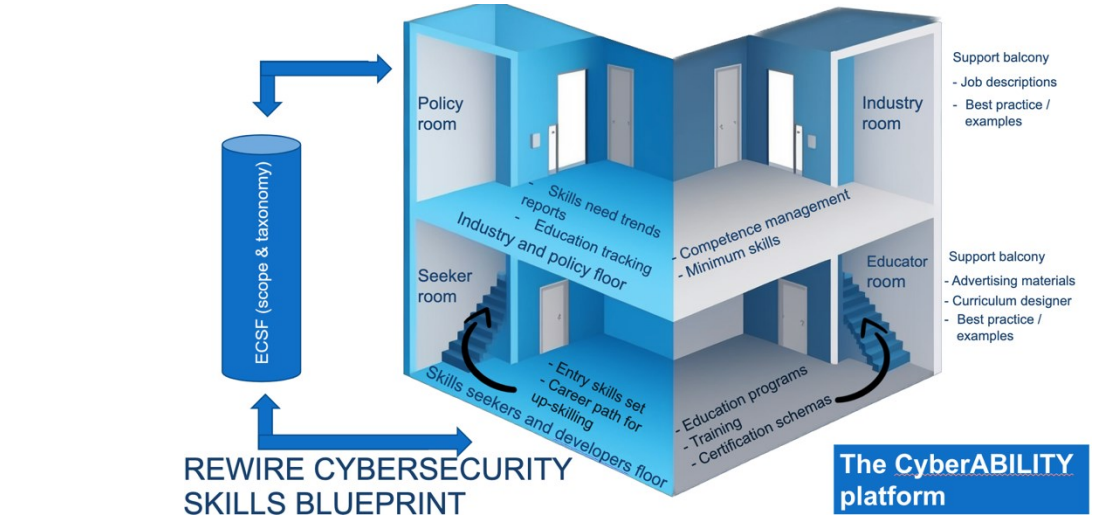


Figure 4: a metaphorical representation of the REWIRE cybersecurity skills blueprint

4.2. EMERGING RESULTS

Eleven events were launched, mainly in the first half of 2023, mostly hybrid. For the implementation of the events, each partner had the flexibility to conduct an in-person, hybrid or online event.

More than 600 participants attended, and in some cases the recorded videos were viewed by additional people (e. g: Lithuanian event). In terms of categories of participants, also in relation to the organizing partner and its network, various types of stakeholders were involved: academics; private sector; policy makers; cybersecurity practitioners, especially the ones at national levels. In the case of the Belgian partners, EU stakeholders

and representatives were involved. The main results, per country, are summarized in the following sections.

Belgium

Through the panel with its distinguished speakers, it was highlighted that cybersecurity should be high on the EU agenda for any schools/colleges/universities with a reliance on IT online systems. The Education sector also needs to review their cybersecurity risk and improve their cyber resilience. In the future of the cybersecurity skills and intelligence, Technical Vocational Education and Training may play a key role in addressing skills gaps and the shortage of the cybersecurity workforce due to the greater exposure of governments, businesses, and individuals to cybersecurity threats.

Cyprus

All panelist speakers highlighted various aspects of the European cybersecurity ecosystem, including the increasing cybersecurity challenges faced by governments, educational institutions, and the public, as well as the shortage of personnel with cybersecurity skills. From the discussion it was clear that there is a pressing need to equip the cybersecurity sector with the right skills and coordinate efforts among stakeholders to address the challenges posed by the continuous digital transformation and increasing cyber threats. The importance of achieving gender equality in the cybersecurity domain was also recognized, since women are underrepresented in this field and various ways to tackle this were mentioned.
Overall, the event provided a comprehensive overview of the European Cybersecurity Blueprint and contributed to increasing cybersecurity awareness.

Czech Republic

The participants showed interest in the project, with one question on possible future collaborations, including the involvement in future networks. The speakers were open to collaboration and provided all the information requested.

France

The event aimed to bring together and animate the French-speaking community of academic and industrial research on cybersecurity. Also, students who attended wanted to know about its development.
The presentation was generally well perceived, here are some comments:

- Lots of interest in the Job analyzer tool, especially for jobs that are related to researcher profile.
- Questions regarding the difference between REWIRE and other pilot projects like Concordia and SPARTA
- The courses on penetration tester profile had a lot of interest and in the jobs tool. Most students liked the fact that it aggregates all jobs across the EU.
- Lots of interest in the KYPO platform and how much access time will be given to users

Greece

Big reach out due to large dissemination in guest speakers' networks: institutional stakeholders (Hellenic Data Protection Authority, Hellenic Authority for Communication Security and Privacy, Hellenic Police – Cybercrime unit) as well as representatives from the Industry and Academia. In the discussion that took place at the end of the event, the guest speakers referred to the challenges and the lack of a tried and tested approach to

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

cybersecurity education. It was, also, highlighted that fearmongering should be avoided when trying to raise awareness about cybersecurity.
There was particular interest from the public regarding certifications - a key point for interdisciplinary cooperation.

Hungary
The participants showed interest in the project, with most of the questions mainly related to the future of REWIRE and the planned courses.

Lithuania
The event indicated a need for such initiatives, since it brought together policy makers, higher education providers and cybersecurity specialists, as well as business to share their experiences with challenges on development of cybersecurity skills in Lithuania. During the event (among other topics) participants engaged into discussion on roots and causes for gender imbalance in the cybersecurity occupation and studies in Lithuania. Participants of the discussion agreed on the need to increase attractiveness of cybersecurity skills at school-level, because females tend to choose not to begin engaging in IT-related studies.

Portugal
The participants showed interest in the project, particularly the tools to be developed for candidates and the courses to be developed and shared by it.
Regarding the analysis of market needs and new trends in cybersecurity, there were also questions regarding the emerging technologies such as Machine Learning, and Large Language Models, their impact in cybersecurity
This event triggered discussions regarding possible cooperation between national universities to provide joint MSc courses enhancing each one's capacity to provide specialized courses.

Serbia
The event was attended by most relevant Serbian stakeholders from the public, private, academic and non-profit spheres. REWIRE representatives presented an ongoing project and engaged in multiple informal discussions with members of the Network. The local experts showed most interest in the REWIRE course development activities conducted in WP4 and offered their expertise if needed. They requested the preliminary versions of the course syllabus and later provided feedback.
The Network meetups allow Serbian cybersecurity stakeholders to discuss ongoing national-level initiatives. This year the event allowed the members to receive updates about the regulatory changes necessary to align with the NIS 2 Directive. Additionally, the participants offered renewed support for the Cyber Hero talent management program in general and the Serbian Cybersecurity Challenge competition in specific.

Spain
The presentation was generally well perceived. It generated great interest in the work undertaken in REWIRE. There was a common perspective that the project is really needed because there is a general problem, especially for the industry, in the current cybersecurity skills gap. There is a huge lack of cybersecurity profiles needed to cover all the required positions and the problem seems to be increasing in time. At an industrial level then it seems completely necessary that we provide tools to align the different cybersecurity ecosystem stakeholders and make it easier to link the job offers with the demanders and

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

the skill trainers (education and academia). It also generated interest on an academic level, with several professors from other Spanish universities interested in REWIRE as an education tool. Students who attended wanted to know when the REWIRE courses and educational (e.g. KYPO cyber-range) and supporting (e.g. job analyzer) tools will be available and how they can access them.
Besides the interest generated in the hall of the Barcelona Cybersecurity Congress, different press releases were published at national level in some of the most well-known Spanish general newspapers, informing about the event and the project, which highly increased the visibility of the event and the work done in REWIRE.

Sweden
The presentation was generally well perceived, most of the comments focused on the Job Analyzing tool, the job profiles and the ENISA cybersecurity skills framework and the cyber-ability platform.
Several participants have expressed interest in the REWIRE project and in the tools being developed. The genuine interest for tools was significantly higher than the interest in taxonomies and frameworks, reflecting the need of the community for pragmatic approaches that improve the security posture of organizations and their awareness, as opposed to holistic frameworks with little impact on systems and organizations.

5. SECOND ROUND

The second round of the Cybersecurity SSA Network building/Campaign events was focused on the launch of the training courses (WP4).

5.1. CONTENT

This second round of National events gave the partners first the possibility to gather stakeholders interested in cybersecurity from various sectors, to show the REWIRE project's achievements, emphasizing the cybersecurity blueprint and, as previously, the emerging and analyzed skills gap.

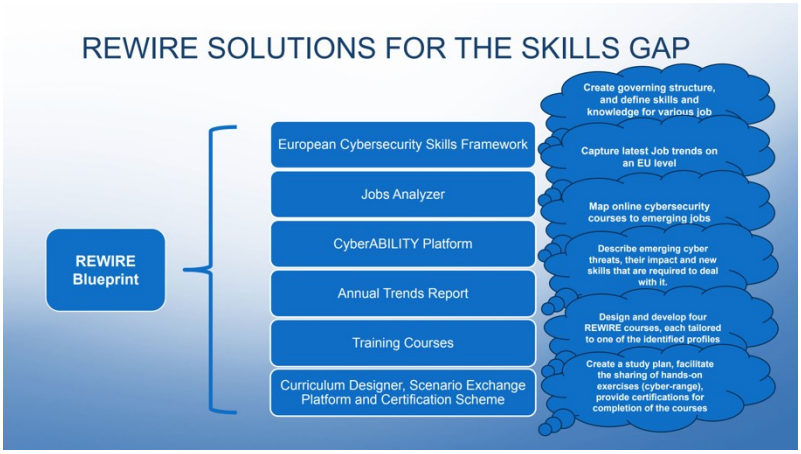


Figure 5: analysis of the skills gap and connection with the REWIRE solutions

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

The solutions to the emerging skills gap have been the focus on this round of events, above all, the upcoming online courses. The links of the virtual learning platform (VLE) for the REWIRE training courses were provided, offering an opportunity to describe the 4 different courses and to engage the audience prior to the launch of the virtual learning platform itself (fig. 6).

Figure 6: connection between profiles, courses and the VLE of the REWIRE project

5.2. EMERGING RESULTS

The second round of T5.5 events was implemented between October and November 2023 and included 10 National meetings, plus an international event organized by EfVET during its conference in Rhodes (October 2023) and a joint event in Belgium by EVTA and EfVET organized under the Lifelong Learning Week initiative (November 2023). Again, most of them were hybrid. Overall, more than 700 participants were involved.

Belgium (EfVET+EVTA event)

The participants attending were really interested and curious to know more. They were interested in enrolling in the courses as well as getting more information about the whole project and more initiatives like REWIRE. They believed that projects like this are relevant for their lives, professional, and personal, and that there should be more and better visibility for these projects. They were all interested in becoming part of the stakeholder's database.

This event increased EfVET and EVTA's visibility on the topics of VET and ICT together. Furthermore, having organized it during the Lifelong Learning Week in Brussels, it gave REWIRE a significant visibility.

Cyprus

There was particular interest from the public regarding the training courses and the opportunities that they will have after the completion of this training and certifications. Specifically, attendees asked a lot of questions such as « when will it be possible to start the course? », « Could we apply for 2 courses? », « is it possible to get an entry level cybersecurity role without 3 years of experience? » etc. Moreover, the presenters received questions from the students about the pathway to follow to build a career in cybersecurity industry «A piece of advice for an undergraduate computer science student wishing to pursue a career in cybersecurity and gain experience in the profession? Also is a Master in cybersecurity enough for an individual to be in the industry? »
New cooperations and potential new «customers» were facilitated.

Czech Republic

The participants showed strong interest in the results of the REWIRE project, mainly in VLE training and certification relevant to the EU Cybersecurity Skills Framework. Direct cooperation with selected stakeholders was also discussed – the cooperation will focus on the testing and implementation of the VLE training at education providers and public institutions. Most participants were asking about the availability of the platform and the role of the REWIRE Cyber Range (KYPO CRP) component in the training.
The main expected impact relates to delivery and testing of the VLE training to the target audience. We confirmed with the stakeholders that they're interested in the results of the project and ready and willing to participate in their dissemination and testing. Main stakeholders for cooperation in this regard are education providers (mainly universities) and Czech National Cyber and Information Security Agency.

France

Interest and positive feedback from the audience regarding the efforts on job profiles and regarding the online courses developed in the REWIRE project. Questions emerged regarding:

- the content of the online courses (including hands-on exercises)
- the certification of the online courses
- the cybersecurity curricula developed in our organization

Promotion/consolidation of our organizations as a key player in cybersecurity was one of the most relevant impacts.

Greece

The audience showed an avid interest in the information provided for the REWIRE project, the ECSF and the European Cybersecurity Challenge. Information was provided by the speakers during their presentation and links were provided through the Teams platform. The actual links of the virtual learning platform (VLE) for the REWIRE training courses were also provided. It was a chance to describe the courses and engage the audience before the launch of the virtual learning platform (VLE).
The event presented the connection of the ECSF and the REWIRE project practically. Specifically, the upcoming courses and certification schemes developed by the REWIRE project were introduced and a call to all interested parties was made.

Hungary

The audience was interested in the course. Main questions arose around:

- pricing;
- availability of the courses;
- certification method;
- long term availability of the courses.

Most interest was shown in the tasks at the cyber range.

Lithuania

The reaction of the audience was largely positive, with participant interest expressed through sustained in-person and online viewership throughout all presentations and the discussion. Questions indicative of genuine appreciation and concern regarding the topic of cybersecurity were asked and profound answers provided by the experts and discussion panel. Participants remained engrossed in the discussion following the allocated event time, thus shaping opportunities for future co-operation and involvement. Relevant materials were distributed to all interested parties' post-event.

The event highlighted the importance of the field of cybersecurity on a societal level by involving students, academic staff and experts within the field. Mykolas Romeris University (MRU) has hosted a similar REWIRE event in the past, resulting in sustained audience participation and as such, this event could further encourage the academic community to become involved in matters related to cybersecurity.

Portugal

The participants showed interest in the courses developed within the project. Main questions were related to the certification, equivalence with existing degrees, and sustainability after the end of the project. Assessment of the entry level of participants was also discussed.

Interesting discussions were generated about the usage of REWIRE courses as entry-level courses for other courses offered locally.

Serbia

The event was attended by most relevant Serbian stakeholders from the public, private, academic and nonprofit spheres. The REWIRE project was showcased, outlining its objectives, initiatives, and achievements. Notably, emphasis was placed on the significance of pertinent and applicable skill frameworks, along with the genesis and the advantages of the REWIRE skill framework. Furthermore, detailed insights were provided on the REWIRE MOOC Courses, highlighting the value of their accessibility to the public.

The National Cyber Conference stands as the largest conference in the Republic of Serbia, convening all pertinent stakeholders in the field of cybersecurity. As awareness of the cybersecurity skills gap grows alongside other challenges, capacity-building initiatives receive significant attention within Serbian society.

Spain

The work carried out in REWIRE has sparked significant interest. A prevailing viewpoint is that the project addresses a crucial need to tackle the widespread issue of the cybersecurity skills gap. The shortage of cybersecurity professionals required to fill various positions appears to be a persistent challenge that is growing over time. From an industrial standpoint, it is imperative to develop tools that can align stakeholders within

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

the cybersecurity ecosystem, facilitating the connection between job offerings, demand, and skill training (in education and academia).
Furthermore, REWIRE has attracted attention at an academic level, with professors from various Spanish universities expressing interest in its potential as an educational tool. People who participated in discussions expressed curiosity about the availability of REWIRE courses, as well as its educational components like the REWIRE Cyber Range Platform.

Sweden
Interest and positive feedback from the audience regarding the job profiles, and the online tools. Questions focused on the business model of the online courses, possible ways of certification, and the intended target audience.

6. THIRD ROUND

The third and final round of the Cybersecurity SSA Network building/Campaign events was focused on the launch of the final version of the training courses and their second delivery (fig.7).

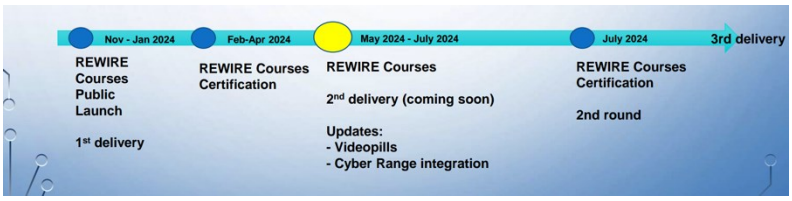


Figure 7: REWIRE courses roadmap

6.1. CONTENT

The third round of National events gave the partners the possibility to promote the REWIRE products to a wide range of VET providers (EQF3-6) and other stakeholders, including students. The primary objective of this round of events has been to spotlight and promote the second delivery of the REWIRE training course, their final structure and the relevant certification schemes tailored to four selected occupational profiles.
For every course, speakers highlighted the essential structure, as represented in fig. 8.

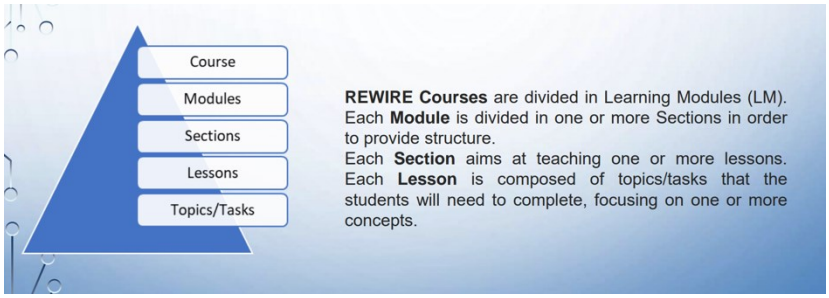


Figure 8: General structure of the REWIRE courses

The four different profiles are explained in the following figure:

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Figure 9: REWIRE courses based on 4 different profiles

6.2. EMERGING RESULTS

For this third round, 11 events were organized, (again: in presence, hybrid or online), between April and June 2024. More than 700 people were reached. In the following sections, an overview of the national initiatives.

Belgium

Participants demonstrated notable interest through the established Zoom channel. Audience members were encouraged to explore the REWIRE training courses further, as they offer invaluable opportunities for building and advancing cybersecurity expertise and contributing to collective resilience against emerging threats. Also, participants were encouraged to email, especially regarding questions or remarks related to the courses developed by REWIRE, to engage further with the speakers and delve deeper into the topics discussed. The post-event email follow-up includes an evaluation survey, the data collection and analysis of which are managed by ReadLab.

The event, "Bridging the Cybersecurity Gap: REWIRE Training Courses," underscored the significance of these courses for four specific occupational profiles, illuminating their role in addressing cybersecurity challenges. Furthermore, the event's exposure could enhance the project by attracting more organizations to participate in the training courses. Increased engagement from diverse entities not only offers valuable feedback but also fosters overall success, growth, innovation, and competitiveness within the cybersecurity sector. The event's impact on EVTA & EfVET at local and national levels was substantial, as it facilitated information dissemination among cybersecurity stakeholders. Moreover, it served as a networking and collaboration platform, fostering connections among key stakeholders, potentially leading to future partnerships and initiatives. Additionally, by showcasing EVTA's & EfVET's active involvement and organizational capabilities, the event solidified its leadership in cybersecurity education and advocacy, potentially opening avenues for funding and strategic partnerships to advance cybersecurity skills and resilience.

Cyprus

The third info day of the REWIRE project in Cyprus focused on providing information on the courses and certifications offered by the REWIRE project. The agenda also included a presentation on challenges related to cybersecurity skills by the Digital Authority of Cyprus.

Czech Republic

The participants were really interested. They had several questions about the online courses created, they were interested in taking other online courses besides Cybersecurity Incident Responder. The main interest was in the CISO and Penetration Tester courses. Students have provided much feedback on the courses being developed, especially wanting to integrate the VLE and KYPO platforms together. Several students expressed interest in repeating the course once these courses are fully finished. In addition, participants have also expressed interest in taking the REWIRE certification exam once they have achieved the REWIRE certification requirements. Almost half of the participants are interested in staying in touch with REWIRE activities and getting up-to-date information on REWIRE activities. Most of the participants already had some experience in cybersecurity, and several of them had already completed several online cybersecurity courses and certifications. The participants confirmed that REWIRE activities make sense and that the courses, despite minor shortcomings, are of high quality and logically structured. From the point of view of some participants, there would also be an interest in integrating some parts of online courses into the cybersecurity courses at BUT. In fact, this option is also being considered at BUT.

France

As in the past editions, there is interesting and positive feedback from the audience regarding the efforts on job profiles and regarding the online courses developed in the REWIRE project.
Promotion/consolidation of our organization as a key player in cybersecurity.
A vector to promote REWIRE activities, but also to promote a new cybersecurity training platform (which includes two professional cyber-ranges) and to highlight our master-level cybersecurity curricula, including our new FISEA curriculum on cybersecurity (FISEA = 1 year as a student, and 2 years as an apprentice) which will start in September 2024. This new diploma is the first FISEA diploma with an engineering degree specialized in cybersecurity accredited by the CTI at the national level (France). It is important to be visible to attract companies/industries proposing apprenticeships for this curriculum.

Greece

The audience showed interest in the information provided for the REWIRE Courses, the VLE and the respective Certifications. Information was provided by the guest speakers through the Role and Work of the National Cyber Security Authority of Greece presentation and the CyberSecPro collaborative project presentation. The links for the European CyberSecurity Challenge (ECSC), the SaferInternet4Kids action, and the CyberSecPro collaborative project were provided through the MS Teams platform. The actual links of the VLE for the REWIRE training courses and the Certifications were provided, as well.

To enhance the network of interested parties for REWIRE, links to the official website and the social media of the project were provided to the attendees.
The event organizers presented the courses, the platform and the certification systems developed by the REWIRE project and invited all interested parties to participate in the relevant training and certifications, also providing their feedback.

Hungary
The audience was interested in the course. Main questions arose around:

- pricing;
- availability of the courses;
- certification method;
- long term availability of the courses.

Lithuania
During the event, REWIRE (Edmundas Piesarskas, EKT) presented the 4 updated REWIRE Cybersecurity Vocational Open Online Courses (VOOCs): CISO, Penetration Tester, Cyber Incident Responder, and Cyber Threat Intelligence Specialist. All courses are free of charge and provide participants with the chance to interact within the cyber-range. Upon successful completion, participants will receive a certificate of attendance and even could obtain a generally recognized certificate (provided they meet the prerequisites that are indicated in the course description).
In the discussion on cybersecurity opportunities that followed, participants listened to expert advice regarding access to free cybersecurity software and training, as well as information on funding, its terms and conditions.

Portugal
The participants showed interest in the courses developed within the project. Main questions were related to the cost and sustainability of the certification scheme, comparison with existing commercial certifications and college degrees, and availability of the courses and certification process after the end of the project. Another question is the pre-requisites to join and attend the courses.
The main impact in the organizations that were present was the potential usage of these modules to reskill and upskill existing talent that is currently not involved in cybersecurity tasks. Many organizations do relate to the lack of cybersecurity professionals and the need to reskill existing professionals.

Serbia
The event was attended by most relevant Serbian stakeholders from the public, private, academic and nonprofit spheres. The REWIRE project was showcased, outlining its objectives, initiatives, and achievements. Notably, emphasis was placed on the significance of pertinent and applicable skill frameworks, along with the genesis and the advantages of the REWIRE skill framework. Furthermore, detailed insights were provided on the REWIRE VOOC Courses, highlighting the value of their accessibility to the public, cyber range hands-on exercises and certification possibilities.
This meetup was held as part of the 3-day event focused on Serbian Cybersecurity Challenge finale, which, being the national competition, convenes all pertinent stakeholders in the field of cybersecurity. As awareness of the cybersecurity skills gap grows alongside other challenges, capacity-building initiatives receive significant attention within Serbian society.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Spain
The public in general was interested in the content shared. The fact that bringing some solutions to their problems (focusing on the business attendees) was very welcome on their side, considering the possibility of offering the courses to their workers. From the side of the students, they were very excited about the courses, the contents tackled and the hands-on part on the Cyber Range. The demo with the Cyber Range was the part that they more enjoyed by far.
Clearly, the impact expected is to have new students on our courses given the presentation hosted at the Barcelona Cybersecurity Congress. The students assured us that they were going to register and going to work on the courses. They were willing to try the Cyber Range platform.

Sweden
The participants were very interested in the methodology used for identifying the security skills needs and the developed course curricula. They expressed interest in the methodologies and brought up interesting questions about certification, automated skills assessment and profiling of individuals, and the potential integration of such efforts with the material developed in REWIRE. The participants were very pleased with the project's results.
Participants were aware of the importance of cyber security education in the future of digitalization. Organizations, such as the newly established national cyber security center CyberCampus, showed great interest for the project´s results, and will likely benefit from knowledge transfer.

7. CONCLUSIONS AND IMPLICATIONS

This report provides a summary of various countries' feedback and engagement regarding the Cybersecurity SSA Network Building/Campaign events, implemented by REWIRE partners during the months 25-45 of the project. This report aims to offer an overview and a summary of the main achievements.

It is possible to identify some common traits: the events were basically very important to promote cybersecurity training and education across multiple countries. Participants expressed strong interest in the courses, particularly in learning about certifications and course contents related to cybersecurity skills and roles. Some essential elements can be listed:

1. **Participant Engagement:** Attendees showed enthusiasm for the REWIRE courses, asking questions about course details, certifications, and future opportunities. This indicates a significant interest in developing cybersecurity skills.
2. **Feedback and Interest Areas:** Participants from various countries provided positive feedback, focusing on the value of hands-on exercises, the integration of cybersecurity training platforms, and potential certifications. There was a notable interest in practical applications and real-world cybersecurity skills.
3. **Impact on Organizations:** The event highlighted the importance of cybersecurity education and its role in fostering new collaborations, enhancing organizational capabilities, and addressing the cybersecurity skills gap at both national and local

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

levels. The event also served as a platform for networking among key stakeholders, promoting future partnerships and initiatives.

4. **Next Steps and Future Implications:** Moving forward, the event emphasized the need for continued education and training in cybersecurity, promoting a more resilient cybersecurity infrastructure. This includes further integration of courses, developing new partnerships, and increasing awareness about the importance of cybersecurity skills and certifications.

This summary captures the essence of the discussions and the potential impact of the event on advancing cybersecurity education and collaboration across Europe thanks to REWIRE. More info, on request, can be provided on the single reports produced by partners for each event.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

8. LIST OF FIGURES

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union