



REWIRE - Cybersecurity Skills Alliance

A New Vision for Europe

R6.3 Impact

Evaluation report No. 3



Title	R6.3 Impact Evaluation Report No. 3
Document description	The Impact Evaluation Report No. 3 presents the second Impact Evaluation of the REWIRE project covering the evaluation of the impact of project outputs delivered between month 25 and 36, namely from 01 November 2022 to 31 October 2023.
Nature	Public
Task	Task 2: Continuous quality control
Status	Draft
WP	WP 6
Lead Partner	ReadLab
Partners Involved	All partners
Date	25/10/2023

Revision history	Author	Delivery date	Summary of changes and comments
Version 01	Olga Karamichailidou (ReadLab), Odysseas Vlachonikolos (ReadLab)	25/10/2023	First version shared with the project coordinator.
Final Version	Olga Karamichailidou (ReadLab)	31/10/2023	Final version incorporating feedback from the project coordinator.

Disclaimer:

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

TABLE OF CONTENTS

1	EXECUTIVE SUMMARY	4
2	INTRODUCTION	5
2.1	Project background	5
2.2	Project objectives	5
2.3	Document objective	6
2.4	Methodology and data collection	6
3	STAKEHOLDERS	7
3.1	Survey on WP 3 MILESTONES.....	7
3.2	National Info Days	14
4	CONCLUSION	23
5	REFERENCES	24
6	LIST OF ABBREVIATIONS AND ACRONYMS	25
7	LIST OF FIGURES	26
8	LIST OF TABLES	27

1 EXECUTIVE SUMMARY

The evaluation of the REWIRE project deliverables and other tangible results is essential for its continuous improvement. The report at hand presents the second Impact Evaluation of the REWIRE project summarizing the major achievements of the REWIRE project from month 25 to month 36, namely from 01 November 2022 to 31 October 2023, and discussing whether the project objectives had been met.

The 3rd Impact Evaluation Report employs a mixed methodology in order to collect and analyse both qualitative and quantitative data on the second year of the project. It assesses the project's impact as it incorporates external feedback received from stakeholder surveys and gives a comprehensive overview of the project's impact during its third year.

Overall, WP3 deliverables, namely the European Cybersecurity Blueprint (R3.2.1), the Cybersecurity Skills Framework (R3.3.1), the Mapping the framework to existing courses and schemes (R3.4.1), and the Analysis of Cybersecurity Career Pathways (R3.5.1), received positive feedback from the stakeholders with the European Cybersecurity Blueprint receiving the highest number of mentions, underlining its prominent status among the various results.

2 INTRODUCTION

2.1 PROJECT BACKGROUND

The Cybersecurity Skills Alliance – New Vision for Europe – REWIRE project is the Alliance formed from the four winning pilot projects of the 2018 Horizon 2020 cybersecurity call "establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap": CONCORDIA, ECHO, SPARTA and CyberSec4Europe. Thus, the REWIRE Alliance represents the more than 160 partners of the four pilot projects, including big companies, SMEs, universities and cybersecurity research institutes, from 26 EU Member States.

This project aims to provide concrete recommendations and solutions that would lead to the reduction of skill gaps between industry requirements and sectoral training provision and contribute to support growth, innovation, and competitiveness in the field of Cybersecurity. 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).

2.2 PROJECT OBJECTIVES

REWIRE builds a Blueprint for the Cybersecurity industry and a concrete European Cybersecurity Skills Strategy. This strategy will bring together lessons learned from other initiatives (i.e. CONCORDIA, SPARTA, ECHO, CyberSec4Europe) and will be outlined from a holistic approach, identifying political, economic, social, technological, legal and other factors which may be affecting sector skills and training offer. Encompassed with activities, milestones, outcomes and outputs, these activities will be developed during the course of the project:

- Design and implementation of a Blueprint for the Cybersecurity industry
- Develop a European Cybersecurity Skills Strategy
- Develop a common methodology for the assessment of the current situation and to anticipate future needs, through identification of existing and emerging skills needs.
- Create a European Cybersecurity Skills Observatory integrated by specific actions, activities and tools that allow for anticipation and matching of skills supply and demands.
- Support the strategy and framework through the implementation of a digital on-line publicly accessible European Cybersecurity Skills Digital Observatory – CyberABILITY (for cybersecurity skills merging the market needs, the profiles, the competencies and the available training courses).
- Create a Cybersecurity Skills Framework containing profiles for the needed cybersecurity profiles and their analysis.
- Pilot a federated cyber range hosted by multiple project partners to support the goals of the project.

- Create at least four (4) educational curricula and relevant skills certification schemes for profiles contained in the Cybersecurity Skills Framework.
- Promoting the attractiveness of the sector and gender balance through specific actions to engage all relevant stakeholders
- Develop actions for encouraging mobility through promoting the use of existing European tools (Erasmus+, EURES, EAfA etc.).
- Create networks to improve skills intelligence and information mechanisms and strengthen the exchange of knowledge and practice between the cybersecurity industry and the VET providers, adapting VET provision to the skills needs demanded by the sector.

REWIRE aims to get main market players involved taking up opportunities to make the best of their talents. They will constitute together with the partnership, the Sector Skills Alliance, the necessary driver to push a sustainable sectoral strategy and Blueprint implementation as mentioned above.

2.3 DOCUMENT OBJECTIVE

This report documents the impact attained during the second year of the project, namely from month 13 to 24. According to the QA plan, the objective of evaluating the impact is to assure *that target groups are satisfied and use the products and methodologies developed by the project, and targets planned for dissemination and exploitation are met.*

The impact of the project is assessed internally by the partnership and externally by the project's stakeholders (including sometimes by the Focus Group and Expert Advisory Board). The purpose of this report is to give an overview of the project's impact.

2.4 METHODOLOGY AND DATA COLLECTION

The impact evaluation reports require the use of both quantitative and qualitative methods using a combination of 5-score Likert scale questions, open-ended questions and social media/literature review.

The current impact analysis is based upon primary and secondary sources such as feedback forms, questionnaires, checklists, web and social media analytics and post-event reports. In order to collect primary and secondary data on the project's impact, ReadLab used the following **tools**:

- Stakeholder evaluation form
- National Info day reports

ReadLab administered a *stakeholder survey* during the roll out of the first series of national info days. The data were collected and processed in anonymous and aggregate form to prepare a summary report of the main elements emerging from the survey.

3 STAKEHOLDERS

3.1 SURVEY ON WP 3 MILESTONES

During the roll out of the national info days, ReadLab, serving as the leader of WP6, initiated a survey campaign aimed at gathering feedback from its stakeholders regarding four WP3 deliverables, namely the European Cybersecurity Blueprint (R3.2.1), the Cybersecurity Skills Framework (R3.3.1), the Mapping the framework to existing courses and schemes (R3.4.1), and the Analysis of Cybersecurity Career Pathways (R3.5.1). The survey campaign remained active for a duration of three months and garnered a total of 24 responses.

The individuals who participated in the survey hailed from a total of six European countries, and this geographical distribution is visually represented in the chart displayed below.

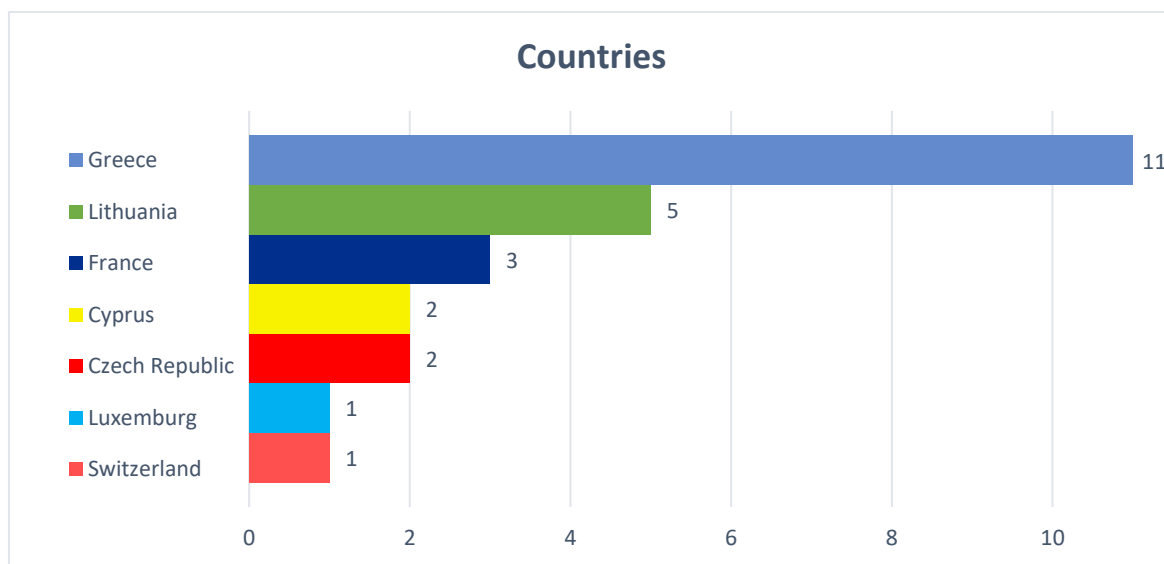


Figure 1 Countries of Respondents to the survey on WP3

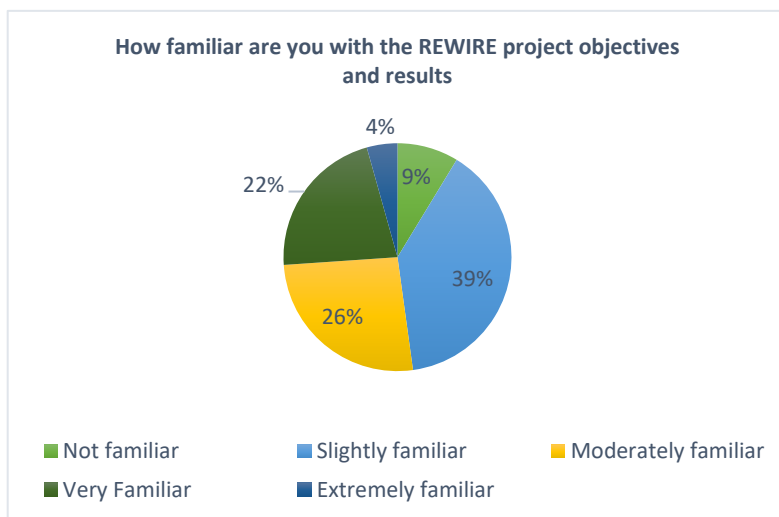


Figure 2 Familiarity with REWIRE results/objectives.

The stakeholders appeared to possess a level of familiarity ranging from slight to moderate with the objectives and outcomes of the REWIRE project. Specifically, among the respondents, a combined 65% indicated a degree of familiarity, with 39 percent expressing a moderate level of familiarity and 26 percent indicating a slight level of

familiarity.

When it comes to the communication of the project's results and achievements, it is notable that a considerable proportion of the stakeholders exhibited a high degree of satisfaction. In particular, 38% of the survey respondents indicated that they were "satisfied," while an additional 25% expressed an even higher level of satisfaction by choosing the option "very satisfied." These satisfaction levels underline the significant impact and effectiveness of the communication efforts directed towards engaging with and informing stakeholders about the project's outcomes and accomplishments.

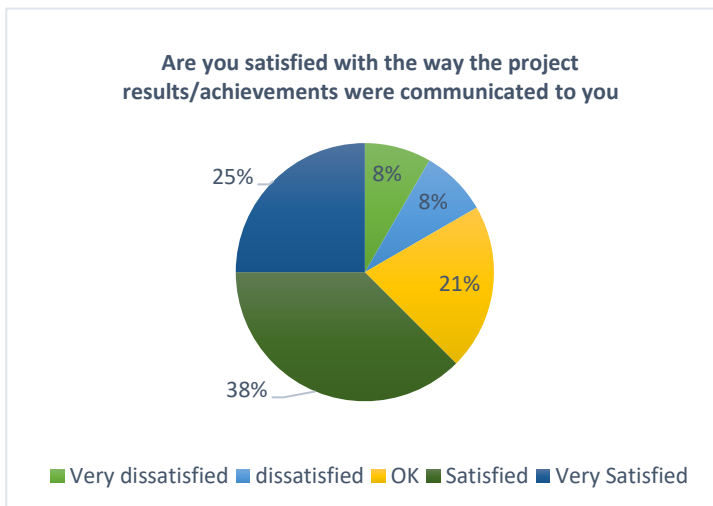
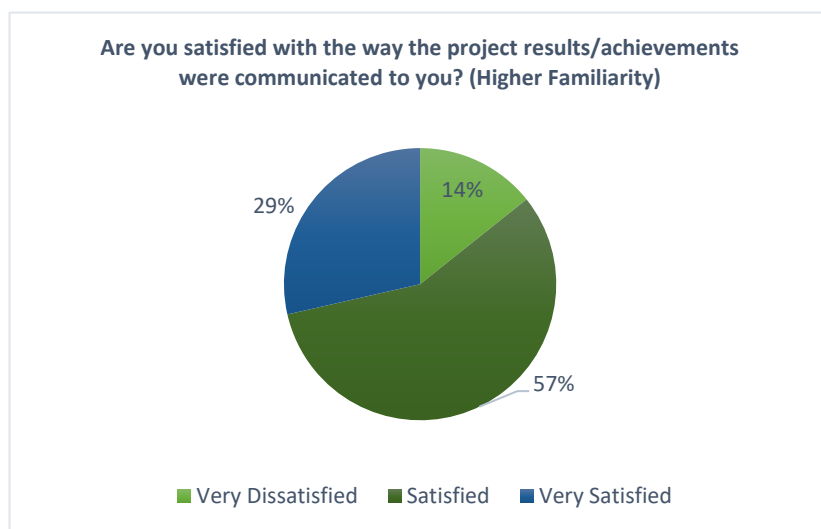


Figure 3 Satisfaction with communication of project results



While the answers provided by various stakeholders have a notable influence, it is imperative to evaluate the responses of individuals who responded with a very and an extreme familiarity with the project's objectives. Those who possess a more profound comprehension of the REWIRE objectives carry more weight in their responses. Hence,

concerning the question of satisfaction with the communication of the results, individuals with greater familiarity registered higher rates of satisfaction. To be specific, 86% of respondents who were familiar expressed either satisfaction or high satisfaction.

Figure 4 Satisfaction with communication of project results - Higher Familiarity

Relevance

Regarding the relevance of the results, stakeholders were questioned about the applicability of these findings within the **context of their country and the alignment with policy developments**. The response data revealed that a substantial majority of respondents expressed satisfaction with the relevance of the results. Nevertheless, 25% of respondents

remained undecided on this matter, and a smaller segment expressed disagreement regarding the relevance of the findings. Notably, during the survey, a comment was documented to elucidate one of the responses: "I would appreciate it if the event's language was in English."

Similarly, when examining responses to the same question, it becomes apparent that individuals with more extensive knowledge and awareness of the objectives demonstrated more assertive opinions regarding the relevance of the results. Their perspectives conveyed a deeper sense of conviction regarding the significance of the findings.

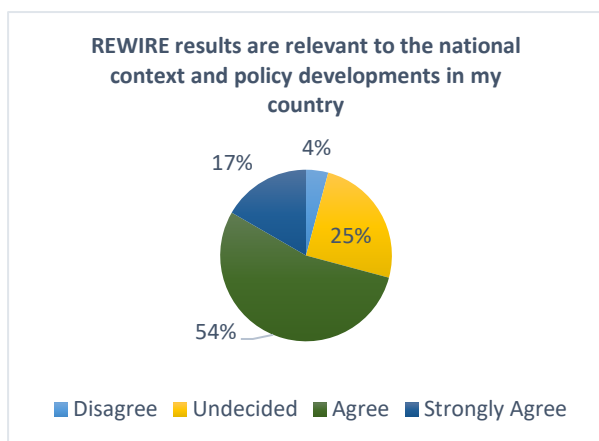


Figure 6 Satisfaction with the national context and policy developments in their country

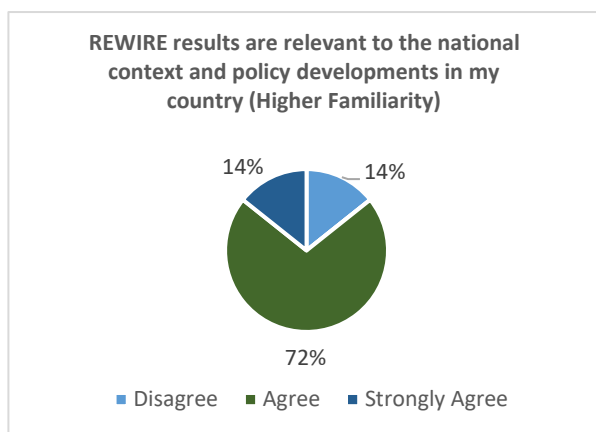


Figure 5 Satisfaction with the national context and policy developments in their country - Higher Familiarity

In terms of the feedback on the **alignment of the REWIRE results with labor market requirements**, the majority of stakeholders expressed a high level of satisfaction. Notably, among those who possessed a deeper familiarity of the REWIRE objectives, there was an absence of any negative responses. This underscores the noteworthy impact and relevance of these results, particularly for those closely attuned to the project's objectives.

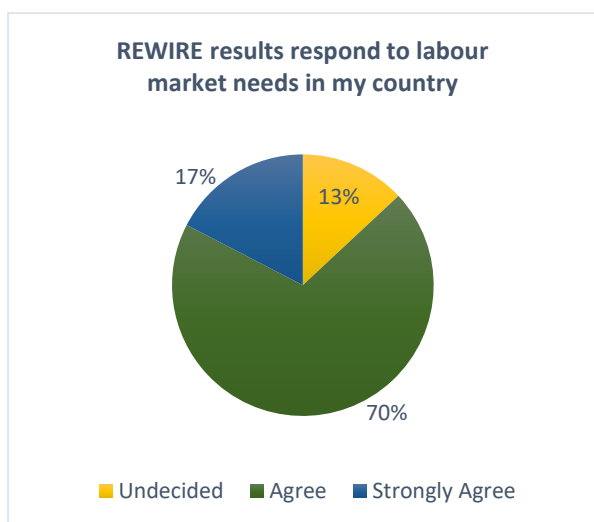


Figure 8 Satisfaction with the response to labour market needs in my country.

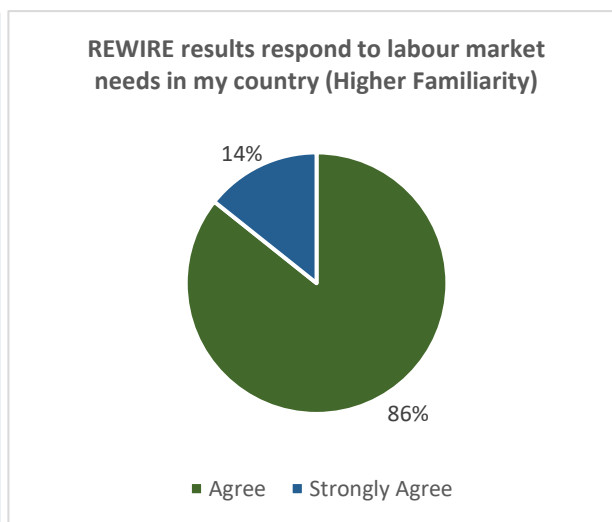


Figure 7 Satisfaction with the response to labour market needs in my country - Higher Familiarity.

Regarding the results, stakeholders were given the opportunity to express their opinion on which of the four choices held the most significance for them. Notably, it is worth mentioning that two results stood out as the most relevant among the respondents. The *R3.3.1 Cybersecurity Skills Framework* and the *R3.2.1 European Cybersecurity Blueprint* both received a major boost. This indicates a remarkable level of alignment and importance attached to these two results by the participants, underscoring their equal prominence in the eyes of those providing their feedback.

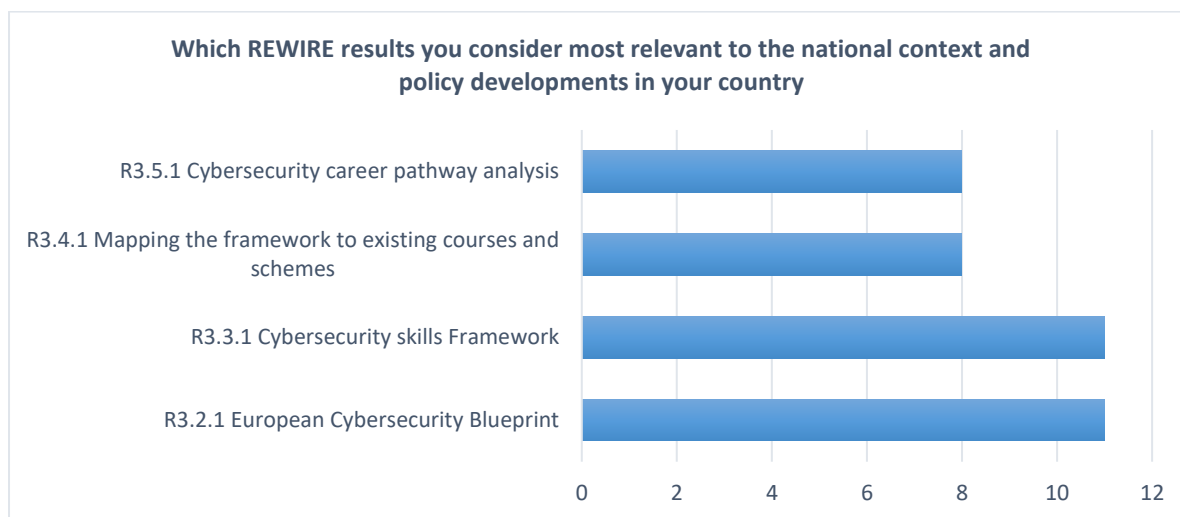


Figure 9 REWIRE Results – Relevance

Usability

In terms of the usability of the results, the stakeholders were categorized into three distinct groups based on their level of agreement with the ease of comprehending the findings. These groups included those who strongly agreed, those who simply agreed, and those who remained undecided.

Notably, within the subgroup consisting of individuals with a high degree of familiarity with the REWIRE objectives, there was a notable increase in satisfaction levels compared to the entirety of the stakeholder group. This signifies that those who possessed an enhanced understanding of the project's goals were more content with the usability of the results,

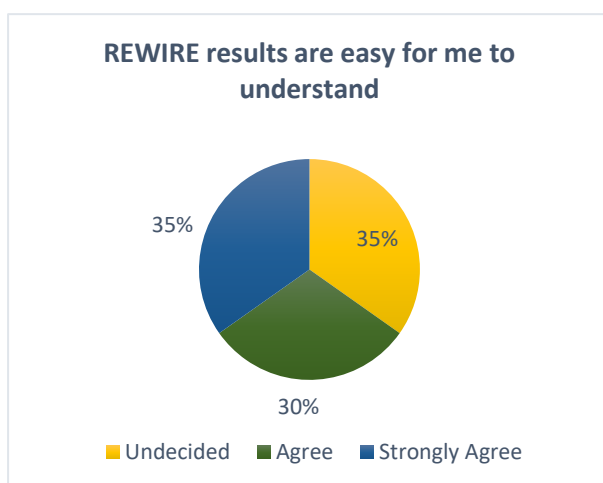


Figure 10 Satisfaction with the easiness to understand.

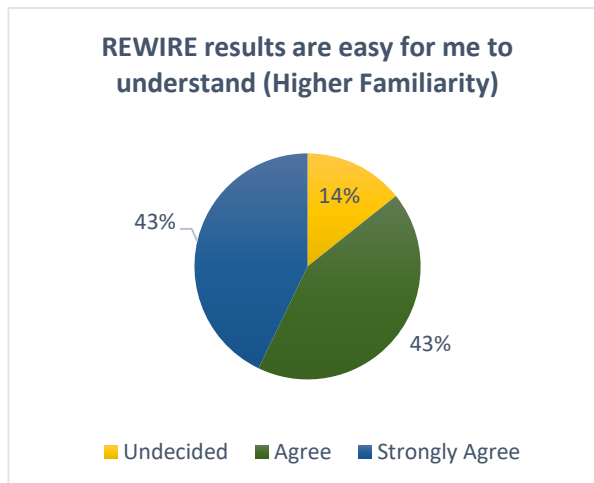


Figure 11 Satisfaction with the easiness to understand – Higher familiarity

As far as the ease of utilizing the results, it is evident that the majority of stakeholders expressed agreement, indicating a general consensus on the usability of the findings. More specifically, 46% and 17% were those who respectively strongly agreed and agreed, while 33% were undecided.

Particularly noteworthy is the fact that individuals with a more profound familiarity with the REWIRE objectives exhibited a higher degree of satisfaction, underscoring the positive impact of their familiarity with the project's goals on their perception of result usability.

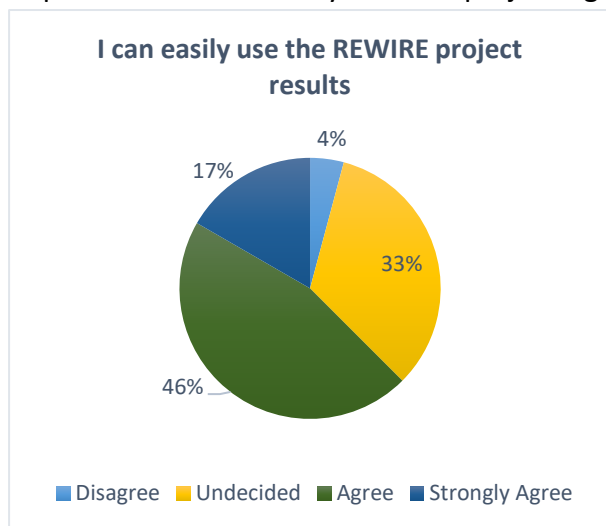


Figure 13 Satisfaction with the easiness to use.

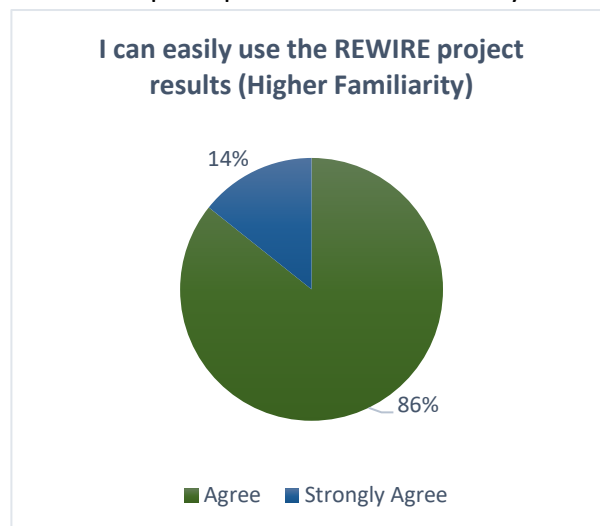


Figure 12 Satisfaction with the easiness to use - Higher Familiarity

When it comes to the REWIRE results, stakeholders were granted the opportunity to articulate their preferences regarding the most used among the four choices. It's noteworthy to highlight that one particular result emerged as the most relevant according to the respondents, which was the *R3.2.1 European Cybersecurity Blueprint*. The subsequent result in terms of preference, although notably lower in comparison to the Blueprint, was the *R3.4.1 Mapping the Framework to Existing Courses and Schemes*. This observation highlights the substantial degree of agreement and **impact importance of the European Cybersecurity Blueprint** by the participants, underscoring its distinct prominence in the view of those sharing their input.

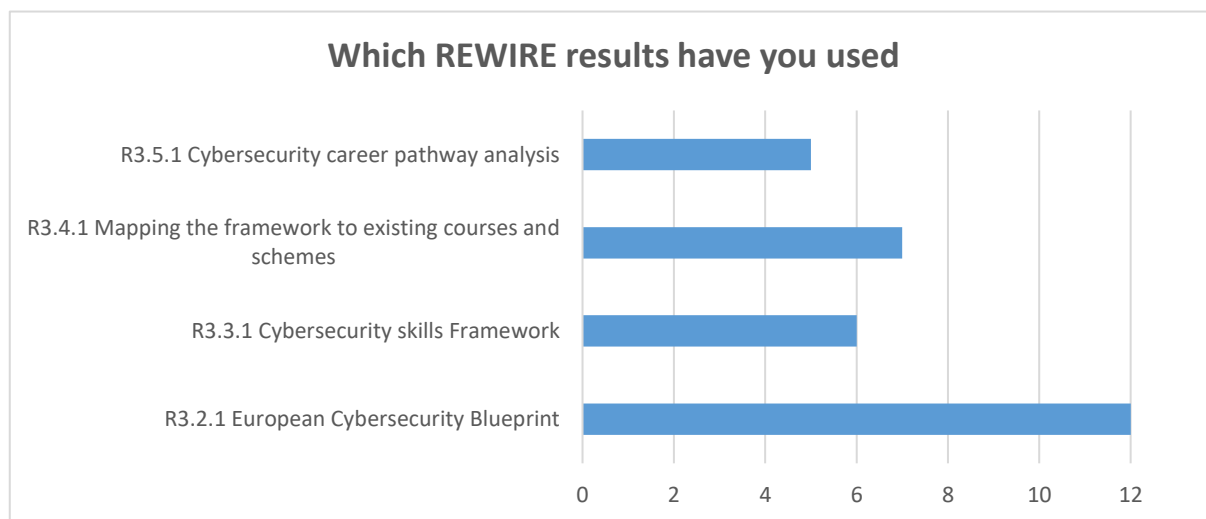


Figure 14 REWIRE Results - Usability

Expandability

Regarding the expandability of the REWIRE results, it's worth noting that nearly all respondents (92 percent) expressed their agreement that the cybersecurity sector or the industry could extend these findings. Furthermore, individuals with a greater level of familiarity with the subject matter exhibited an even higher level of satisfaction.

These responses underline the substantial impact and importance of the results for the pertinent stakeholders, highlighting their **potential for further development and relevance within the cybersecurity sector.**

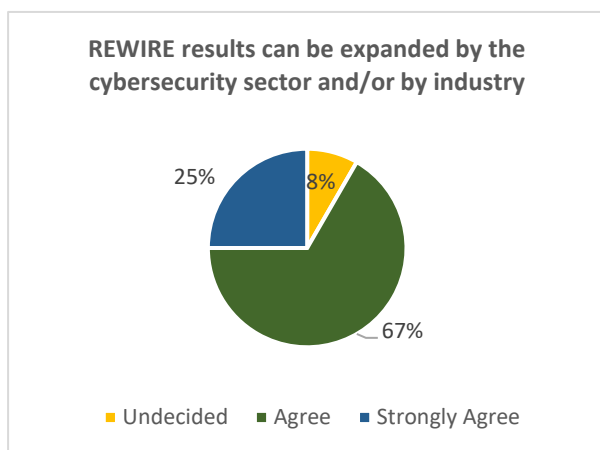


Figure 16 Satisfaction with the expandability to the

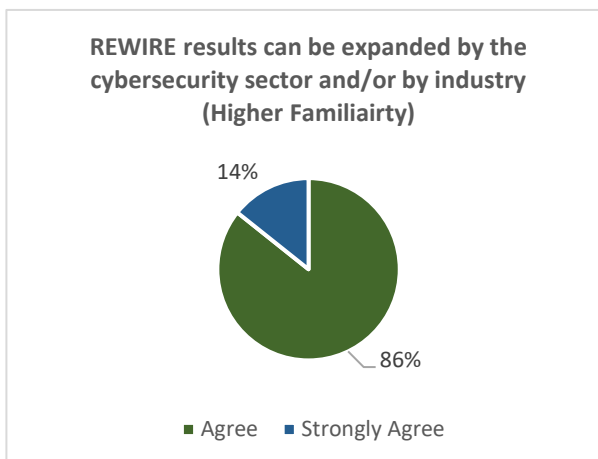


Figure 15 Satisfaction with the expandability to the industry - Higher Familiarity

Regarding the specific results targeted for expansion, it is worth mentioning that the majority of stakeholders once again pointed to the *R3.2.1 European Cybersecurity Blueprint*, underscoring the significant weight and relevance attributed to this particular outcome. However, it is important to note that the remaining three outcomes were also cited by some stakeholders, although with a relatively lower frequency and impact compared to the European Cybersecurity Blueprint.

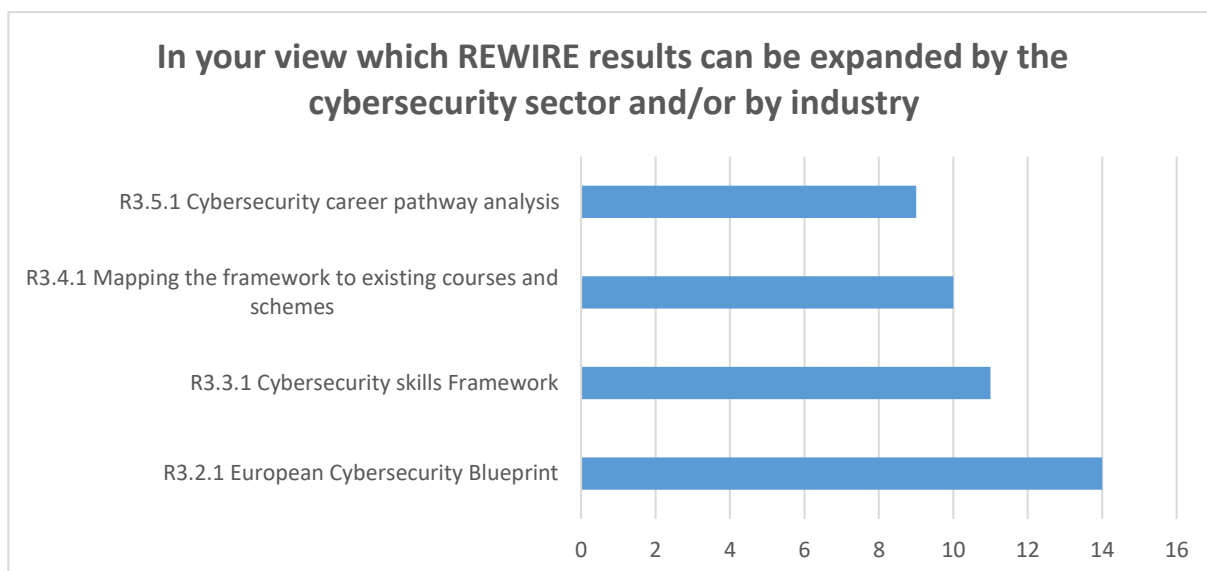


Figure 17 REWIRE Results - Expandability

Future Potential

Regarding the future Potential of the REWIRE outcomes, the respondents were questioned in four different aspects of this sector. Respondents were able to fill more than one result. Particularly, the most satisfactory result was the *R3.4.1 Mapping the framework to existing courses and schemes*, while the second most liked was the *R3.5.1 Cybersecurity career pathway analysis*. Regarding the most useful for the country's industry, the most satisfactory outcome was the *R3.4.1 Mapping the Framework to Existing Courses and Schemes*, as seen in the below tables.

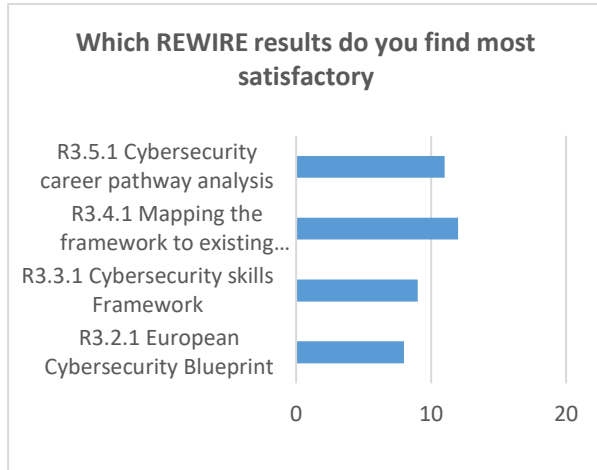


Figure 19 REWIRE Results - Future Potential & Overall Satisfaction

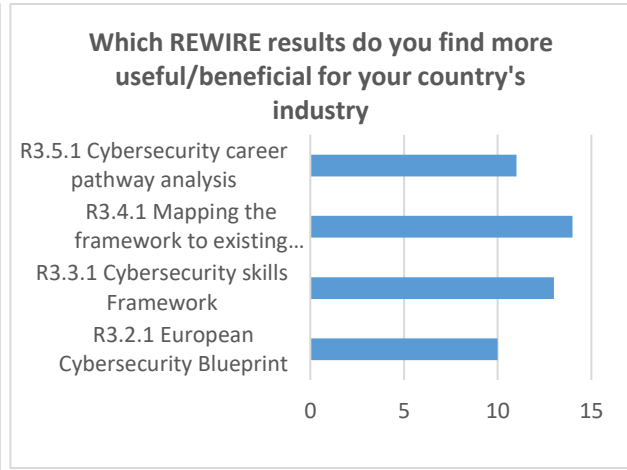


Figure 18 REWIRE Results - Future Potential & Useful for its country's Industry.

Regarding the **practical applicability** of the results to their respective roles and responsibilities, it's noteworthy that the *R3.5.1 Cybersecurity Career Pathway Analysis* emerged as the most prominently referenced outcome. Furthermore, there was a notable level of parity in responses between the *R3.4.1 Mapping the Framework to Existing Courses and Schemes* and the *R3.2.1 European Cybersecurity Blueprint* concerning their ongoing relevance and utility. This mosaic of answers underlines the significance of its REWIRE results in creating beneficiary impact for every stakeholder.

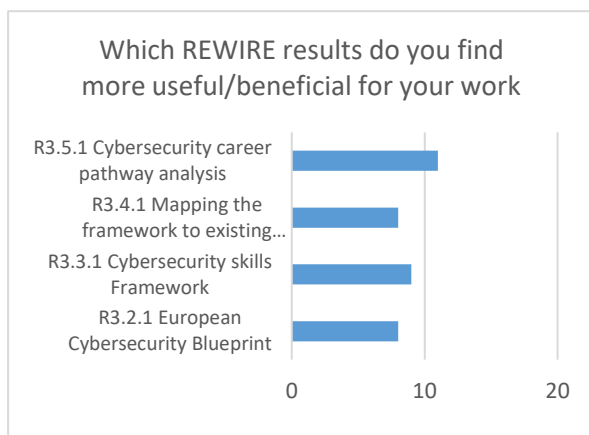


Figure 21 REWIRE Results - Future Potential & Useful for its work.

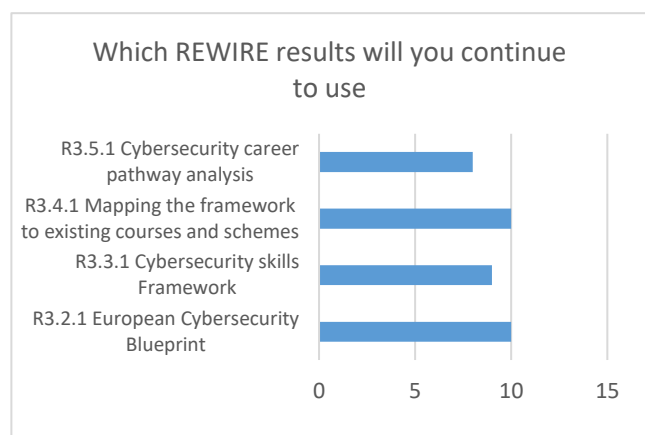


Figure 20 REWIRE Results - Future Potential & Continuity of usage.

Finally, the table provided below offers an exhaustive overview of the feedback received from diverse stakeholders concerning the REWIRE Outcomes. It is evident from this tabulation that the vast majority of the outcomes proved to be advantageous and of utility across a range of sectors. Nevertheless, it is noteworthy to highlight that the European Cybersecurity Blueprint received the highest number of mentions, underlining its prominent status among the various results.

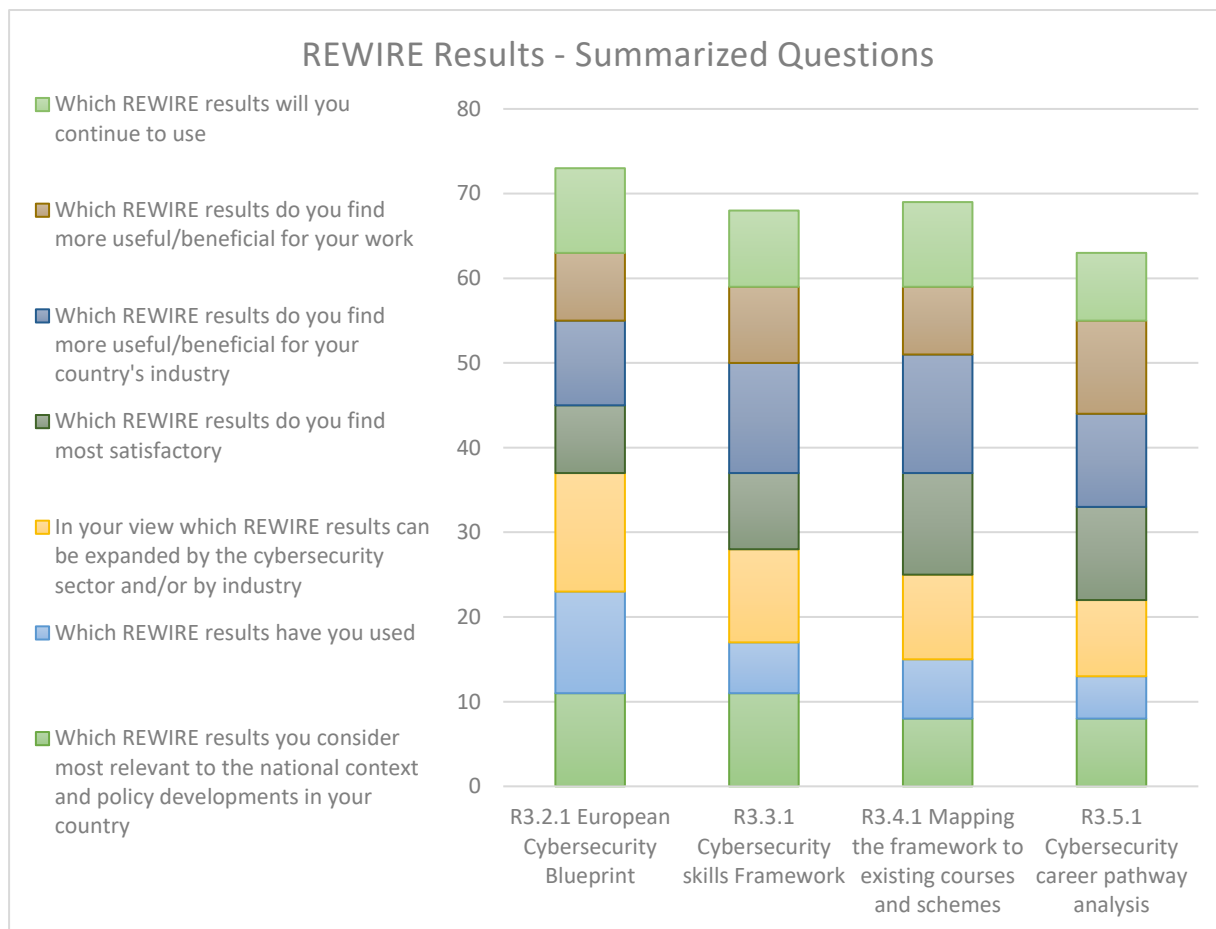


Figure 22 REWIRE Results - Summarized Questions

3.2 NATIONAL INFO DAYS

As the REWIRE Project makes strides towards achieving its goals, it has orchestrated a sequence of National Info Days across various European countries, playing a pivotal role in its continuous outreach and dissemination endeavors.

The principal and paramount aim of these events is to proficiently and extensively disseminate the significant outcomes, advancements, and objectives of the REWIRE project to a wide-ranging group of stakeholders. This, in turn, aims to cultivate a deeper comprehension of the project's mission and accomplishments among a diverse and influential audience.

The subsequent two tables provide a visual representation of the number of participants in each country, employing both a heatmap and a pie chart for illustrative purposes.

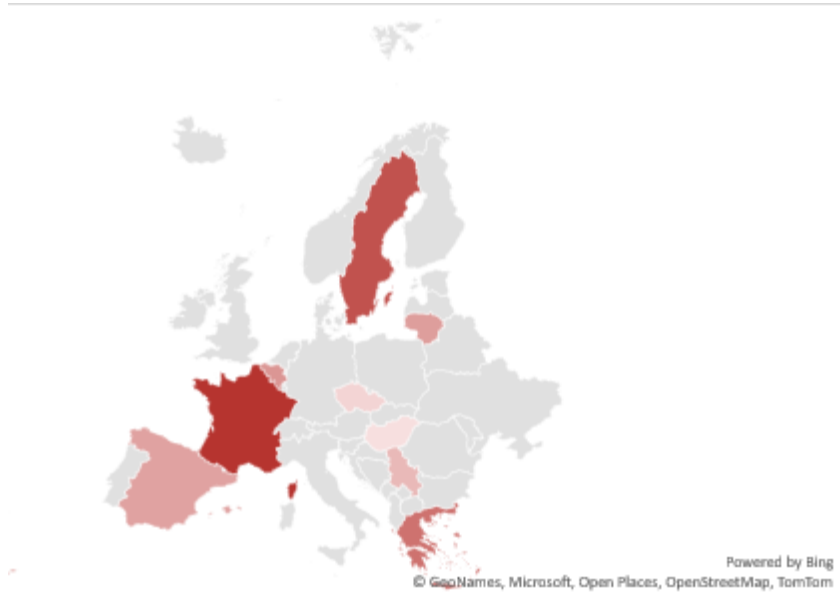


Table 1 National Info Days - Heatmap

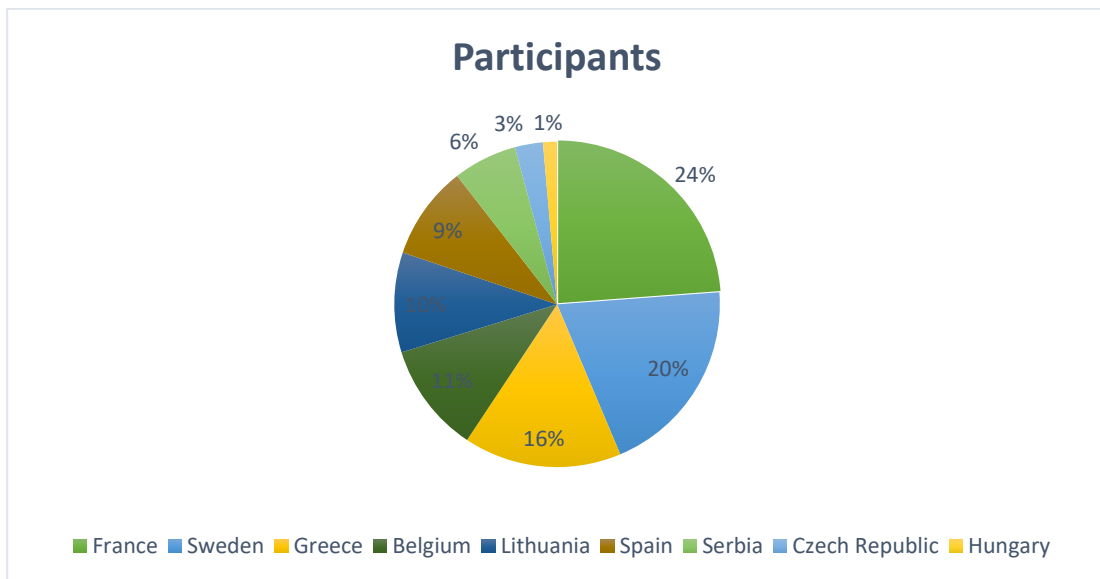


Table 2 National Info Days - Chart pie

Belgium

In May of 2023, an online event took place in Belgium, co-hosted by EfVET and EVTA. This well-attended event drew a total of 55 participants, and it was meticulously organized with a rich and diverse agenda. The primary focus of this event was to furnish the attendees with an extensive and in-depth comprehension of the European Cybersecurity Blueprint, the ongoing results of the REWIRE initiative, and the forthcoming milestones within the realm of cybersecurity.

Furthermore, the event was strategically designed to instill a sense of enthusiasm among the participants, igniting their interest in potential career opportunities and growth prospects in the dynamic field of cybersecurity. It aimed to inspire and inform, making a valuable contribution to the knowledge and aspirations of those who took part.

<p><u>Potential Impact:</u></p> <p>Belgium</p>	<p>According to our Belgian partners, during the panel discussion featuring distinguished speakers, the importance of elevating cybersecurity to a prominent position on the EU agenda, especially for educational institutions, such as schools, colleges, and universities, that heavily rely on online IT systems was highly emphasized. It was also stressed that the education sector should conduct a thorough assessment of its cybersecurity risks and actively enhance its capacity for cyber resilience.</p>
--	--

Lithuania

Lithuanian Mykolas Romeris University hosted an event attended by 50 individuals, comprising national stakeholders in the Lithuanian cybersecurity community hailing from diverse sectors. These participants included members of the academic community, such as those from Kaunas University of Technology, representatives from the private sector, including NGO Intechcentras, policymakers from the National Agency Education under the Ministry of Education, Sport and Science of the Republic of Lithuania, and cybersecurity practitioners from institutions like the National Cyber Security Centre under the Ministry of National Defence and the L3CE Lithuanian Cybercrime Competence and Research Center.

The event had several key objectives. Firstly, it aimed to bring together the various segments of the national cybersecurity skills community into a cohesive and significant gathering. Secondly, the event served as a platform to introduce attendees to the REWIRE project. Lastly, it sought to initiate discussions pertaining to the industry's development.

<p><u>Potential Impact:</u></p> <p>Lithuania</p>	<p>According to the event's host, both the overall turnout and the remarks expressed during the event underscored a notable absence and an evident demand for discussions surrounding cybersecurity skills in Lithuania. Events like these, coupled with further national endorsement activities, can effectively serve as valuable promotional tools to engage the cybersecurity community in more extensive dialogues and promotional initiatives concerning topics related to cybersecurity skills.</p>
--	--

Serbia

Unicom-Telecom hosted an information day for Serbia during summer, which attracted a noteworthy turnout. Specifically, the event was graced by the presence of at least 32 participants from the Cybersecurity Network Foundation. This foundation operates as a diverse, multi-stakeholder network, regularly convening meetings that bring together a broad spectrum of stakeholders from the public and private sectors, academia, and civil society. As a result, this gathering saw the active participation of the most pertinent stakeholders in Serbia.

Within this context, representatives from the REWIRE project took the opportunity to provide insights into the ongoing project developments and engaged in several informal conversations with the members of the Network. Of particular note was the heightened interest displayed by local experts in the REWIRE course development activities conducted

within Work Package 4. These experts kindly offered their expertise and expressed a desire to receive preliminary versions of course syllabi for review and feedback.

<p><u>Potential Impact:</u></p> <p>Serbia</p>	<p>The Network meetups served as a platform for Serbian cybersecurity stakeholders to deliberate on ongoing national-level initiatives. The event also facilitated updates on regulatory changes essential for compliance with the NIS 2 Directive. Lastly, participants reaffirmed their support for the Cyber Hero talent management program in a broader context and, more specifically, the Serbian Cybersecurity Challenge competition</p>
---	---

Greece

The Greek Info Day witnessed a collaborative effort from four partners, namely the Technical University of Crete (TUC), the Athens Metropolitan College (AMC), ReadLab, and LRQA Hellas. This gathering garnered substantial attention, drawing in an audience of 79 participants, thanks to the extensive outreach within the networks of the guest speakers. The attendees represented a diverse spectrum of stakeholders, including institutional authorities like the Hellenic Data Protection Authority, Hellenic Authority for Communication Security and Privacy, and the Hellenic Police - Cybercrime unit. Additionally, the event featured representatives from the realms of both industry and academia.

The overarching aim of this event was multifaceted. Firstly, it sought to introduce and elucidate the REWIRE Cybersecurity Blueprint. Simultaneously, it aimed to encourage a robust engagement with national stakeholders in meaningful conversations about cybersecurity, thereby expanding the project's stakeholder database. Notably, there was a pronounced level of interest from the public, particularly with regard to certifications, an aspect deemed pivotal in fostering and enhancing interdisciplinary collaboration.

<p><u>Potential Impact:</u></p> <p>Greece</p>	<p>The event was effectively communicated and circulated within the internal network of TUC, which had the positive outcome of attracting a considerable number of co-workers involved in other EU projects. Additionally, the event also piqued the interest of MSc (Master of Science) and undergraduate students, who gained valuable insights into the goals and endeavors of the REWIRE initiative. This wide-reaching dissemination facilitated a broader understanding of REWIRE among a diverse group of participants.</p>
---	--

Cyprus

The REWIRE project's Info Day in Cyprus was jointly organized by European University Cyprus (EUC), APIROPLUS Solutions Ltd., and the Cyprus Certification Company (CCC). Held online in February 2023, the event was primarily dedicated to the promotion of the REWIRE Cybersecurity Blueprint.

The event featured a range of informative presentations, commencing with a keynote session on the European Cybersecurity Skills Framework (ECSF), its associated advantages, and forthcoming steps, which shed light on the European dimension of cybersecurity skills.

Additionally, the Chief Officer of the Digital Security Authority of Cyprus delivered a presentation focusing on the national perspective of cybersecurity skills. Lastly, the event included a presentation dissecting the various components of the REWIRE Cybersecurity Blueprint.

Throughout the event, attendees were afforded the opportunity to delve deeper into the REWIRE project, provide constructive feedback on its primary outcomes and recommendations, utilizing a structured questionnaire. Moreover, participants actively engaged in a spirited discussion with the panel of speakers concerning the future of cybersecurity education. In sum, the event not only offered a comprehensive insight into the European Cybersecurity Blueprint but also significantly contributed to raising awareness about cybersecurity.

<p><u>Potential Impact:</u></p> <p>Cyprus</p>	<p>The event was communicated to various stakeholders in Cyprus and abroad. The participants of the event represented various categories with the majority being private and public organizations. The participants showed interest in the information provided from the presentations and the panel discussion. Moreover, through a survey that was launched during the event, participants showed an alignment with the rankings and directions provided by the blueprint presentation. This allowed the project partners to get an assurance regarding the main directions of the work implemented.</p>
---	--

Czech Republic

The Czech National Info Day was conducted online and was jointly organized by the Brno University of Technology and Masaryk University. The event brought together 14 participants representing various sectors, including government, academia, and the cybersecurity industry.

The primary objectives of the event centered around the promotion of the REWIRE Cybersecurity Blueprint, alongside the European and Czech national cybersecurity skills frameworks, as well as applications aimed at facilitating the development of cybersecurity skills.

Participants exhibited a keen interest in the project, with inquiries pertaining to potential future collaboration, particularly in terms of involvement in the forthcoming network. These attendees were subsequently included in the WP7 REWIRE stakeholder database, signifying their active engagement with the project. The speakers at the event were receptive to collaborative efforts, providing comprehensive information in response to queries. Furthermore, they made the presentation slides publicly available, ensuring that the content was readily accessible to the audience.

<p>Potential Impact:</p> <p>Czech Republic</p>	<p>Brno University of Technology (BUT) announced its forthcoming role as a co-investigator, collaborating with five other universities in the development of a Joint master's in advanced Cybersecurity. This program will be designed under the Erasmus Mundus Design Measures (EMDM) and is based on the principles of the REWIRE grouping and the Cybersecurity Profiler app, both integral components of the REWIRE Blueprint.</p>
--	--

France

The French National Info Day was collaboratively hosted by the University of Lorraine and Telecom Sud-Paris. This gathering proved to be the most significant event, with a notable turnout of 120 attendees representing a diverse range of backgrounds, including academia, professionals from the cybersecurity industry, and a substantial contingent of PhD students.

Throughout the course of this event, the hosts undertook the task of presenting the REWIRE project, providing a comprehensive and detailed overview of the project's structure and its broader objectives. Their efforts were particularly successful in kindling the interest of other universities and industry players, sparking discussions and potential collaborations in support of the REWIRE initiative.

Additionally, the Info Day had a tangible impact on student engagement, resulting in an increase in sign-ups for REWIRE courses. The event was particularly notable for its effectiveness in generating academic interest, with numerous professors expressing enthusiasm about integrating REWIRE into their educational programs.

<p>Potential Impact:</p> <p>France</p>	<p>Students who attended the event demonstrated a strong desire to learn more about the availability and implementation of tools such as the job analyzer tool in their academic and professional pursuits. This multifaceted success highlighted the event's contribution to advancing the goals and reach of the REWIRE project within the French academic and cybersecurity communities.</p>
--	---

Hungary

The National Info Day for Hungary was thoughtfully organized by the BME partner. The event attracted a gathering of seven participants, all of whom displayed a commendable level of interest in the REWIRE project.

As an integral component of this event, a comprehensive presentation was thoughtfully shared with a broader audience, promoting transparency, and fostering an environment conducive to the open exchange of information. Throughout the interactive session, the engaged participants actively engaged in posing a series of insightful questions. These inquiries were primarily geared towards gaining a deeper understanding of the prospective trajectory of the REWIRE project and delving into the intricacies and specifics of the courses that are in the planning stages. The event, in this way, served as a platform for meaningful discussion and exploration of the project's future endeavors.

<p><u>Potential Impact:</u></p> <p>Hungary</p>	<p>The attendees demonstrated a notable curiosity about the upcoming REWIRE courses, expressing a particular interest in their structure, content, and accessibility. Moreover, there was enthusiasm surrounding the practical aspects of the KYPO cyberage, with a focus on understanding how exercises on the platform could be accessed and effectively utilized. This heightened interest and engagement underscored the value of the Info Day in fostering meaningful discussions and cultivating a community of stakeholders invested in the REWIRE project in Hungary.</p>
--	---

Spain

The Spanish National Info Day, jointly hosted by Caixabank and Universitat Ramon Llull (URL), was an event that drew more than 45 participants, representing a blend of national and international academic and industrial partners.

The primary objective of this event was to officially introduce the REWIRE project, which is designed to address the prevailing skills gaps within the cybersecurity sector. This is to be achieved through the development of a comprehensive skills framework and blueprint, as well as the delivery of training programs. The event also sought to assess the current cybersecurity needs of the industry by scrutinizing recent educational and training initiatives. Moreover, it aimed to impart knowledge about the European Cybersecurity Blueprint, which is a systematic framework describing the various job profiles, skills, and knowledge necessary for the field of cybersecurity. The objective here was to build upon existing work and streamline the organization of these essential components.

The Info Day generated considerable interest and enthusiasm for the work undertaken within the REWIRE project. There was a unanimous recognition that the project is highly necessary due to the pressing issue of the existing skills gap in the field, particularly within the cybersecurity industry. The shortage of cybersecurity professionals is increasingly problematic, making it essential to provide tools that foster alignment among various cybersecurity stakeholders. This, in turn, would facilitate better connections between job offers, job seekers, and educational institutions.

<p><u>Potential Impact:</u></p> <p>Spain</p>	<p>The event generated substantial interest within the academic sphere, with several professors from other Spanish universities expressing a desire to incorporate REWIRE into their educational programs. Students who attended the event were particularly eager to learn about the availability of REWIRE courses and associated educational tools like the KYPO cyber-range, as well as supporting tools like the job analyzer. They were keen to understand when and how these resources would be accessible to them.</p>
--	--

Sweden

The Swedish Info Day, orchestrated by KTH Royal Institute of Technology in Stockholm, witnessed a robust turnout with approximately 100 participants in attendance.

The overarching objectives of the event revolved around unifying the Swedish cybersecurity community. The primary aim for REWIRE was to acquaint companies and policymakers with the project and pique their interest, while also collecting valuable feedback.

Throughout the event, the presentation encompassed an introduction to REWIRE, offering insights into the project's overall structure and detailing the tools that have been developed. Additionally, future plans for the project were outlined and discussed.

<p>Potential Impact:</p> <p>Sweden</p>	<p>The host reported that several attendees expressed a genuine interest in the REWIRE project and, notably, in the tools under development. What was particularly striking was the significantly heightened enthusiasm for these tools compared to taxonomies and frameworks. This differential interest underscores the community's pressing need for practical and actionable approaches that can effectively enhance the security posture of organizations and raise awareness, as opposed to all-encompassing frameworks that might have limited tangible impact on systems and organizations.</p>
--	---

Portugal

The National Info Day for Portugal, hosted by IST, attracted 11 participants representing academia and the industry.

The objective of the event was to promote the REWIRE project and present of the REWIRE Cybersecurity Blueprint. The event specifically aimed at presenting the work developed so far in the project REWIRE and the tools to be developed in the context of REWIRE, focusing on their impact in the cybersecurity education and training and in the identification of market needs.

The event encompassed a presentation by the host on the European Cybersecurity Blueprint proposed by the REWIRE project, a presentation on the Portuguese cybersecurity landscape, based on a study developed by AP2SI aiming at characterizing the cybersecurity professionals in Portugal, a discussion on the proposal and impact on the training of resources in cybersecurity at national level and a Q&A open to all participants.

The participants showed interest in the project, in particular to the tools to be developed for candidates, and the courses to be developed and shared by the project. Regarding 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. In addition, the event triggered discussions regarding possible cooperation between national universities to provide joint MSc courses enhancing each one's capacity to provide specialized courses.

<p>Potential Impact:</p> <p>Portugal</p>	<p>The participants showed interest in the courses to be developed and shared by the project. In addition, the event triggered discussions regarding possible cooperation between national universities to provide joint MSc courses enhancing each one's capacity to provide specialized courses. In addition, the event triggered discussions</p>
--	---

	regarding possible cooperation between national universities to provide joint MSc courses enhancing each one's capacity to provide specialized courses.
--	---

4 CONCLUSION

The results of the internal and external evaluations indicate that external stakeholders are satisfied with major project deliverables (WP3) that were released during the period M25 to M36 of the project delivery, namely from November 2022 to October 2023. Considering the above graphs and tables, we think that the whole project has maintained a good level of performance and that REWIRE results are impactful.

5 REFERENCES

REWIRE project description

REWIRE project – R.6.1 Quality Assurance plan

REWIRE survey European Cybersecurity Blueprint results

REWIRE National Info Day report – Belgium

REWIRE National Info Day report – Cyprus

REWIRE National Info Day report – Czech Republic

REWIRE National Info Day report - Hungary

REWIRE National Info Day report – Greece

REWIRE National Info Day report – France

REWIRE National Info Day report – Portugal

REWIRE National Info Day report – Serbia

REWIRE National Info Day report – Spain

REWIRE National Info Day report - Sweden

6 LIST OF ABBREVIATIONS AND ACRONYMS

Abbreviation	Explanation/Definition
EFVET	European Forum of Technical and Vocational Education and Training
M1	Month 1
QA	Quality Assurance
SME	Small and medium-sized enterprise
VET	Vocational Education and Training
WP	Work Package

Table 3 List of abbreviations and acronyms

7 LIST OF FIGURES

Figure 1 Countries of Respondents to the survey on WP3	7
Figure 2 Familiarity with REWIRE results/objectives.	7
Figure 3 Satisfaction with communication of project results	8
Figure 4 Satisfaction with communication of project results - Higher Familiarity	8
Figure 6 Satisfaction with the national context and policy developments in their country - Higher Familiarity	9
Figure 5 Satisfaction with the national context and policy developments in their country.....	9
Figure 7 Satisfaction with the response to labour market needs in my country - Higher Familiarity.....	9
Figure 8 Satisfaction with the response to labour market needs in my country.....	9
Figure 9 REWIRE Results – Relevance	10
Figure 11 Satisfaction with the easiness to understand.	10
Figure 10 Satisfaction with the easiness to understand – Higher familiarity Higher Familiarity.	10
Figure 13 Satisfaction with the easiness to use - Higher Familiarity	11
Figure 12 Satisfaction with the easiness to use.	11
Figure 14 REWIRE Results - Usability	11
Figure 16 Satisfaction with the expandability to the industry - Higher Familiarity	12
Figure 15 Satisfaction with the expandability to the industry	12
Figure 17 REWIRE Results - Expandability.....	12
Figure 18 REWIRE Results - Future Potential & Useful for its country's Industry.....	13
Figure 19 REWIRE Results - Future Potential & Overall Satisfaction	13
Figure 20 REWIRE Results - Future Potential & Continuity of usage.	13
Figure 21 REWIRE Results - Future Potential & Useful for its work.....	13
Figure 22 REWIRE Results - Summarized Questions	14

8 LIST OF TABLES

Table 1 National Info Days - Heatmap	15
Table 2 National Indo Days - Chart pie.....	15
Table 3 List of abbreviations and acronyms.....	25