Enhancing Cybersecurity Education in Europe: The REWIRE's Course Selection Methodology

Alan Briones Delgado
alan.briones@salle.url.edu
La Salle - Ramon Llull University
Barcelona, Spain

Sara Ricci
ricci@vut.cz
Brno University of Technology
Brno, Czech Republic

Argyro Chatzopoulou
ac@apiroplus.solutions
APIROPLUS Solutions Ltd.
Limassol, Cyprus

Jakub Čegan
cegan@fi.muni.cz
Masaryk University
Brno, Czech Republic

Petr Dzurenda
dzurenda@vut.cz
Brno University of Technology
Brno, Czech Republic

Ioannis Koutoudis
koutoudis@akmi-international.com
AKMI Internacional
Athens, Greece

ABSTRACT

The European Cybersecurity Skills Framework (ECSF) was introduced by the European Union Agency for Cybersecurity (ENISA) to identify the necessary competencies, knowledge, and skills required for European cybersecurity professionals. The ECSF condenses all cybersecurity-related positions into 12 role profiles, aiming to establish a mutual understanding of essential roles and support the creation of cybersecurity training programs. In order to address the shortage of cybersecurity experts, a multi-criteria selection method is developed to increase the availability, accessibility, and quality of cybersecurity courses and certifications. This Course Selection methodology ensures high-quality training materials that meet the current and future needs of the cybersecurity industry and benefit a wide range of participants. The methodology considers six criteria and provides a scoring system to rank the occupational profiles and select the most relevant profiles for the course design. Our final score formula identifies Chief Information Security Officer (CISO), Cyber Incident Responder, Cyber Threat Intelligence Specialist, and Penetration Tester for the Course creation.

CCS CONCEPTS

• **Social and professional topics** → **Computing education**; • **Applied computing** → **Education**; • **Human-centered computing** → *Human computer interaction.*

KEYWORDS

Cybersecurity, Education, Training Program, Methodology, Cyber Ranges

ACM Reference Format:
Alan Briones Delgado, Sara Ricci, Argyro Chatzopoulou, Jakub Čegan, Petr Dzurenda, and Ioannis Koutoudis. 2023. Enhancing Cybersecurity Education in Europe: The REWIRE's Course Selection Methodology. In *The 18th International Conference on Availability, Reliability and Security (ARES 2023), August 29–September 01, 2023, Benevento, Italy*. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3600160.3605091

ARES 2023, August 29–September 01, 2023, Benevento, Italy

ACM ISBN 979-8-4007-0772-8/23/08.
https://doi.org/10.1145/3600160.3605091

1 INTRODUCTION

Cybersecurity is currently suffering from a noticeable skills shortage. In 2022, the International Information System Security Certification Consortium (ISC)^2 [8] estimated that there was a global shortfall of approximately 3.4 million cybersecurity experts, overpassing the 2.7 million of 2021. This leads to the need of improving the availability, accessibility and quality of cybersecurity education to face the cybersecurity skills shortage [1] while bridging the gap between the needs of the market and the knowledge of the graduates [5].

The European Union Agency for Cybersecurity (ENISA)[6] introduced the European Cybersecurity Skills Framework (ECSF) [7] in 2022 as a practical tool that helps to identify and specify the tasks, competencies, skills, and knowledge necessary for European cybersecurity professionals. The framework aims to condense all cybersecurity-related positions into 12 following role profiles: Chief Information Security Officer (CISO), Cyber Incident Responder, Cyber Legal, Policy & Compliance Officer, Cyber Threat Intelligence Specialist, Cybersecurity Architect, Cybersecurity Auditor, Cybersecurity Educator, Cybersecurity Implementer, Cybersecurity Researcher, Cybersecurity Risk Manager, Digital Forensics Investigator, and Penetration Tester. The ECSF aims to establish a mutual understanding of the essential roles, competencies, skills, and knowledge required for European cybersecurity professionals. It also facilitates the recognition of cybersecurity expertise and supports the creation of cybersecurity training programs.

This paper is organized as follows: Section 1.1 introduces the Cybersecurity Skills Alliance – A New Vision for Europe (REWIRE) Project mission and its interconnection to the ECSF framework. Section 2 presents details of our Course Selection methodology. Section 3 shows the deployment of the methodology in the REWIRE project case. In the last section, we conclude this work.

1.1 The REWIRE Project mission

The REWIRE project [11] is a European initiative that aims to address the shortage of cybersecurity experts by improving the availability, accessibility, and quality of cybersecurity courses and certifications. To achieve this goal, the project has incorporated

the ECSF framework as a key reference point in its actions. Furthermore, a PESTLE analysis [13] has identified several challenges that directly affect the complexity of cybersecurity education and training. These challenges include the lack of relevant European regulatory frameworks, the complexity of the cybersecurity domain and the rapid technology and threat evolution, the lack of dedicated curricula and training and no clear identification of skills, the limited existence of Cyber Ranges and other tools, and the licensing costs and different licensing models of software in cybersecurity education. The analyses if the basement of the REWIRE European Cybersecurity Blueprint [3]. This document aims to advance the cybersecurity education in Europe. It covers several facets of cybersecurity education that the REWIRE project deems necessary.

The first aspect is a skills framework [12], which categorizes job profiles, skills, and knowledge necessary for cybersecurity education systematically. The framework builds upon pre-existing work such as ENISA ECSF, ESCO [2], and output from the pilot projects. The second aspect is an analysis of the attractiveness of the cybersecurity sector. This element investigates the job market and demand for cybersecurity professionals. The third element provides an analysis of tools for skills identification, aiding parties to generate more accurate job descriptions and course descriptions. The fourth element examines the tools for skills development, identifying programs and courses for acquiring skills and knowledge and career pathways to enable skills development over time. The final element is an analysis of a governance framework that describes how the cybersecurity skills framework could be maintained in the long term for the benefit of the European community. This European Cybersecurity Blueprint aims to promote cybersecurity education and maintain a cybersecurity skills framework for the benefit of the European community.

The REWIRE project has worked extensively on the 12 profiles included in version 0.5 of the ECSF proposed by ENISA, with the aim of enhancing the framework by addressing gaps in competencies, skills, and knowledge identified during the review of similar documents. The team's efforts include analyzing existing practices of ICT-03 pilots (CONCORDIA[1], ECHO[2], CyberSec4Europe[3], and SPARTA[4]), reviewing information within the profiles, examining existing information from other national and international cybersecurity skills frameworks, and correlating each task to the required knowledge, skills, and competencies.

One of the objectives of the REWIRE project is the creation of training courses. This paper presents the Course Selection methodology proposed by the REWIRE project, providing insights into the criteria used and the outcomes of the selection process. By presenting this methodology, the paper aims to contribute to the development of effective cybersecurity education programs that meet the needs of both the job market and the learners.

2 COURSE SELECTION METHODOLOGY

The methodology for selecting the occupational profiles is a crucial element in bridging the gap between the current state of cybersecurity education and the demands of the job market. The authors propose a multi-criteria selection method to ensure that the selected profiles meet the following objectives.

The first objective (O1) aims to guarantee the high quality of training materials. Criterion A, which examines the educational levels of ENISA Occupational Profiles, ensures that the materials cater to different levels of expertise, promoting comprehensive understanding and depth of knowledge. Additionally, Criterion C prevents redundancy in course design and ensures the inclusion of relevant and up-to-date information. The second objective (O2) focuses on meeting the current and future needs of the cybersecurity industry. Criterion B considers job market demand, aligning the courses with industry requirements. Criterion D gathers input from stakeholders to ensure the courses meet their needs and expectations. Criterion E incorporates practical exercises on the Cyber Range, reflecting evolving trends and developments. Lastly, the third objective (O3) centers on accessibility and benefit to a wide range of participants. Criterion A ensures the courses are accessible to learners with different expertise levels, while Criterion C offers diverse options tailored to participants' needs. Criterion F ensures the provided certification is widely recognized, promoting professional growth and career advancement for participants.

According to the presented objectives, six criterions were used for the Course Selection methodology:

(1) CRITERION A – Educational Levels of ENISA Occupational Profiles [O1, O3]
(2) CRITERION B – Demand of The Job Market [O2]
(3) CRITERION C – Already Available Courses [O1, O3]
(4) CRITERION D – Stakeholders' Input [O2]
(5) CRITERION E – Hands-on exercises on the Cyber Range [O2]
(6) CRITERION F – Certification [O3]

In the following subsections, these criterions are presented, along with their objectives, rationale, and methodology for scoring.

2.1 CRITERION A – Educational Levels of ENISA Occupational Profiles

Criterion A evaluates the educational levels of the ENISA Occupational Profiles in order to ensure that the training materials respond to different European Qualifications Framework (EQF) levels [15].

Based on that, the methodology proposes that the profiles present more levels are given higher scores due to the wide range of possible candidates. Also, for this reason, those that are in the lowest levels (introductory level), and in the highest levels (high expertise) are given lower score, while the others will be given medium scores. This allows for a fair scoring system that allows a wider range of participants to benefit from the designed training courses.

Criterion A - Scoring proposed

- Tier S - Score 5: 3 or more EQF levels represented
- Tier A - Score 4: medium EQF levels (closer to higher levels)
- Tier B - Score 3: medium EQF levels (closer to lower levels)
- Tier C - Score 2: higher EQF levels
- Tier D - Score 1: lower EQF levels

The main input collected for the Criterion A comes from the REWIRE Cybersecurity Skills Framework [12], which maps the

[1] https://www.concordia-h2020.eu/
[2] https://echonetwork.eu/
[3] https://cybersec4europe.eu/
[4] https://www.sparta.eu/

ENISA profile and the corresponding EQF levels, as it is shown in Table 1 in a simplified way.

Table 1: Criterion A - ENISA profiles and its corresponding EQF levels (simplified).

ENISA Profile	EQF levels	A
Chief Information Security Officer	4/5	2
Cyber Incident Responder	2/3/4	5
Cyber Legal, Policy & Compliance Officer	3/4	3
Cyber Threat Intelligence Specialist	3/4	4
Cybersecurity Architect	3/4	3
Cybersecurity Auditor	3/4	4
Cybersecurity Educator	2/3	1
Cybersecurity Implementer	2/3	1
Cybersecurity Researcher	2/3/4/5	5
Cybersecurity Risk Manager	3/4	3
Digital Forensics Investigator	3/4	4
Penetration Tester	2/3/4	5

It can be seen that most of the profiles are set between the EQF 2 and the EQF 4 levels. Cyber Incident Responder, Cybersecurity Researcher and Penetration Tester cover 3 EQF levels.

2.2 CRITERION B – Demand of The Job Market

The objective of Criterion B is to identify the ENISA profiles that are most in demand in the job market at the EU level. The goal of the course is to develop training materials to help upskill and reskill professionals and, also, to prepare students who can fill these job positions. The objective is increasing the pool of suitable candidates and successfully responding to the needs of the cybersecurity job market.

The methodology used was to analyze the demand of the job market at the EU level using job ads on the web. To match job titles with the ENISA Occupational Profiles, the team set the matching based on the requirements and skills described in each job ad. Scores for each profile varied based on the number of job ads linked to it, and different tiers were formed based on the distribution of the number of ads per profile. The higher tiers gave higher scores to the profiles entering in, while the lower tiers gave lower scores.

Criterion B - Scoring proposed

- Tier S - Score 5: Occurrences >50
- Tier A - Score 4: Occurrences >40
- Tier B - Score 3: Occurrences >30
- Tier C - Score 2: Occurrences >20
- Tier D - Score 1: Occurrences >10

The main source of the criterion has been the REWIRE Cybersecurity Job Ads Analyzer [14], a dynamic web application that collects and analyzes job ads using a machine learning algorithm to detect the skills required in advertised cybersecurity work positions. The Job Analyzer uses the ENISA ECSF in its analysis, allowing identifying which cybersecurity skills are needed in each profile from a job market point of view and anticipating future needs.

Table 2 shows how the ads are spread among the profiles. At the moment of the analysis, the database of job ads counted 358 entries.

Table 2: Criterion B - ENISA profile occurrences in the database.

ENISA Profile	Number	B
Cybersecurity Implementer	93	5
Cybersecurity Architect	50	5
Cyber Incident Responder	47	4
Chief Information Security Officer	32	3
Cyber Threat Intelligence Specialist	31	3
Penetration Tester	25	2
Cybersecurity Risk Manager	24	2
Cyber Legal, Policy & Compliance Officer	19	2
Cybersecurity Auditor	15	2
Cybersecurity Researcher	6	0
Cybersecurity Educator	4	0
Digital Forensics Investigator	3	0
Not Applicable	9	N/A
Total	358	N/A

2.3 CRITERION C – Already Available Courses

Criterion C aims to assess the number of existing curricula and trainings available for each of the ENISA Occupational Profiles. The main objective is to identify training gaps in the field of cybersecurity and deliver innovative and effective training methods through the courses. It was agreed that it is important not to duplicate existing courses and training materials, but rather to focus on delivering courses for Occupational Profiles with limited availability of training at the EU level.

The methodology aimed to map available courses at the EU level and match them with the 12 ENISA Occupational Profiles based on the competencies covered in the course. The score for each profile is based on the number of curricula and trainings linked to it, and different tiers are formed based on the distribution of the number of them per profile.

Criterion C - Scoring proposed

- Tier S - Score 5: Percentage <30
- Tier A - Score 4: Percentage <35
- Tier B - Score 3: Percentage <40
- Tier C - Score 2: Percentage <50
- Tier D - Score 1: Percentage <60

Table 3 depicts the percentage of ENISA profile coverage in the collected professional trainings and master and bachelor curricula. Specifically, the analysis was run on a total of 145 courses (86 cybersecurity curricula and 59 cybersecurity professional trainings) available in the database. Note that if we sum up the percentages, we would achieve a value bigger than 100. This is due to the fact that the same trainings covers skills and knowledge that are needed in different ENISA profiles. Moreover, the same curriculum can cover more profiles with different percentages.

The main source of the criterion has been the Cybersecurity Profiler [4], a web application that maps existing cybersecurity curricula, trainings, and certifications to work roles. This web application recommends courses for specific roles, and helps create study programs or certifications suited for specific roles. Figure 1

Table 3: Criterion C - corresponding curricula and trainings coverage in percentage per ENISA profile.

ENISA Profile	Percent	C
Cybersecurity Implementer	49	2
Cybersecurity Architect	55	1
Cyber Incident Responder	28	5
Chief Information Security Officer	31	3
Cyber Threat Intelligence Specialist	40	2
Penetration Tester	30	4
Cybersecurity Risk Manager	48	2
Cyber Legal, Policy & Compliance Officer	56	1
Cybersecurity Auditor	30	4
Cybersecurity Researcher	38	3
Cybersecurity Educator	45	2
Digital Forensics Investigator	47	2

depicts the ENISA profiles occurrences in the Cybersecurity Profiler curricula database.

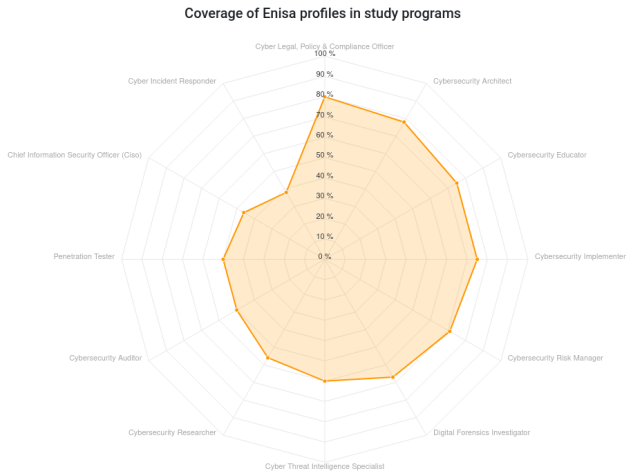

Figure 1: Statistical analysis in Cybersecurity Profiler.

2.4 CRITERION D – Stakeholders' Input

Criterion D involves utilizing the expertise of all stakeholders involved to grade the 12 ENISA Occupational Profiles. The partners were asked to grade the profiles based on their knowledge and perception of the importance of each profile, ensuring that the selected profiles respond to real needs. The partners' wide range of expertise includes academia, VET providers, and the job market, among others. The scoring has been distributed among the profiles based on the importance.

Criterion D - Scoring proposed

- Tier S - Score 5: 2 profiles with higher importance scores
- Tier A - Score 4: next 2 profiles with higher scores
- Tier B - Score 3: next 3 profiles with higher scores
- Tier C - Score 2: next 3 profiles with higher scores
- Tier D - Score 1: last 2 profiles with lower scores

The scores for each profile were based on the importance for the consortium and their stakeholders, with higher scores given to those deemed most important and feasible to create, as it shown in Table 4. 47 responses were collected from a questionnaire and the results were collected and normalized to 5, being 5 the maximum score of importance and 0 the minimum.

Table 4: Criterion D - normalized Importance perception (over 5) per ENISA profile by REWIRE partners and stakeholders.

ENISA Profile	Importance	D
Cybersecurity Educator	5	5
Chief Information Security Officer	5	5
Cybersecurity Implementer	4.9	4
Cyber Incident Responder	4.6	4
Penetration Tester	4	3
Cybersecurity Researcher	3.7	3
Cybersecurity Architect	3.6	3
Cybersecurity Risk Manager	3.4	2
Cyber Threat Intelligence Specialist	2.6	2
Cybersecurity Auditor	2.2	2
Digital Forensics Investigator	2.1	1
Cyber Legal, Policy & Compliance Officer	0.8	1

2.5 CRITERION E – Hands-on exercises on the Cyber Range

Criterion E focuses on the use of hands-on exercises in the REWIRE courses, specifically using the REWIRE Cyber Range based on the open-source KYPO Cyber Range Platform [10] developed by Masaryk university. KYPO CRP has been a reference in the cybersecurity training sector since they started in 2009 and they have been a key player in the European Projects CONCORDIA and CyberSec4Europe, allowing the creation of scenarios where different attack/defense tools are required. The Cyber Range is a unique training tool that supports practical activities and real case scenarios, meeting the needs of the job market and modern pedagogical approaches. It aims to create an interactive training that is appealing to learners, regardless of their status, and can lead to a larger number of participants.

In order to evaluate the relevance of the ENISA Occupational profiles related to the use of hands-on scenarios, a 3 Tier list was utilized. The first tier includes profiles which are considered essential for the training as they require practical knowledge of offensive/defensive tools and are focused on technical tasks. The second tier consists of profiles which are somewhat important for the training as they have a mixed focus on technical tasks and policies/management, and practical knowledge of offensive/defensive tools is beneficial. The third tier includes profiles which are deemed unnecessary for the training as they are focused on policies and management, and only theoretical knowledge of offensive/defensive tools is sufficient. This tiered approach allows for a more structured evaluation of the ENISA Occupational profiles and their relevance to the practical and theoretical aspects of the REWIRE project.

Criterion E - Scoring proposed

- Tier S - Score 5: Essential
- Tier B - Score 3: Important
- Tier D - Score 1: Unnecessary

The scores were provided by the KYPO CRP team and their experience. The profiles has been classified in three categories depending on the possible use of the Cyber Range: Essential, Important, and Unnecessary.

The cyber range is considered essential for the profile if the profile is focused on technical tasks and practical knowledge of offensive/defensive tools is necessary. The cyber range is considered important if the profile's focus is mixed between technical tasks and policies/management, and practical knowledge of offensive/defensive tools is beneficial. Using of the cyber range is considered unnecessary for profiles focused on policies and management or if theoretical knowledge of offensive/defensive tools is sufficient. This classification is depicted in Table 5.

Table 5: Criterion E - Cyber Range use categorization per ENISA profile.

ENISA Profile	Cyber Range	E
Chief Information Security Officer	Unnecessary	1
Cyber Incident Responder	Essential	5
Cyber Legal, Policy & Compliance Officer	Unnecessary	1
Cyber Threat Intelligence Specialist	Important	3
Cybersecurity Architect	Important	3
Cybersecurity Auditor	Important	3
Cybersecurity Educator	Important	3
Cybersecurity Implementer	Important	3
Cybersecurity Researcher	Important	3
Cybersecurity Risk Manager	Unnecessary	1
Digital Forensics Investigator	Essential	5
Penetration Tester	Essential	5

2.6 CRITERION F – Certification

Criterion F focuses on the existing certifications available for each of the 12 ENISA Occupational Profiles. The objective is to identify any gaps in the market or academic/VET field, and offer a training program that covers those specific needs. The aim is not to add another certification to those that already exist for an Occupational Profile. By mapping the existing certifications, the REWIRE project can ensure that the training program is more attractive than others available, and can cover specific gaps in the market. This criterion is important in order to provide a training program that meets the needs of learners and the job market.

The methodology used for mapping certifications to the ENISA Occupational Profiles involved two main factors. Firstly, the ability of the profiles to develop and implement a trustworthy certification scheme was considered. Secondly, a set number of certifications at the EU level were identified and matched to the relevant ENISA Occupational profiles. In some cases, a certification could be linked to more than one Occupational Profile to cover a wider range of roles and competencies. The roles of Cybersecurity Educator and Cybersecurity Researcher are not well-suited for a certification scheme, as the certifications already available for education cover the necessary skills, and the abstract and interdisciplinary nature of cybersecurity research makes it challenging to develop a meaningful certification for researchers.

Criterion F - Scoring proposed

- Tier S - Score 5: 1 to 2 certifications
- Tier A - Score 4: 3 to 5 certifications
- Tier B - Score 3: 6 to 10 certifications
- Tier C - Score 2: Over 10 certifications
- Tier D - Score 1: N/A

The Security Certification Roadmap [9] was used to map the existing certifications at the EU level and match them with the ENISA Occupational profiles. This approach aimed to identify the certifications that could be linked to each profile, covering a wider range of roles and competences. The focus was on identifying certifications that were well-established and reliable, rather than adding yet another certification to an already crowded market. In the following Table 6, the number of certifications registered per ENISA profile is shown.

Table 6: Criterion F - Certifications registered per ENISA profile.

ENISA Profile	Certifications	F
Cybersecurity Implementer	16	2
Digital Forensics Investigator	13	2
Penetration Tester	10	3
Cybersecurity Auditor	7	3
Cyber Threat Intelligence Specialist	6	3
Chief Information Security Officer	5	4
Cyber Legal, Policy & Compliance Officer	4	4
Cybersecurity Architect	3	4
Cyber Incident Responder	3	4
Cybersecurity Risk Manager	1	5
Cybersecurity Researcher	N/A	1
Cybersecurity Educator	N/A	1
Total	68	N/A

The final distribution of scores per ENISA profile and criterion is shown in Figure 2.

2.7 Final Score formula definition

After defining the six criterions (A-F), their scoring distribution and the associated inputs scored, the final Score Formula is defined in order to provide the weighted score per ENISA Profile. First of all, it is necessary to set the conditions. Each criterion must be weighted in order to consider the impact of the criteria in the final Score. Three levels are defined:

- Light: 1
- Medium: 1.5
- Heavy: 2

Based on the criteria (A-F) and their respective scoring distributions, the final Weighted Score formula (WScore) is calculated by multiplying the score of each criterion by its respective weight, summing all six weighted scores. In order to finalize the establishment of weights for the six criteria (A-F) in the Course Creation

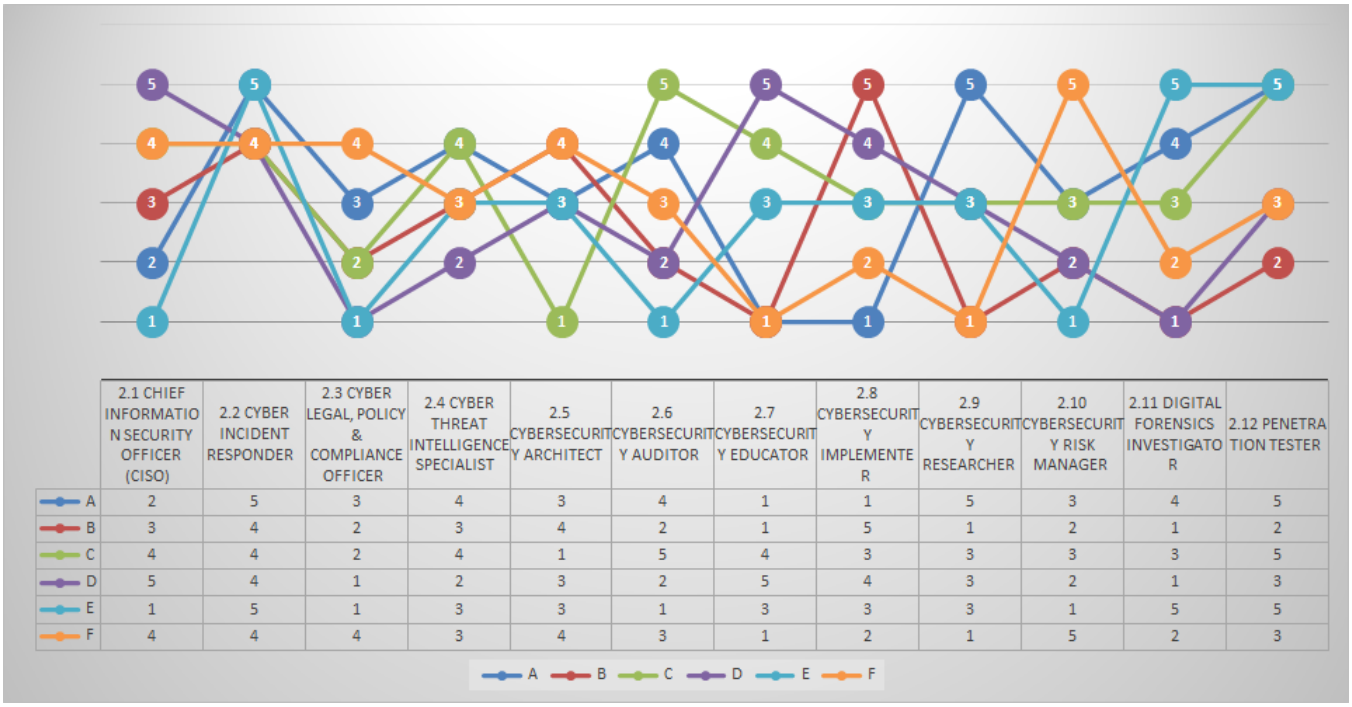

Figure 2: REWIRE final score (criterions A-F) per ENISA Profile.

related to Occupational Profiles from ENISA, a sensitivity analysis was performed to evaluate the impact of different inputs and assumptions on the results. The scoring formula was tested using different scores, and the weights of the criteria or the scores of the occupational profiles were varied to evaluate the robustness of the results. This analysis helped to ensure that the final weights for the criteria were appropriate and that the prioritization of course creation was accurate.

Mathematically, the formula can be expressed as: *WScore* = [(A x WA) + (B x WB) + (C x WC) + (D x WD) + (E x WE) + (F x WF)]

- A, B, C, D, E, and F are the scores obtained for each criterion.
- WA, WB, WC, WD, WE, and WF are the weights assigned to each criterion.

It is also considered, the Average Weighted Score formula (AWScore): *AvgWScore* = [(A x WA) + (B x WB) + (C x WC) + (D x WD) + (E x WE) + (F x WF)] x NumberOfCriterions

3 REWIRE COURSE SELECTION

In this section, the selection of the courses to be developed by the REWIRE project is presented. First of all, the weights are assigned to each criterion according to the three objectives (O1, O2 and O3), presented at the beginning of Section 2, that the selected courses need to meet:

Criterions - Weight proposed

- Criterion A - WA: Heavy (2)
- Criterion B - WB: Light (1)
- Criterion C - WC: Light (1)
- Criterion D - WD: Heavy (2)
- Criterion E - WE: Heavy (2)
- Criterion F - WF: Medium (1.5)

Second, following the WScore and AWScore formulas, the Occupational Profiles are prioritized considering their scores (A-F) and their associated weights (WA-WF). In the following table (Table 7), the ENISA profiles are sorted by the highest WScore score to the lowest:

Table 7: REWIRE final Scores - ENISA profiles priorization (WScore and AvgWScore)

ENISA Profile	WScore	AvgWScore
Cyber Incident Responder	42	4.3
Penetration Tester	37.5	3.8
Cyber Threat Intelligence Specialist	29.5	3.2
Chief Information Security Officer	29	3.2
Cybersecurity Architect	29	3.0
Cybersecurity Researcher	27.5	2.7
Cybersecurity Implementer	27	3.0
Digital Forensics Investigator	27	2.7
Cybersecurity Auditor	25.5	2.8
Cybersecurity Educator	24.5	2.5
Cybersecurity Risk Manager	24.5	2.7
Cyber Legal, Policy & Compliance Officer	20	2.2

It can be seen that the Chief Information Security Officer and the Cybersecurity Architect have the same WScore. For this reason, the AvgWScore is used to break the tie. Finally, the profiles are selected for the REWIRE Course creation:

Selected profiles by the REWIRE project

- Chief Information Security Officer (CISO)
- Cyber Incident Responder
- Cyber Threat Intelligence Specialist
- Penetration Tester

After the selection of these four ENISA profiles, the next steps are the definition of the syllabus and, the design and creation of the training contents. Also, the certification schemes are going to be defined. Finally, the four training courses are going to be available in the REWIRE Virtual Learning Environment at the end of 2023.

4 CONCLUSIONS

The ECSF framework aims to identify and specify the necessary tasks, competencies, skills, and knowledge required for European cybersecurity professionals. In particular, this framework condenses all cybersecurity-related positions into 12 role profiles. The REWIRE project aims to address the shortage of cybersecurity experts by improving the availability, accessibility, and quality of cybersecurity courses and certifications, and it has incorporated the ECSF as a key reference point in its actions.

To do so, Course Selection methodology was designed to contribute to the development of effective cybersecurity education programs that meet the needs of the job market and learners. The authors propose a multi-criteria approach to ensure high-quality profiles that meet industry needs. The methodology has three objectives: first, to ensure high-quality training materials that provide comprehensive knowledge and up-to-date information; second, to meet current and future industry requirements; and third, to make the training accessible to a wide range of participants. Six criteria were employed: Criterion A assesses educational levels to align with the European Qualifications Framework (EQF); Criterion B identifies profiles in high demand in the EU job market; Criterion C avoids redundant courses; Criterion D considers stakeholder input; Criterion E evaluates practical exercises on the Cyber Range, and Criterion F verifies certification recognition. The methodology assigns scores to each criterion, ranking the profiles and selecting the most relevant ones for course design.

Moreover, the authors define the final score formula for ENISA profiles selection for the REWIRE project. The formula takes into account the weights assigned to each criterion (A-F) and their associated inputs scored. In particular, a sensitivity analysis is performed to evaluate the impact of different inputs and assumptions on the results. The authors assign weights to each criterion according to the three objectives (O1, O2, and O3) that the selected courses need to meet. Finally, based on the WScore and AWScore formulas, the authors prioritize the ENISA profiles and select the Chief Information Security Officer (CISO), Cyber Incident Responder, Cyber Threat Intelligence Specialist, and Penetration Tester for the REWIRE Course creation.

As the REWIRE project has selected the occupational profiles to prioritize for course creation, the next step is to define the syllabus (topics, learning objectives, and assessment methods, among other sections) for each of the selected profiles. The syllabus will guide the development of the training contents for each profile. After the training contents are developed, they will be tested and refined through a pilot program. The pilot program will provide an opportunity to evaluate the effectiveness of the training contents and make necessary adjustments before the final release.

ACKNOWLEDGMENTS

The following funding source is gratefully acknowledged: the ERASMUS+ programme of the European Union (grant 621701-EPP-1-2020-1-LT-EPPKA2-SSA-B 'REWIRE').

REFERENCES

[1] 2020. Cybersecurity Professionals Stand Up to a Pandemic. https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B

[2] Filippo Chiarello, Gualtiero Fantoni, Terence Hogarth, Vito Giordano, Liga Baltina, and Irene Spada. 2021. Towards ESCO 4.0–Is the European classification of skills in line with Industry 4.0? A text mining approach. *Technological Forecasting and Social Change* 173 (2021), 121177.

[3] Herve Debar. 2022. REWIRE-WP3 European Cybersecurity Blueprint. https://rewireproject.eu/wp-content/uploads/2022/11/REWIRE_R3.2.1_European-cybersecurity-blueprint_Final_ForRelease-1.pdf

[4] Petr Dzurenda and Sara Ricci. 2022. REWIRE-WP3 Mapping the framework to existing courses and schemes. https://rewireproject.eu/wp-content/uploads/2023/03/REWIRE_R3.4.1_Deliverable-v8-Final-EC-Check.pdf

[5] European Cyber Security Organisation (ECSO). 2018. Gaps in European Cyber Education and Professional Training. https://ecs-org.eu/documents/publications/5fdb282a4dcbd.pdf

[6] ENISA. 2004. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/

[7] ENISA. 2022. European Cybersecurity Skills Framework Role Profiles. https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

[8] (ISC)^2. 2022. (ISC)^2 Cybersecurity Workforce Study. https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

[9] Paul Jerimy. 2017. Security Certification Roadmap. https://pauljerimy.com/security-certification-roadmap/

[10] Masaryk University (MRU). 2013. KYPO Cyber Range Platform (KYPO CRP). https://crp.kypo.muni.cz/

[11] REWIRE. 2020. REWIRE: Cybersecurity Skills Alliance - A new Vision for Europe. https://rewireproject.eu/

[12] REWIRE. 2022. WP3 Cybersecurity skills Framework. https://rewireproject.eu/wp-content/uploads/2022/11/R3.3.1.-Cybersecurity-Skills-Framework_FINAL.pdf

[13] Sara Ricci, Vladimir Janout, Simon Parker, Jan Jerabek, Jan Hajny, Argyro Chatzopoulou, and Remi Badonnel. 2021. PESTLE Analysis of Cybersecurity Education. In *Proceedings of the 16th International Conference on Availability, Reliability and Security*. 1–8.

[14] Sara Ricci, Marek Sikora, Simon Parker, Imre Lendak, Yianna Danidou, Argyro Chatzopoulou, Remi Badonnel, and Donatas Alksnys. 2022. Job Adverts Analyzer for Cybersecurity Skills Needs Evaluation. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*. 1–10.

[15] European Union. 2023. Europen Qualification Frameworks. https://europa.eu/europass/en/europass-tools/european-qualifications-framework

Received 20 February 2007; revised 12 March 2009; accepted 5 June 2009