REWIRE - Cybersecurity Skills Alliance: A New Vision for Europe

Matthews Jose[1], Rémi Badonnel[1], Thibault Cholez[1], Hervé Debar[2], Olivier Levillain[2], and Grégory Blanc[2]

[1]Université de Lorraine, {matthews.jose,remi.badonnel,thibault.cholez}@univ-lorraine.fr
[2]Telecom SudParis, {herve.debar,olivier.levillain,gregory.blanc}@telecom-sudparis.eu

PROJECT DETAILS

- Project name and acronym: REWIRE – Cybersecurity Skills Alliance: A New Vision for Europe
- Project lead and affiliation (in France): TELECOM SudParis/IMT, TELECOM NANCY/University of Lorraine
- Consortium: Mykolas Romeris University and various research institutions, universities, and companies from several European countries, including France, Italy, Spain, Cyprus, Greece, Austria, Norway, Portugal, Czech Republic, Lithuania, Hungary, and Sweden
- Funding: Grant Agreement with the Erasmus+ program (621701-EPP-1-2020-1-LT-EPPKA2-SSA-B) for a duration of four years
- Project start and end dates: Q2 2020 to Q4 2024
- Associated TRL range for innovations: N/A

INTRODUCTION

The rise of the internet and proliferation of smart devices has led to an increase in the number of cyber threats, such as denial of service, data theft, and ransomware. These threats pose a risk to both individuals and organizations, as sensitive information and financial assets can be compromised. The shortage of skilled engineers and security personnel exacerbates the problem, as there is a limited pool of resources to defend against these threats. As a result, it is essential for governments to promote cybersecurity and invest in training and resources to prevent and respond to these threats. The REWIRE project is a European cybersecurity project that aims to address this skill gap in the European Union [5]. The project brings together a wide range of partners from academia, vocational education and training, the cybersecurity industry, non-cyber industries, certification partners, and umbrella organizations. The project builds upon the work of four pilot projects: CONCORDIA [1], SPARTA [6], ECHO [3], and CyberSec4Europe [2].

OBJECTIVES

The main goal of the project is to address the current and future cybersecurity skills gap in Europe by developing a comprehensive skills strategy and blueprint for the cybersecurity industry. The project is developing a set of recommendations for the industry, educational institutions, and policymakers on how to improve the cybersecurity skills of the workforce. It is also building a set of educational materials and resources that can be used to train and educate cybersecurity professionals, and is working to promote the recognition and certification of cybersecurity skills across Europe. This can be summarized as the following:

- Innovation: development of the European Cybersecurity Blueprint, the European Cybersecurity Skills Framework, and training programs in cutting-edge fields, creation of a digital Skills Observatory to merge market needs, profiles, competencies, and training courses.
- Impact: involvement of all stakeholders in exploiting the potential of cutting-edge subjects for growth and jobs in the cybersecurite de Lorraine, (thibault.cholez,remi.badonnel,matthews.jose)@univ-lorraine.fry sector, promotion of cyber ranges and the application of quality and transferability frameworks.
- Sustainability: creation of a lasting partnership of stakeholders to monitor and adapt to changes in the sector's needs, and facilitation of transnational mobility and transversal skills, career guidance, and access to the labor market to improve long-term employability.

RESULTS

The key issue highlighted in REWIRE is the limited demand for cybersecurity skills from prospective applicants, demonstrated by the number of unfilled seats in cybersecurity training programs. This is due to a lack of awareness of cybersecurity threats and a lack of a common skills framework. This has resulted in a mismatch between supply and demand in cybersecurity skills. Proposals are needed to increase the attractivity of the careers including promoting cybersecurity as a career choice, fostering gender balance, providing reliable information on cybersecurity skills, and connecting stakeholders. The results have been summarized in the project blueprint, detailed in [7].

So far the project has consolidated and extended course identification maps and integrated 85 university curricula, 59 professional trainings, and 15 certification schemes to provide a comprehensive coverage of the field. The mapping strategy guarantees consistency by using a mapping methodology that fits within the ENISA framework [4] and highlights relationships among different profiles. The project also promotes a dynamic web application, called Cybersecurity Profiler, that enables mapping curricula, professional trainings and certification schemes to cybersecurity skills, knowledge, and profiles, and serves as a support to determine existing courses or to drive the elaboration of new courses that are relevant for specific cybersecurity profiles.

REFERENCES

[1] Concordia: Cybersecurity Competence for Research and Innovation. URL: https://www.concordia-h2020.eu/.

[2] Cybersec4europe - Working Together to Boost the Security of all Citizens of the European Union in their Everyday Digital Transactions. URL: https://cybersec4europe.eu/.

[3] Echo network: The European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations. URL: https://echonetwork.eu/.

[4] ENISA: The European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/.

[5] REWIRE: Cybersecurity Skills Alliance – a new vision for Europe. URL: https://rewireproject.eu/.

[6] SPARTA: Building a European Cybersecurity Network. URL: https://www.sparta.eu/.

[7] REWIRE: European Cybersecurity Blueprint. URL: https://rewireproject.eu/blueprint/.