REWIRE
CYBERSECURITY SKILLS ALLIANCE

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

REWIRE - Cybersecurity Skills Alliance
A New Vision for Europe

R.5.1.1 CyberABILITY Platform

Title	R5.1.1 CyberABILITY
Document description	The present deliverable serves as a short description of the CyberABILITY platform. This deliverable is complementary to T5.1 whose main output is the platform.
Nature	Public
Task	T.5.1 Design and Development of the Digital European Cybersecurity Skills Observatory
Status	Draft
WP	WP5
Lead Partner	TUC
Partners Involved	All
Date	06/03/2024

Disclaimer:

Contents

EXECUTIVE SUMMARY

The CyberABILITY platform emerges as a publicly available, digital online hub, designed to bridge the existing gap in the cybersecurity domain across Europe. It is a publicly accessible platform that provides insights into the job market, competencies, training courses, and certification schemes. This platform not only serves as a bridge between demand, abilities, and training resources but also fosters knowledge sharing and intra-institution collaboration, thereby significantly enhancing the cybersecurity skill set across the continent.

Through regular updates in the last year of the REWIRE project, the CyberABILITY platform will substantially address the cybersecurity skills gap, making it an asset in the evolving cybersecurity landscape.

1. REWIRE CYBERABILITY PLATFORM

1.1. Technology Stack

1.1.1. Back-end

CyberABILITY's backend infrastructure is built upon the robust combination of PHP and MySQL, ensuring a seamless and efficient data management system. PHP, known for its server-side scripting capabilities, facilitates dynamic content delivery, while MySQL, a renowned relational database management system, ensures data integrity and swift retrieval. Together, they form the backbone of the CyberABILITY platform, providing a stable, scalable, and secure environment that can handle vast amounts of data and user interactions, ensuring optimal performance and reliability for its users.

In particular, the server part of the application consists of several PHP (i.e., PHP: Hypertext Preprocessor) scripts, located on the web server next to the source JavaScript codes of the client part. These server scripts handle requests coming from clients' Internet browsers and serve as an intermediary for data manipulation. Each script is for a specific action. They are triggered by a query for a specific URL such as *https://SERVER_URL/addJob.php*. The scripts require specific data in the query body according to the required operation, as well as an authorization token. They will read or write data to the application database based on a valid request. The connection to the database is provided by PHP Data Objects (PDO), which helps to prevent SQL injection and character set inconsistencies by design.

1.1.2. Front-end

CyberABILITY’s frontend is developed using ReactJS, a JavaScript library known for its efficiency in building interactive user interfaces. Specifically, the platform leverages the Antd package, a high-quality React component library that offers a suite of rich UI elements and

widgets. This combination ensures that CyberABILITY's frontend is not only responsive and user-friendly but also aesthetically pleasing, adhering to modern design principles.

1.1.3. Version Control

Git is used as a version control system, ensuring a streamlined and efficient development process. Using git, developers from BUT and TUC who are the technical partners involved in the development process, can track modifications, collaborate seamlessly across different features, and maintain a comprehensive history of code changes. This adoption not only safeguards the integrity of the platform's codebase but also facilitates agile development, allowing for rapid iterations and adjustments.

1.2. Components

1.2.1. Cybersecurity Job Ads Analyzer

Cybersecurity Job Ads Analyzer is a dynamic web application to identify which cybersecurity skills are required in a work role. The tool has four main views: **1) The database**, **2) The Machine Learning (ML) result**s, **3) Create your ad** tab, and **4) The statistics** tab. The **database** allows users to add job adverts and filter the adverts using several fields such as country and year. When this deliverable was submitted, the Job Ads Analyzer counted 938 jobs inserted thanks to the joint effort of the whole REWIRE consortium. The database is depicted in Figure 2. The application database is implemented on the same machine via the MySQL server MariaDB. The database currently contains only a table with users and a table with job adverts. The job table contains, in addition to the values displayed on the web, dozens of other parameters that act as raw truths for the ML algorithm. For a better visualization, a map showing the number of job ads per country has been developed as shown in Figure 1. In the map, job adverts are split per country and several filter options are also available.

Figure 1 - The map

Furthermore, Job ads can easily be added through the application, as shown in Figure 2, after creating an account in the platform.

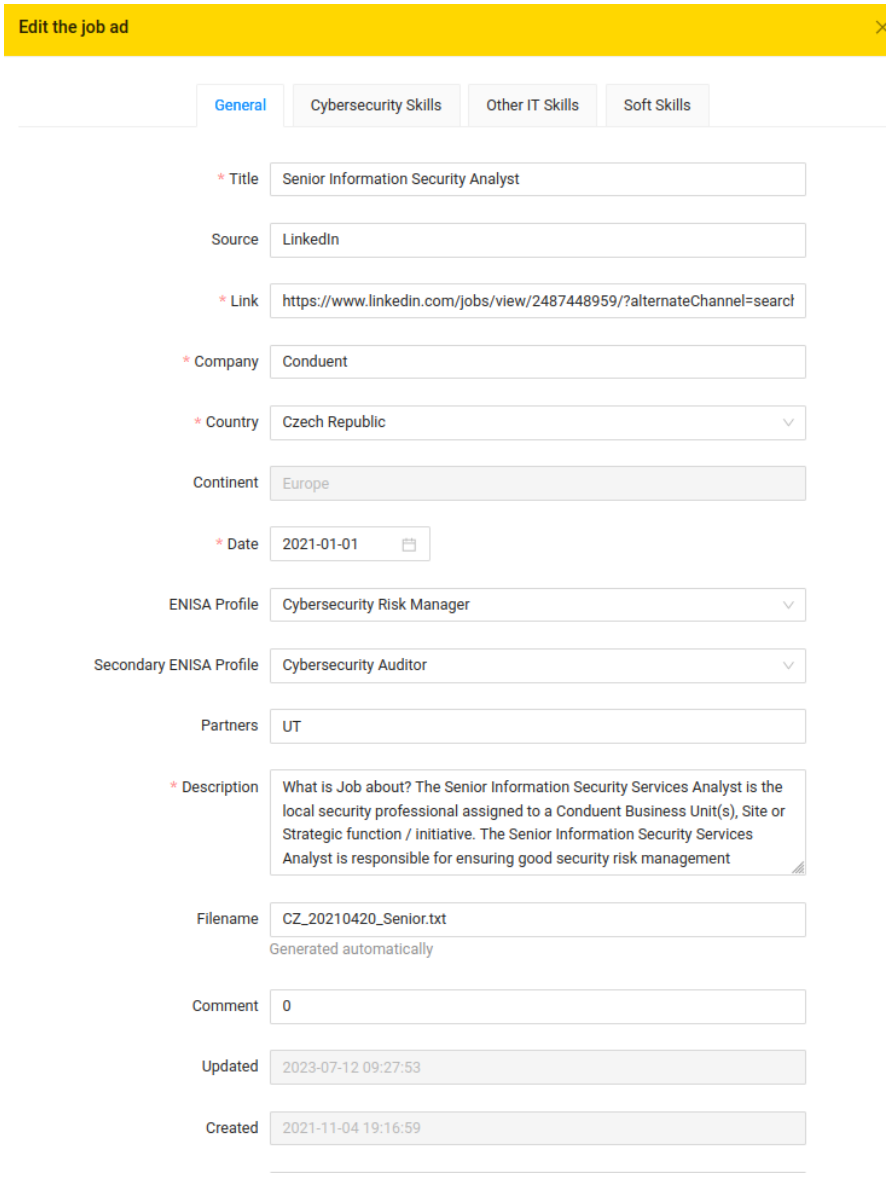

Figure 2 - The Add Job tab

ML results show the identified cybersecurity skills within the selected job adverts. The analysis of skills needs in the market started to be developed in WP2 and fed in WP3. This tool supports the achieved results. We refer to R3.6.1 European Cybersecurity Blueprint for more details. The ML algorithm for skill prediction and keyword processing is implemented as a Python program. The program consists of a tokenizer and an LSTM model. The machine learning model can also be re-created and re-learned. The ML program is stored on the webserver in a sub-directory of web content. When requesting data processing by the ML algorithm, an HTTP request is sent from the client application to a PHP script which, in the first step, reads all the necessary data from the database and creates a dataset in a temporary directory on the server. In the second step, the PHP script executes the terminal command using *exec* function to run the Python ML program. After performing the ML analysis, the program outputs the return code back to the PHP script and creates the analysis output files

in a temporary folder. The PHP script then loads these files, processes them, and sends the results back to the client application for viewing by the user. This tool has already been extended to adopt the ENISA framework. A new field "Profile" allows assigning the ENISA profile to the job ads. Therefore, by selecting the job ads related to a profile one can compare the skills assigned to it in the framework to the ones suggested by the labor market. The database with the possibility to select ads related to a specific ENISA profile is shown in Figure 3.

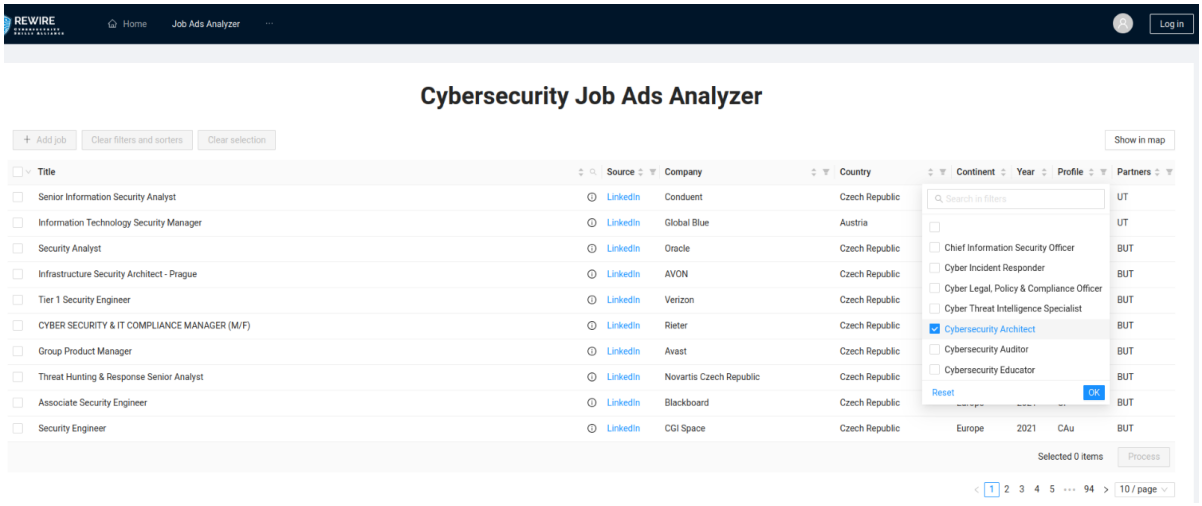

Figure 3 - The database

The **create your ad** environment supports the design of a new ad with the analysis of the provided text. A user can use the ML algorithm to check which skills are in its description and compare them with the ones normally proposed in similar job ads through the ENISA characterization. Figure 4 shows the analysis of a description meant for a cybersecurity architect with identified skills and match to ENISA profiles. By pointing on the coverage of a profile, a list of suggested skills is provided.

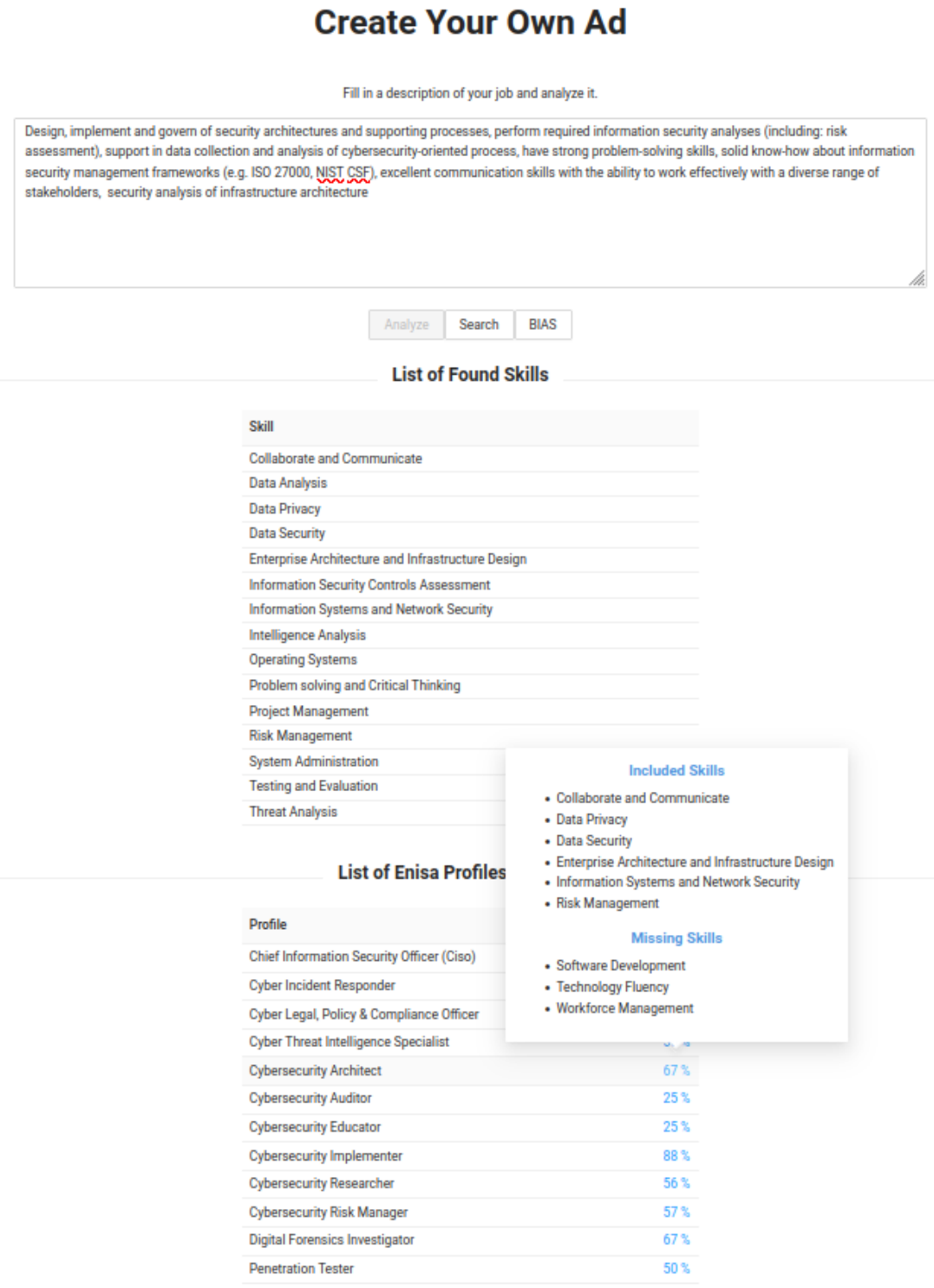

Figure 4 - Create your ad tab

Moreover, a gender balance analysis can be run on the text and, in case the text is found gender-oriented, an alternative text is provided with the help of a ChatGPT model. This analysis can be applied by pushing on the button BIAS.

Finally, the **statistic** tab shows the ML results on the whole dataset, i.e., the top 10 skills identified and the radar plot of the skills occurrences. Figure 5 depicts the results.

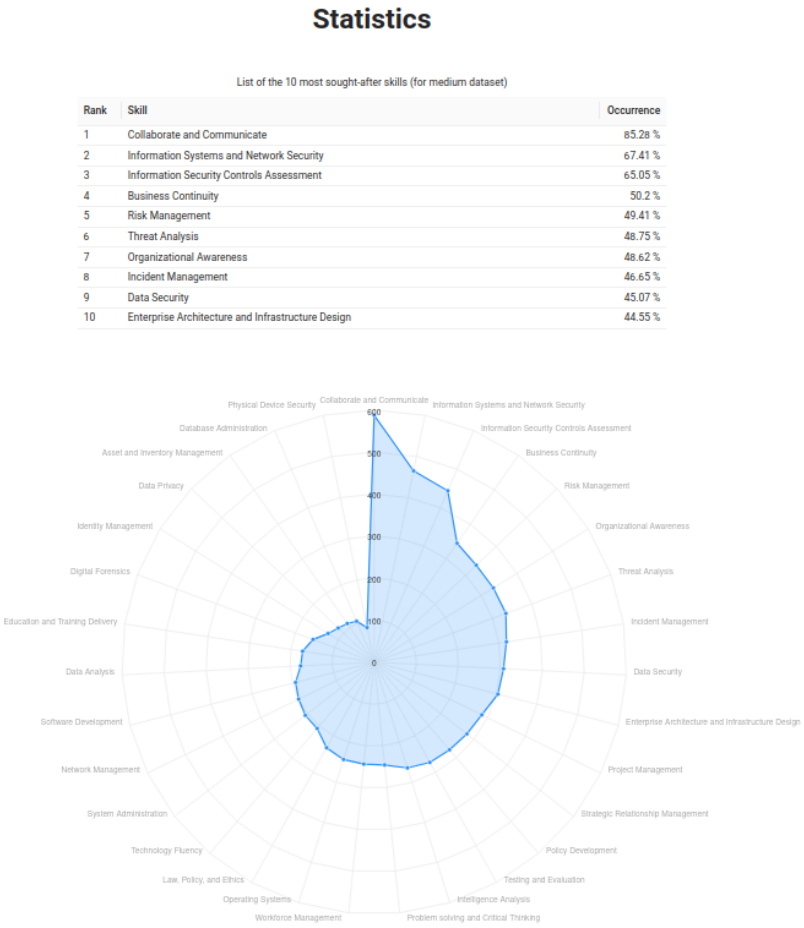

Figure 5 - Statistics tab

1.2.2. Cyber Security Profiler

The Cyber Security Profiler has been created to collect and analyze cybersecurity skills in curricula, trainings, and certification schemes. Moreover, this app helps to create a bridge between demand and offer in cybersecurity with a clear career path starting from the studied skills to the work roles that can be achieved. Filtering features and statistics are shown as well as the possibility to create your curricula, certification, or training while having on-time statistics and connection to the ENISA profile and NICE work roles.
The Cyber Security Profiler (CSP) is built on Cybersecurity Curricula Designer (CCD-v2) and will extend it with additional features. It must be emphasized that the CCD is a result of SPARTA, while CSP will be a result of REWIRE. The main differences are:

1. The CSP app will extend the CCD-v2 by cybersecurity trainings and certifications. helps users to create new or upload existing trainings or certifications in compliance with ENISA requirements.

2. Furthermore, the CSP app allows uploading/creating databases of existing curricula, trainings, and certifications with bilateral flow

For more information we refer to R3.4.1 Mapping the framework to existing courses and Schemes.

The tool has three main views: 1) **Curricula**, 2) **Training**, and 3) **Certification**.

These environments have similar features, for instance, in curricula a user can create courses, drag them in the central column and several statistics will be displayed. Figure 6 sketches an example of curricula courses and statistics.

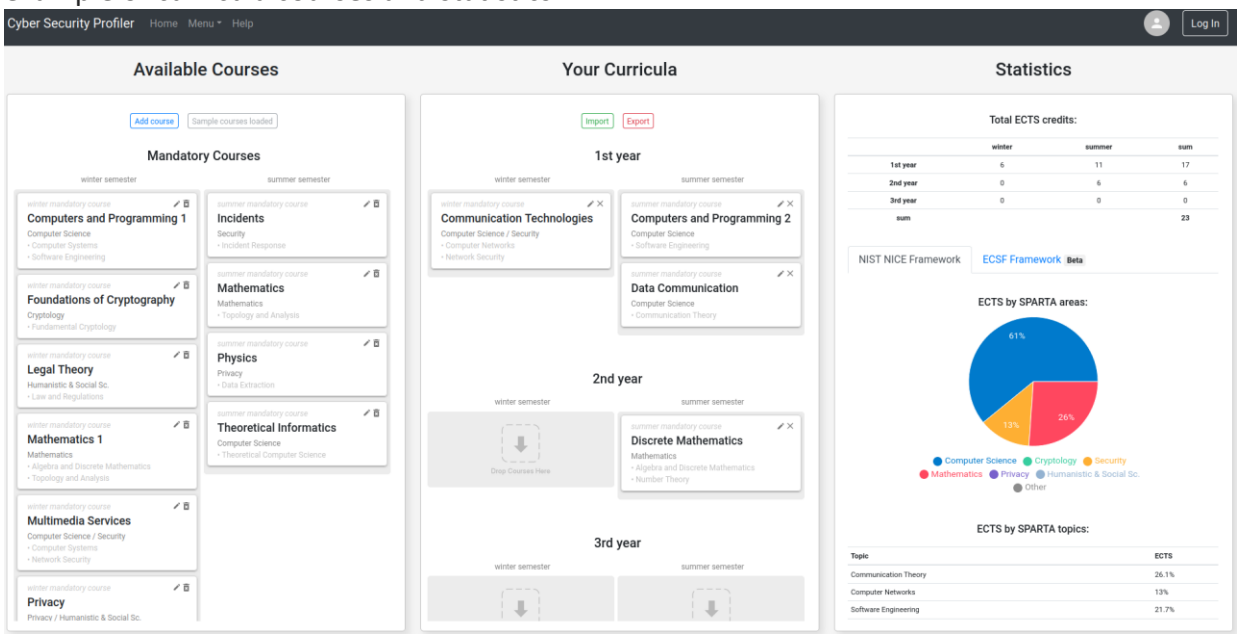

Figure 6 - Curricula tab

Moreover, a user can export and then import its work any time. This tool is also a database, therefore, a user can either create and analyse a created curriculum, training, or certification scheme or brose in the dataset. Figure 7 shows a filtering of the available trainings. The training information are provided such as language, description, and skill coverage. Once the trainings are selected, they can be loaded and analyzed in a similar environment as in Figure 6 for curricula.

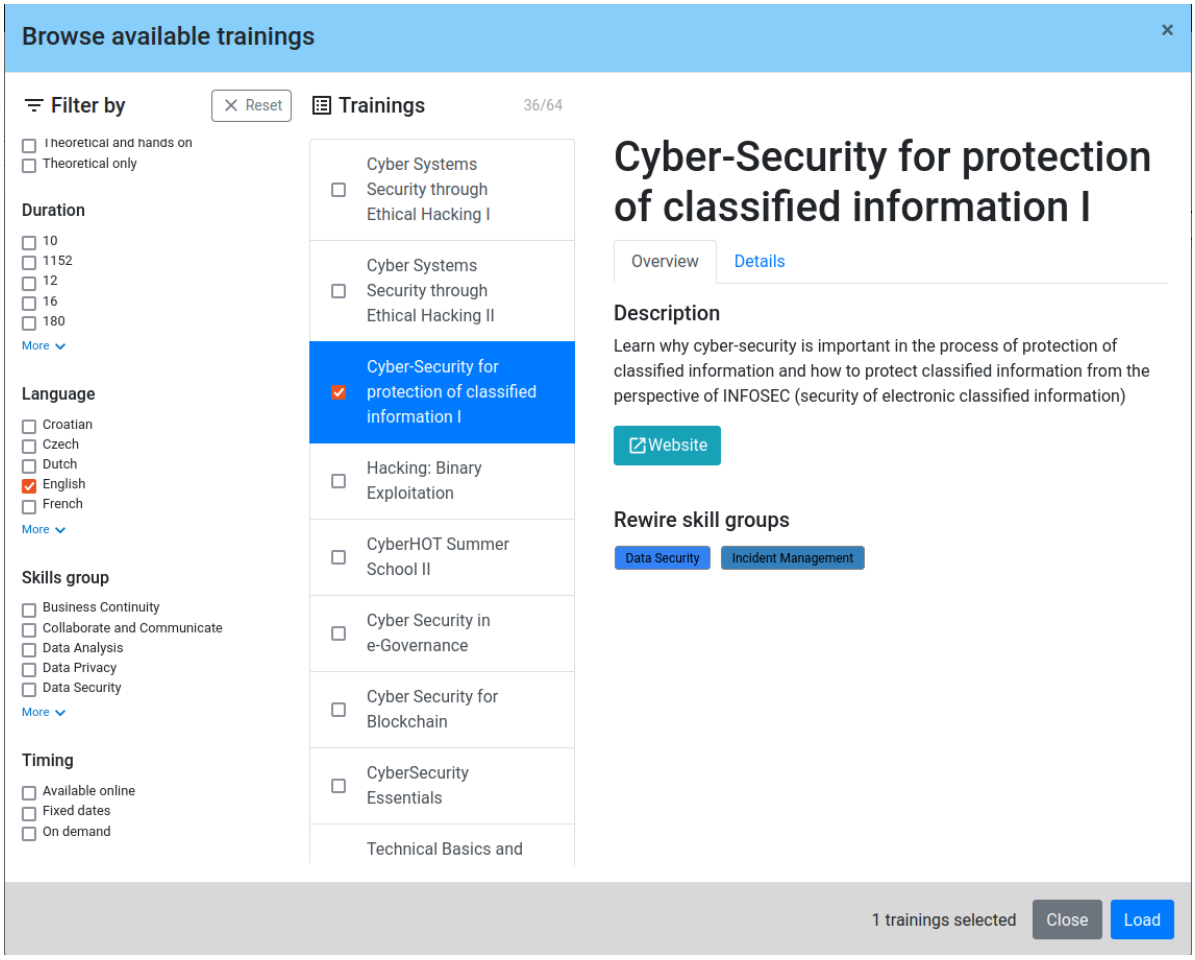

Figure 7 - Browse available traings tab

The CS Profiler app among other trainings, also interfaces the "CONCORDIA interactive map of trainings"[1]. One can explore the trainings and have a detailed overview of the percentage-based profile matching.
In the picture below, the "Cyber Incident Handling Workshop" offered by Airbus Cybersecurity and also present in the CONCORDIA map, is analyzed.

[1] https://www.concordia-h2020.eu/map-courses-cyber-professionals/

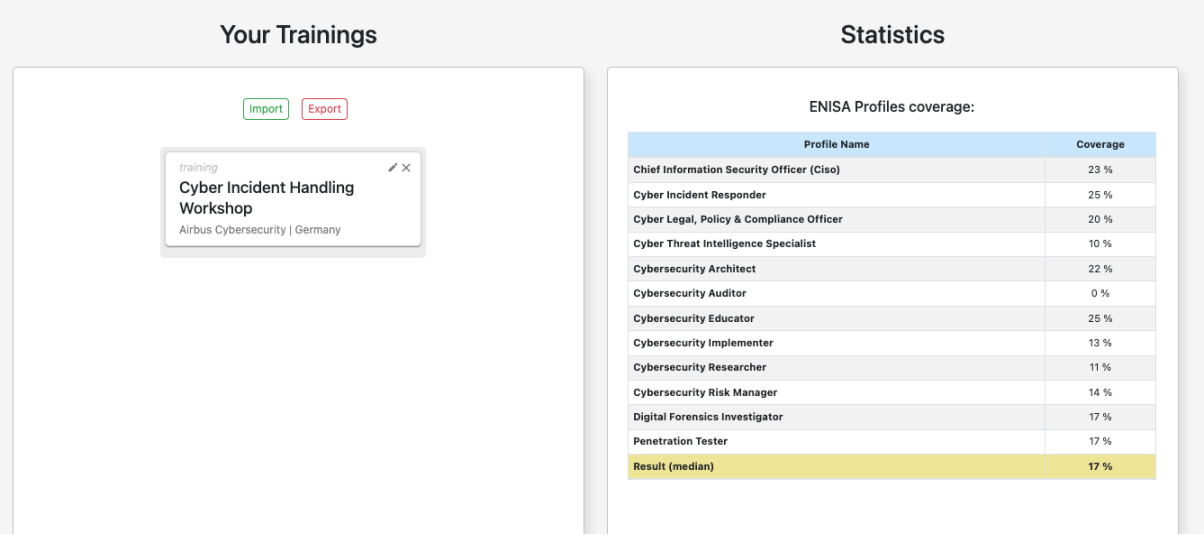

Figure 8 - Example ECSF Profile Training Coverage

1.2.3. ECSF Explorer

The ECSF Explorer is a tool that enables users to explore the ECSF (European Cybersecurity Skills Framework)[2] interactively. Figure 7 shows its main view. By clicking on the roles, users can view alternative titles, summary statements, missions, deliverables, main tasks, key skills, key knowledge, and e-competences. Within the e-competences section, hovering over the level tags reveals their descriptions.

The primary objective of this application is to provide a more efficient and user-friendly alternative to the traditional method of manually searching through the document. Instead of spending valuable time and effort scrolling through pages and trying to locate specific information, users can now leverage this web-based tool. By transitioning to this application, users can not only save time but also enhance their overall experience.

Following similar styling and layout, depending on the current work in progress of the REWIRE project, information can be added/edited/removed from this tool.

[2] https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

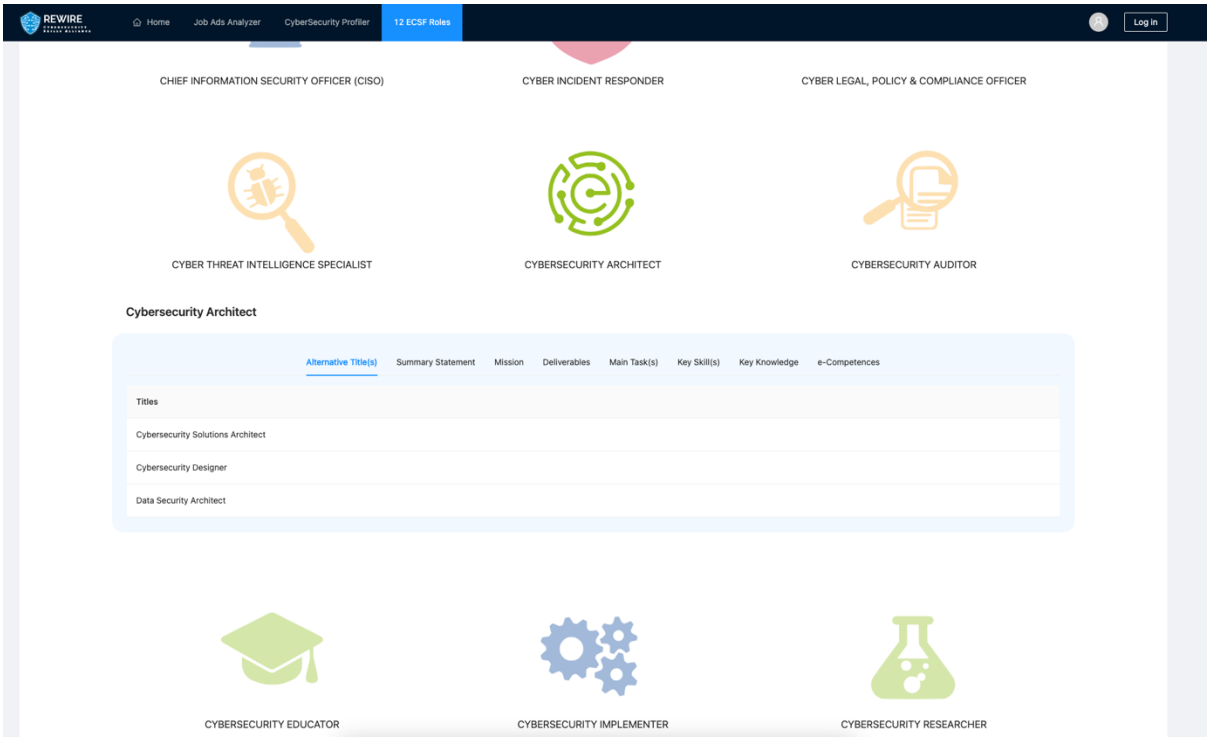

Figure 9 - ECSF Explorer

1.2.4. Career Path / Development

The Career Path/Development tool is designed to help users self-manage their career path and development, simply by targeting a Cybersecurity Role profile. This tool is very easy to use as it consists of 4 simple steps, which are illustrated in figures 10, 11, 12 and 13, respectively, where users can navigate by selecting boxes and clicking the “Next” button. At each step they are allowed to go back to the previous one by clicking the "Back" button.

1. **Role Selection:** users can choose one of the 12 ECSF roles explored in the ECSF Explorer tool, namely:
   - 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
   - Penetration Tester

2. **Skills Selection:** depending on the role selected in the first step, a different list of skills appears, from which users can select those they already own.
3. **Knowledge Selection:** similarly, users can select the knowledge they already possess from the list displayed in this step.
4. **Cybersecurity Career Pathway:** a list of skills and knowledge that remain to be acquired so that users can reach their desired role they selected in step one. For further assistance, the tool invites users to navigate the official REWIRE project platforms of Cyber Range[3], Online Courses[4] and Certification[5] to continue their upskilling/reskilling journey. Finally, as shown in figure 14, in this last step users have the option to export the results to a pdf file, which is illustrated in figure 15, by clicking on the "Export" button.

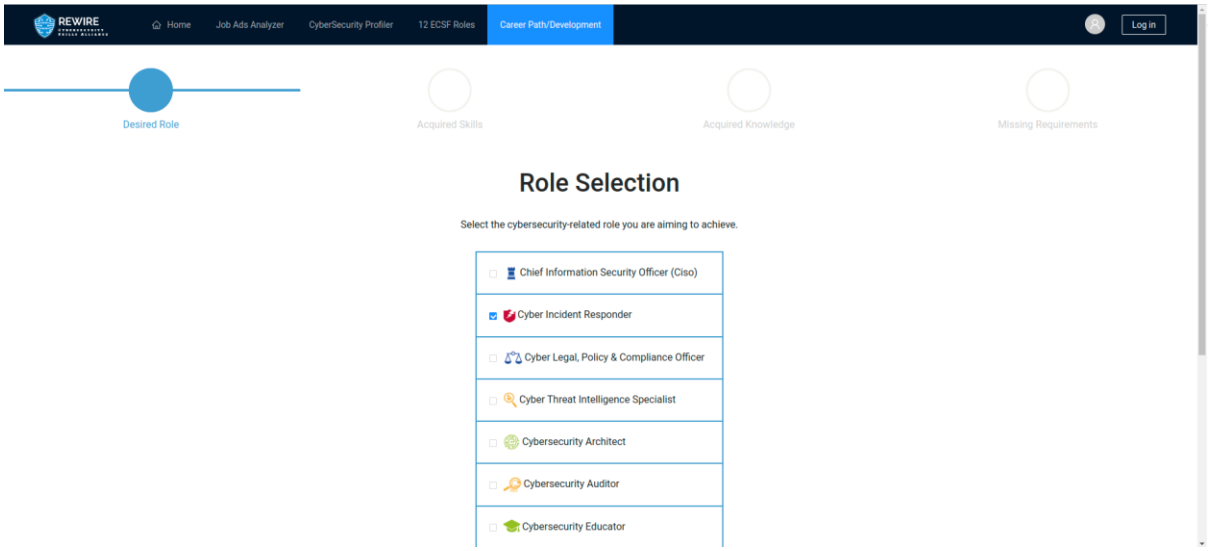

Figure 10 - Career Path/Development, Step 1 – Role Selection, example of Cyber Incident Responder role

[3] https://rewireproject.eu/cyber-range/
[4] https://vle.rewireproject.eu/
[5] https://rewireproject.eu/certification/

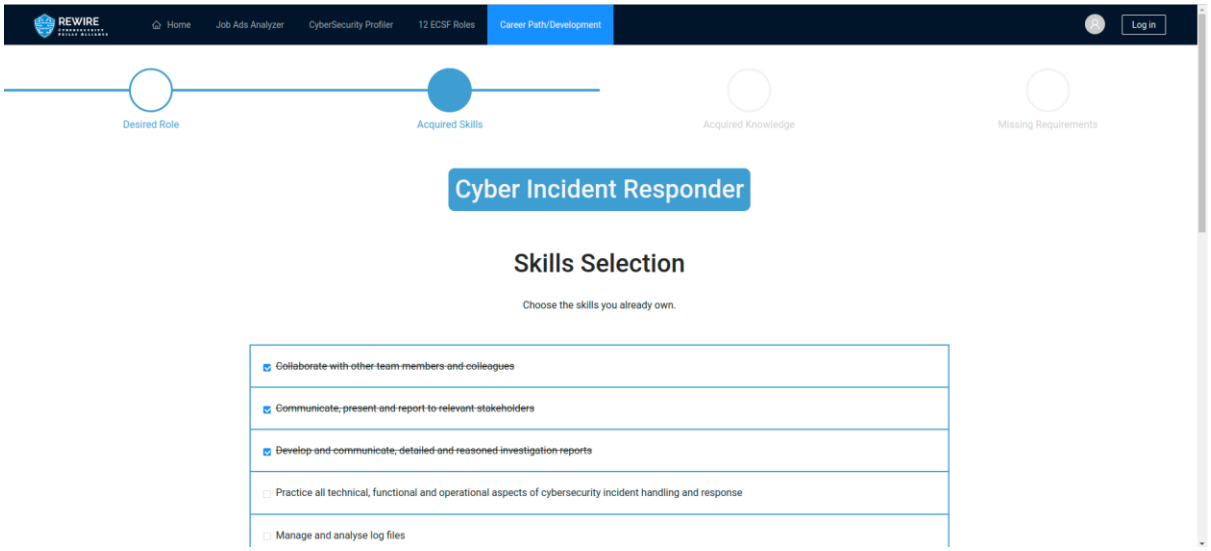

Figure 11 - Career Path/Development, Step 2 – Skills Selection, example of Cyber Incident Responder role

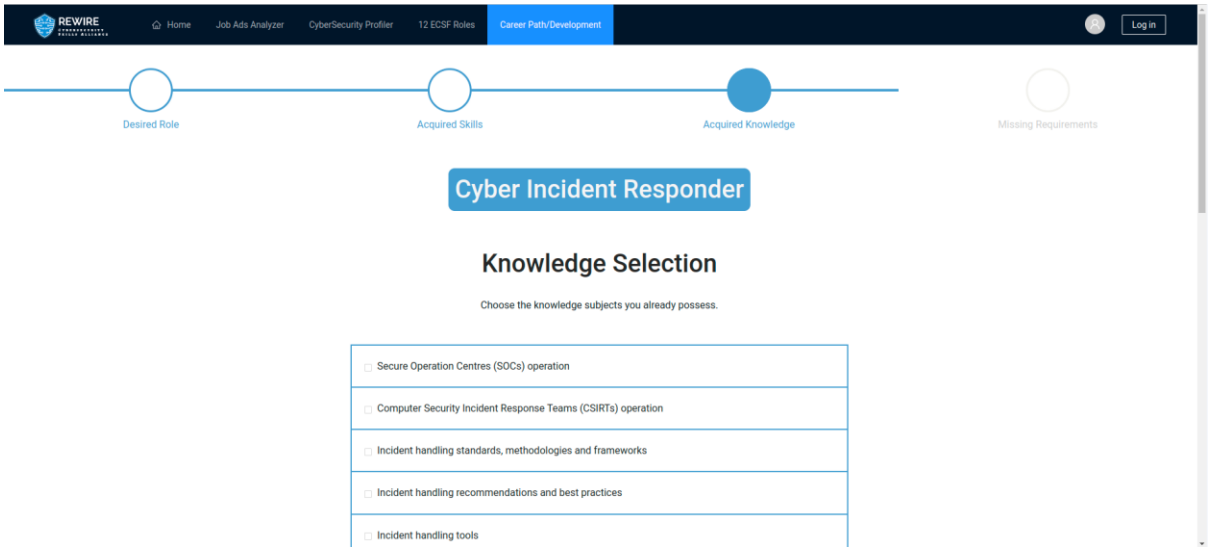

Figure 12 - Career Path/Development, Step 3 – Knowledge Selection, example of Cyber Incident Responder role

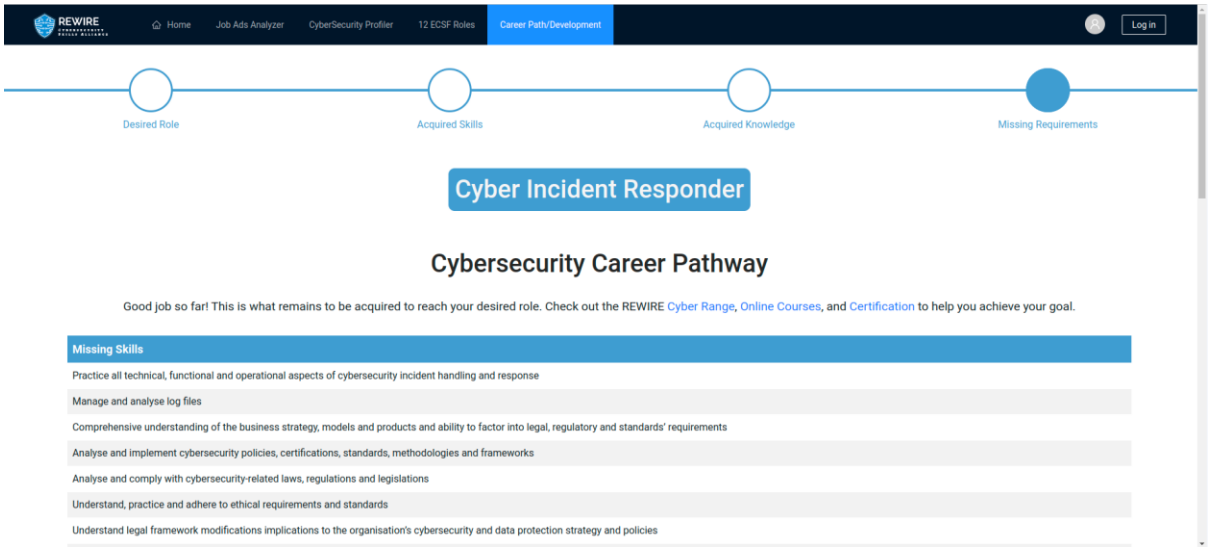

Figure 13 - Career Path/Development, Step 4 – Cybersecurity Career Pathway output, example of Cyber Incident Responder role

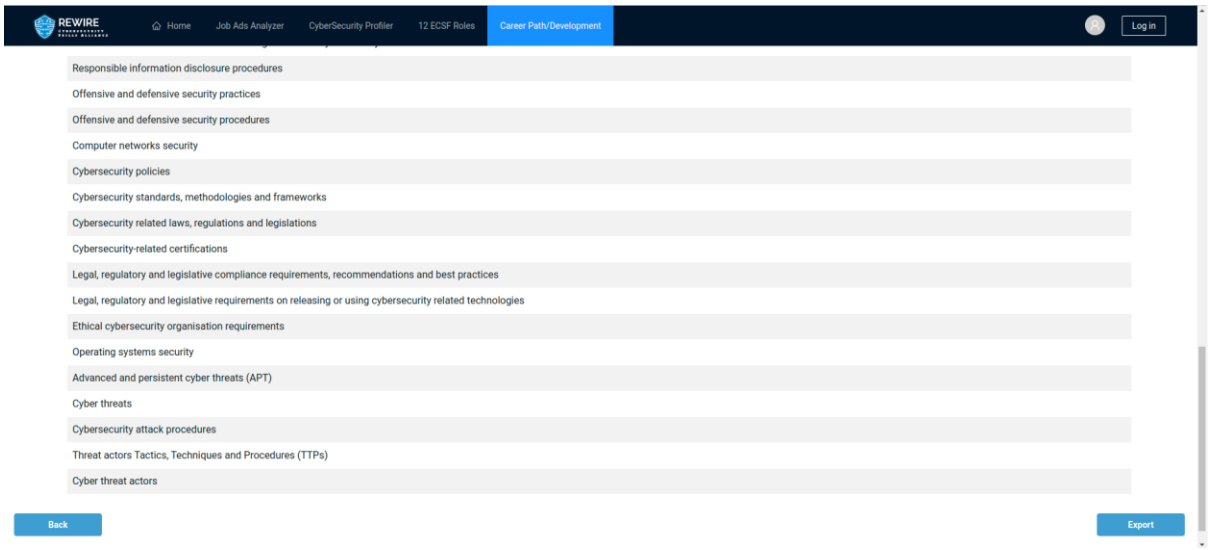

Figure 14 - Career Path/Development, Step 4 – Cybersecurity Career Pathway, export to pdf option

Cyber Incident Responder

Cybersecurity Career Pathway

Good job so far! This is what remains to be acquired to reach your desired role. Check out the REWIRE Cyber Range, Online Courses, and Certification to help you achieve your goal.

Missing Skills
Manage and analyse log files
Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements
Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks
Analyse and comply with cybersecurity-related laws, regulations and legislations
Work ethically and independently; not influenced and biased by internal or external actors
Work on operating systems, servers, clouds and relevant infrastructures
Missing Knowledge
Incident handling communication procedures
Offensive and defensive security practices
Cybersecurity policies
Cybersecurity-related certifications
Legal, regulatory and legislative compliance requirements, recommendations and best practices
Legal, regulatory and legislative requirements on releasing or using cybersecurity related technologies
Advanced and persistent cyber threats (APT)

Figure 15 - Career Path/Development, Step 4 – Cybersecurity Career Pathway, pdf document example of Cyber Incident Responder role

1.3. Access and documentation

The CyberABILITY platform is available in the main menu of the official REWIRE project website[6] or directly here[7].

Finally, the demonstration of the use of tools is available on the REWIRE project YouTube channel[8].

[6] https://rewireproject.eu
[7] https://rewireproject.eu/cyberability/
[8] https://www.youtube.com/channel/UC2-zInGvTsUOB5F5dM2lHtw