Adding European Cybersecurity Skills Framework into Curricula Designer

Jan Hajny
hajny@vut.cz
Brno University of Technology
Brno, Czech Republic

Marek Sikora
marek.sikora@vut.cz
Brno University of Technology
Brno, Czech Republic

Fabio Di Franco
fabio.difranco@enisa.europa.eu
ENISA
Athens, Greece

Athanasios Vasileios Grammatopoulos
avgrammatopoulos@ssl-unipi.gr
SSL, University of Piraeus
Piraeus, Greece

ABSTRACT

We present the updated version of the Curricula Designer, a tool that is devoted to helping study program administrators and education providers to create cybersecurity curricula that are modern and reflect the needs of the job market. Our main contribution is the inclusion of the European Cybersecurity Skills Framework (ECSF) developed by ENISA to the Curricula Designer. The ECSF makes it possible to directly link knowledge and skills with professional profiles, which in turn reflect actual work roles on the job market. By adding ECSF to the Curricula Designer, we get a simple yet powerful tool that helps to identify the right content of cybersecurity curricula using rigorous, deterministic methods, applicable at any higher education provider. At the time of the paper submission, the Curricula Designer is the first practical application that is based on ECSF. However, due to its focus on practicality, usability and simplicity, we expect ECSF to become the dominant framework for cybersecurity knowledge and skills identification in Europe.

CCS CONCEPTS

• **Social and professional topics** → **Computing education programs**; **Employment issues**; • **Applied computing** → **Education**; • **Software and its engineering** → Designing software.

KEYWORDS

education, training, tools, cybersecurity, frameworks, profiles, skills, knowledge

ACM Reference Format:
Jan Hajny, Marek Sikora, Fabio Di Franco, and Athanasios Vasileios Grammatopoulos. 2022. Adding European Cybersecurity Skills Framework into Curricula Designer. In *The 17th International Conference on Availability, Reliability and Security (ARES 2022), August 23–26, 2022, Vienna, Austria.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3538969.3543799

ARES 2022, August 23–26, 2022, Vienna, Austria

ACM ISBN 978-1-4503-9670-7/22/08…$15.00
https://doi.org/10.1145/3538969.3543799

1 INTRODUCTION

Rapid digitization affecting all domains brought cybersecurity into the attention of general public. Software and hardware solutions are not evaluated only according to their pure functionality but also with respect to requirements on cybersecurity. National and international legislation already contains cybersecurity-specific standards that need to be met by manufacturers, government, infrastructure operators and other relevant organizations. These requirements are often not only technical but concern also employees of companies. At least for larger organizations or organizations running critical infrastructures, dedicated staff responsible for cybersecurity is required. However, it is not only legal requirements that keeps the demand for cybersecurity professionals very high. The commercial sectors, in particular financial sector, advanced manufacturing and IT, realize that cyber attacks can pose very significant threats [5]. Both financial and reputation losses can be expected if cybersecurity is not adequately addressed.

The high demand for cybersecurity experts on the job market resulted in a strong push on education and training institutions. Not only universities, but also secondary education providers, try to answer this demand by opening new study programs on cybersecurity. Similar dynamic development can be seen in the area of professional training, where new courses and programs, often with some form of certification, arise. However, this very dynamic and often even precipitous development of new courses and programs brings also new problems. Cybersecurity is a very wide interdisciplinary area, which needs combination of expertise from different fields, including IT, law, social science, economy and more. No general rules or guides usually exist, so education providers are left alone with the freedom to design their programs without specific bounds. However, the lack of guidance and good practices often results in "novel" cybersecurity programs that are only modifications of existing study programs (usually on general computer science), as education providers try to save resources and use as much as possible of the existing staff and equipment. In this model, based on existing resources rather than on actual needs of the job market, it is very easy to provide education that is lacking important areas of knowledge, is incompatible with programs of other providers and not reflecting the requirements of employers. Furthermore, it is difficult to create focused programs and avoid shallow education.

In this paper, we present a practical tool that is aimed to help education providers to design novel cybersecurity study programs

in a structured and more deterministic way. We combine the web application called Curricula Designer [15] with the recent European Cybersecurity Skills Framework [7] and present a tool that is able to map the content of study programs with jobs that are available on the cybersecurity job market. In particular, our tool can be used to design new and analyse existing study programs with respect to requirements on knowledge and skills of particular job profiles defined in the European Cybersecurity Skills Framework. As this work is a continuation of previous activities based on the U.S.'s NIST NICE framework [12], the users of the application are free to choose the right framework for them, either the European or U.S. one.

The tool should give answers to curricula supervisors on questions such as "What jobs are relevant for our graduates?", "What courses are missing in our program?" or "What courses of other providers can be matched with our courses?". Therefore, we facilitate better focus of study programs, higher mobility of students and better connection between cybersecurity industry and education sectors.

1.1 Current State

Our tool is based on the requirements on cybersecurity experts defined in cybersecurity skills frameworks. Some of these frameworks already exist and can be considered proven by practice. The NIST National Initiative for Cybersecurity Education (NICE) framework is an example of such an existing framework. It has been already standardized as NIST Special Publication 800-181 Rev. 1 in 2020 [12] and contains definitions of Skills, Knowledge, Tasks, Competencies and Work Roles. In particular, the Reference Spreadsheet [11] is a helpful tool for the mapping between Work Roles and necessary KSA (Knowledge, Skills and Abilities). The actual version covers 48 Work Roles and hundreds of KSAs. While NIST NICE is currently one of the most advanced frameworks and is already used in the Curricula Designer, it does not reflect specifics that may be important for non-U.S. countries. For example, the European legal environment is not obviously captured by the NICE framework, although it may affect the way how education and training should be provided in Europe.

There are also other frameworks and lists of requirements on training and education. Besides others, we recall CyBOK [14], ACM Framework [3] and national certification programs such as NCSC Certification Program [10], SecNumedu [4] or Australian Guideline [13]. However, none of these frameworks and recommendations is universally accepted across the Europe as the governing guideline. This ambition has the European Cybersecurity Skills Framework (ECSF) which has been published by ENISA in mid 2022[1]. We describe this framework more in details in the Section 2.1.

There are only very few practical tools that help education providers to create and maintain their study programs. ENISA provides the Cybersecurity Higher Education Database (CyberHEAD) [6] which lists validated higher education programs in EU and EFTA countries. SPARTA project provides the Curricula Designer [15], which is the tool used also in this paper. The NICE Reference Spreadsheet can be used for building curricula, but it is still only a document, not an interactive application. CyberSeek [2] is an excellent interactive application focused on the identification of cybersecurity vacancies in U.S. and on creating career pathways.

1.2 Our Contribution

To our best knowledge, we present the first interactive tool for curricula design and analysis based on the European Cybersecurity Skills Framework. While the main purpose of the application is straightforward, i.e. to help education providers create new programs, the secondary goal is also to evaluate the fresh-new ECSF in its early stage and find ways for its improvements and further development.

2 EXISTING WORK

We base our result on two existing components, ie. the ECSF and the previous version of the Curricula Designer application. Their short description is provided in this section.

2.1 European Cybersecurity Skills Framework - ECSF

The European Cybersecurity Skills Framework has been defined by the Ad-Hoc Working group established in Nov 2020 [1]. The group includes experts from both private and public sector. The initial task for the group was to create a tool that would serve as a common European vocabulary in the cybersecurity context and help the employers, education providers and individuals to better understand cybersecurity roles, knowledge and skills. In mid 2022, the first draft of the ECSF was published [2].

The basic purpose of the ECSF is similar to other frameworks, i.e. to create links among the work roles/profiles and KSAs (knowledge, skills and abilities). However, besides reflecting European specifics, the ECSF approach is a bit different. The ECSF defines only 12 professional role profiles:

- Chief Information Security Officer (CISO),
- Cyber Threat Intelligence Specialist,
- Cybersecurity Educator,
- Cybersecurity Risk Manager,
- Cyber Incident Responder,
- Cybersecurity Architect,
- Cybersecurity Implementer,
- Digital Forensics Investigator,
- Cyber Legal, Policy & Compliance Officer,
- Cybersecurity Auditor,
- Cybersecurity Researcher,
- Penetration Tester.

For each profile, a set of characteristics is defined, including alternative titles, mission, deliverables and main tasks. Most importantly for our work, the set of expected skills and knowledge is defined. Unlike other frameworks, the ECSF is tied with the European e-Competence Framework (e-CF) [8] by assigning the e-Competencies to each profile, including the expected level. The profiles do not necessarily map to work roles directly, as these may be a combination of multiple profiles.

[1] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/ecsf-profiles-v-0-5-draft-release.pdf

[2] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/ecsf-profiles-v-0-5-draft-release.pdf

ECSF has been created using principles of simplicity, interoperability, neutrality and accessibility, market relevance and sustainability. It should be usable by variety of users, in particular by:

- Employers: to precisely define and advertise job offers, assess candidates, structure teams, develop strategies, ...
- Education and training providers: to create, update and evaluate study programs, provide career orientation, develop mobility programs, ...
- Employees: develop personal skills, select pathways, react to job advertisement, select training providers, ...
- Policy makers: understand the cybersecurity field, stimulate the job market, adequately regulate education/training providers, ...

In this work, we use the v0.5 Draft version of the ECSF, so it is expected that some definitions may change in future versions, in particular the specification of knowledge and skills.

2.2 Curricula Designer

The Curricula Designer is a web-based application developed and maintained by Brno University of Technology within the SPARTA project [15]. In its initial version, it was based on the NIST NICE framework that allows the mapping between NICE Work Roles and Competencies. As Competencies are not directly usable for tertiary education, SPARTA Topics were used as the intermediate step between Work Roles and Competencies. In particular, the usage of SPARTA Topics allows work with fundamental courses, such as mathematics or computer science, and uptake of upcoming topics, such as quantum technologies or blockchains, that may not yet been captured in NIST NICE.

However, the use of SPARTA Topics in the Curricula Designer has also its disadvantages, as the mapping between NIST Competencies and SPARTA Topics may be sometimes inaccurate or imprecise. Although BUT involved experts from different fields to create the mapping between the two sets of items and evaluated the results publicly, the indirect use of NIST's Competencies may bring imperfections in evaluations. Fixing these imperfections in evaluation is one of the main goals of this work, by the addition of the ECSF.

The basic functionality of the tool is straightforward and already described in paper [9]. The user may define its own cybersecurity courses, classify them accroding to SPARTA Topics (area 1 in Fig. 1) and compose the curriculum using the drag and drop method (area 2). After the curriculum is finished, the statistics may be analyzed on the right side of the application (area 3). Information about the credit structure, SPARTA Topics coverage, supported NICE Work Roles and provided Competencies is provided. In the original version, only statistical data based on NIST NICE framework were presented, see Fig. 2. The overall graphical user interface of the application is depicted in Fig. 1.

In this work, we use the existing functionality and add new features described in the next section.

3 UPDATING CURRICULA DESIGNER

The enhanced version of the Curricula Designer presented in this paper is one of the first applications based on the novel ECSF. We were not able to follow good practices from other implementations or use-cases and the approach taken in the previous NICE-based version could not be replicated as NICE has significant differences to ECSF (particularly, it defines work roles and competencies, groups knowledge, abilities and skills into larger sets, is already used in practice). Therefore, the first decision was regarding how the ECSF could be used to help mapping work roles into the content of courses that are taught at education providers and vice versa. The role of ECSF in this process is shown in Fig. 3.

The ECSF is in the core of the mapping, shown as the blue box in Fig. 3. It defines 12 professional profiles and for each of them, besides other items, it defines necessary knowledge and skills. We decided not to use other items, such as e-Competences from the e-CF (European Competence Framework) as they are not cybersecurity-specific and are usually hard to map to the content of university study programs. However, even these items can be added later if proven usable.

Having clearly mapped knowledge and skills to each profile, we need to connect the study courses to ECSF (marked green on left in Fig. 3). That can be done by mapping the content of courses directly to knowledge and skills defined in ECSF. This task must be done by the course/curricula administrators at education providers as they are responsible for the content of study courses and know the best what knowledge and skills are provided to students in their courses.

Finally, it is necessary to connect actual jobs to ECSF (marked yellow on right in Fig. 3). By the design of ECSF, each work role representing a vacancy on a job marked yellow may be defined by one or more ECSF profiles. Therefore, the task of mapping work roles (or job profiles, vacancies) is devoted to employers, who should be able to describe, what are the tasks, responsibilities and deliverables of employees they seek.

The scheme in Fig. 3 also shows an example of how education providers learn the content of courses necessary for particular work roles. The steps are:

(1) For a specific Work Role 1, education providers find the relevant Profiles (Profile 1 and Profile 12 in our example). This mapping, marked by brown arrows, should be specified by the job advertisers/employers.
(2) Education providers identify the necessary knowledge and skills for selected profiles. These requirements are defined by the ECSF, marked by blue arrows.
(3) Education providers design new or reuse existing courses (in our example courses 1, 2, 3, 4) that address the knowledge and skills identified in the step above. This mapping between courses and their content must be done by course administrators.
(4) Having all necessary courses (and all prerequisites for them, general non-cybersecurity courses, other courses for broadening the scope of students, etc.), the core of the curriculum is ready.

Using the approach above gives at least basic guarantee, that requirements for particular work roles are reflected in the curriculum.

Of course, the ECSF can be applied also in an exactly opposite way: first composing the curriculum from individual courses,

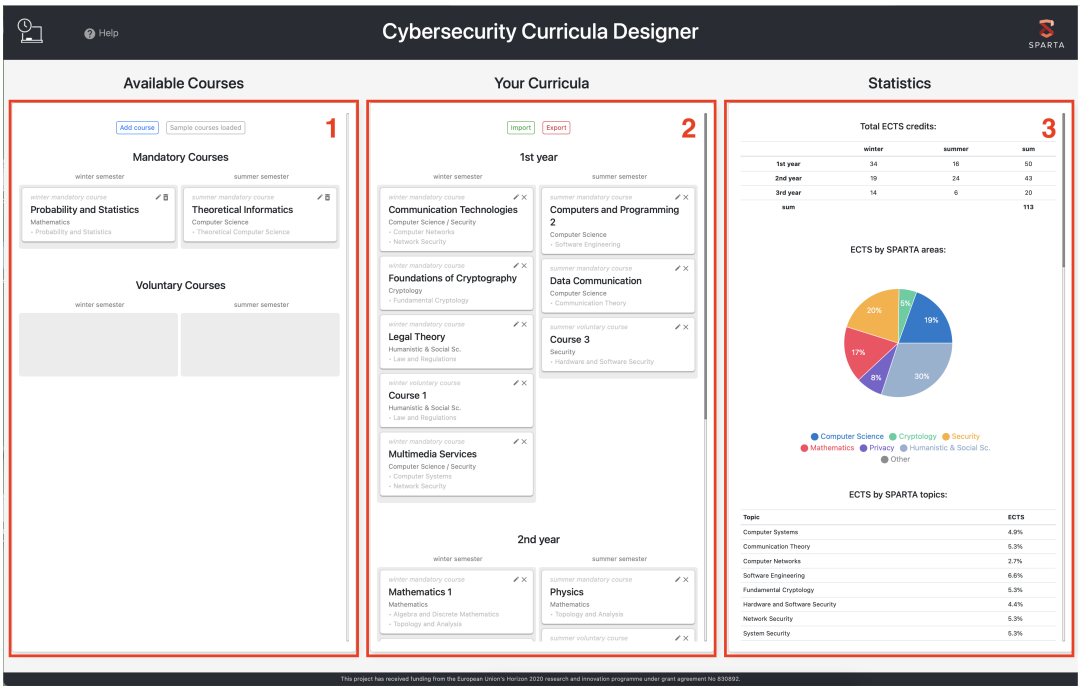

Figure 1: GUI of the Curricula Designer

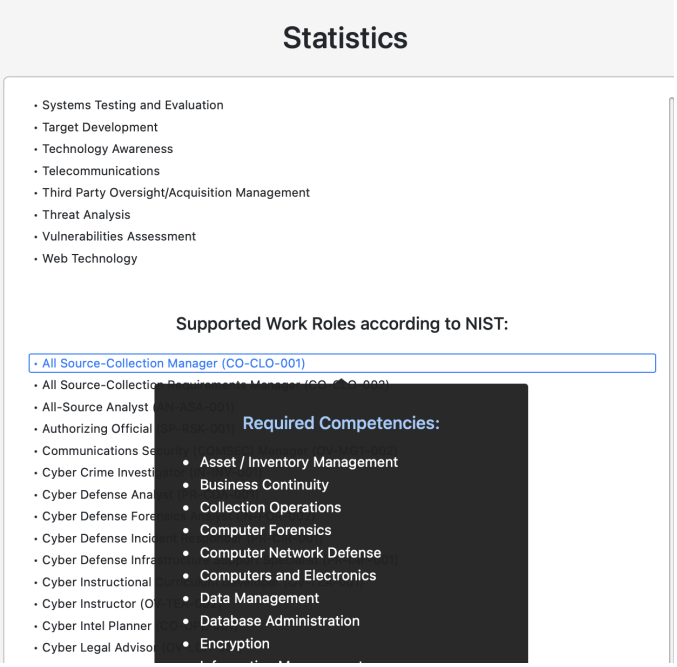

Figure 2: Statistical data based on NIST NICE.

analysing the knowledge and skills provided, using the ECSF to identify profiles and, finally, finding the work roles that are supported by the curriculum. In this way, we can analyze existing study

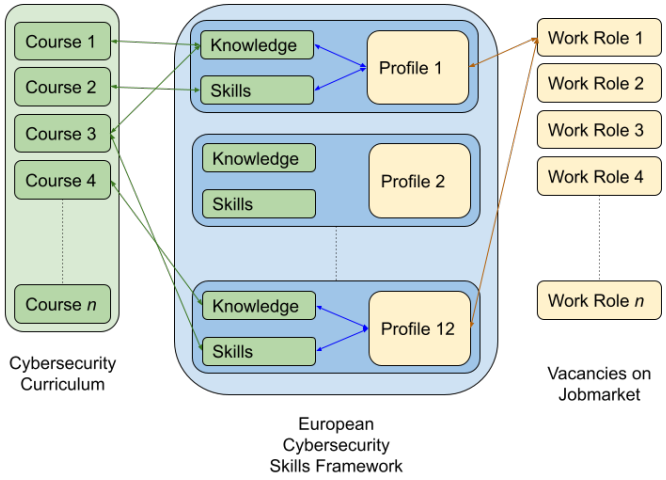

Figure 3: Usage of ECSF in Curricula Designer.

programs with respect to the needs of the job market and improve them by adding new courses with necessary knowledge and skills.

Compared to the use of NICE, the integration with ECSF was easier and more straightforward. We avoided using intermediary steps, such as SPARTA Topics and NICE Competencies, which are necessary in the NICE case. The direct mapping between course content and skills/knowledge defined in the ECSF lowers the probability of matching courses with wrong work roles. These mismatch can still happen due to potentially imprecise definition of course

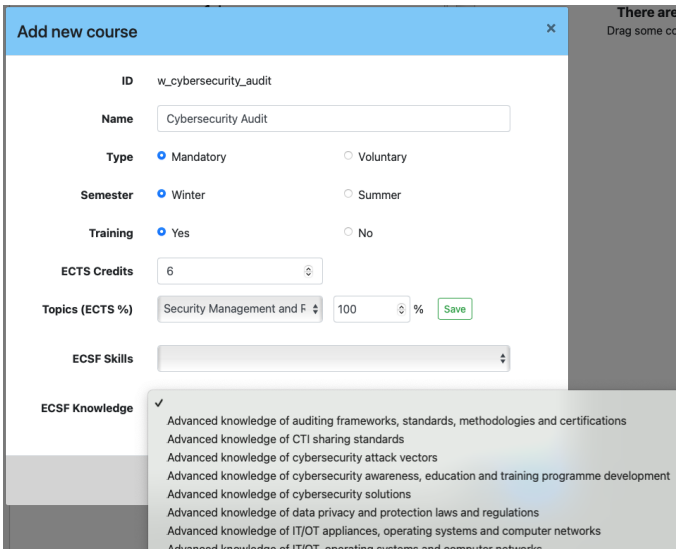

Figure 4: Add new course tab with ECSF Knowledge and Skill items.

content or skills/knowledge in ECSF but is less probable as the number of intermediate steps (thus mappings) is lower. The price for this more-precise mapping is higher generality of skills and knowledge defined in ECSF, compared to high detailness (and enormous number) of KSAs defined in NICE.

In addition to the design and analysis tasks, the enhanced Curricula Designer can be also used for finding course matches in mobility programs, such as Erasmus. Using the curricula designer and ECSF, it is easier to describe the course content using a standard language and allow students (and lecturers) to find a good match for their internships. The integration of Curricula Designer with other tools, such as ENISA's CYBERHEAD [6] or SPARTA Education Map [16] is of our future interest.

3.1 Implementation and User Interface

The updated Curricula Designer is based on the original web application developed in JavaScript language using the React framework, Syntactically Awesome Style Sheets Cascading Style Sheets (SASS CSS) preprocessor and Node Package Manager (NPM). More details on the original version, including the list of packages can be found here [9].

The updates are mainly in the Add new course section (available through Add course button in area 1 in Fig. 1) and the Statistics section (area 3 in Fig. 1).

In the course definition tab, we added two menus containing the knowledge and skills as defined in the ECSF. The course administrator can therefore select what skills and knowledge are taught to students in his courses. The GUI is depicted in Fig. 4.

Once all courses are defined in the left part of area 1 and composed into the curriculum in area 2, the Statistics are available in the area 3, see Fig. 5. Here, users can choose whether they want to use NIST NICE or ECSF. In case of ECSF, the list of ECSF Profiles that are supported by the defined curricula is presented. By moving the cursor over each profile, users can see the required knowledge and skills for each Profile. These skills and knowledge are present in the courses of the curriculum designed.

4 NEXT STEPS

We redesigned the Statistics section so that it is possible to use multiple cybersecurity skills frameworks for simultaneous analysis of the curriculum without the need to re-specify it. Currently, the statistical data that are relevant only to one of the framework are displayed in the respective tab. Therefore, it is possible to add more frameworks in the future. Should there be more frameworks in the future, they can be easily added to the application.

Currently, the application uses only knowledge and skills from ECSF, although more items are defined in the framework. We will consider updating the tool with additional items in the next versions.

We also plan to enhance the application to support not only university programs, but also professional training courses.

Finally, we seek for the integration of the Curricula Designer with other cybersecurity education applications, such as education maps or career pathway planners.

5 CONCLUSIONS

In this paper, we show the results of activities focused on the integration of the European Cybersecurity Skills Framework (ECSF) into the Curricula Designer web application. In the updated version of the tool, it is possible to design and/or analyze cybersecurity study programs with respect to the requirements of ECSF. As a result, the new cybersecurity study programs may better reflect the actual needs of the job market, be more modular and supportive for study internships. The will also allow easier update of existing study programs that need to reflect the current trends on the job markets. The tool is publicly available[3] for free.

ACKNOWLEDGMENTS

This paper is supported by European Union's Horizon 2020 research and innovation program (grant No 830892 "SPARTA"), the ERASMUS+ programme of the European Union (grant 621701-EPP-1-2020-1-LT-EPPKA2-SSA-B 'REWIRE') and by the Ministry of the Interior of the Czech Republic (grant VJ01030001).

REFERENCES

[1] 2020. Ad-Hoc Working Group on the European Cybersecurity Skills Framework. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls.
[2] 2022. CyberSeek. https://www.cyberseek.org.
[3] AIS SIGSEC & IFIP ACM, IEEE. 2017. Cybersecurity Curricular Guideline CSEC 2017. https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf.
[4] ANSSI. 2021. SecNumedu, labeling of higher education courses in cybersecurity. https://www.ssi.gouv.fr/en/cybersecurity-in-france/formations/secnumedu-labeling-of-higher-education-courses-in-cybersecurity/.
[5] ENISA. 2021. ENISA Threat Landscape 2020 - Phishing. https://www.enisa.europa.eu/publications/phishing.
[6] ENISA. 2022. CYBERHEAD - Cybersecurity Higher Education Database. https://www.enisa.europa.eu/topics/cybersecurity-education/education-map.
[7] ENISA. 2022. European Cybersecurity Skills Framework. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework.

[3] https://www.sparta.eu/curricula-designer/

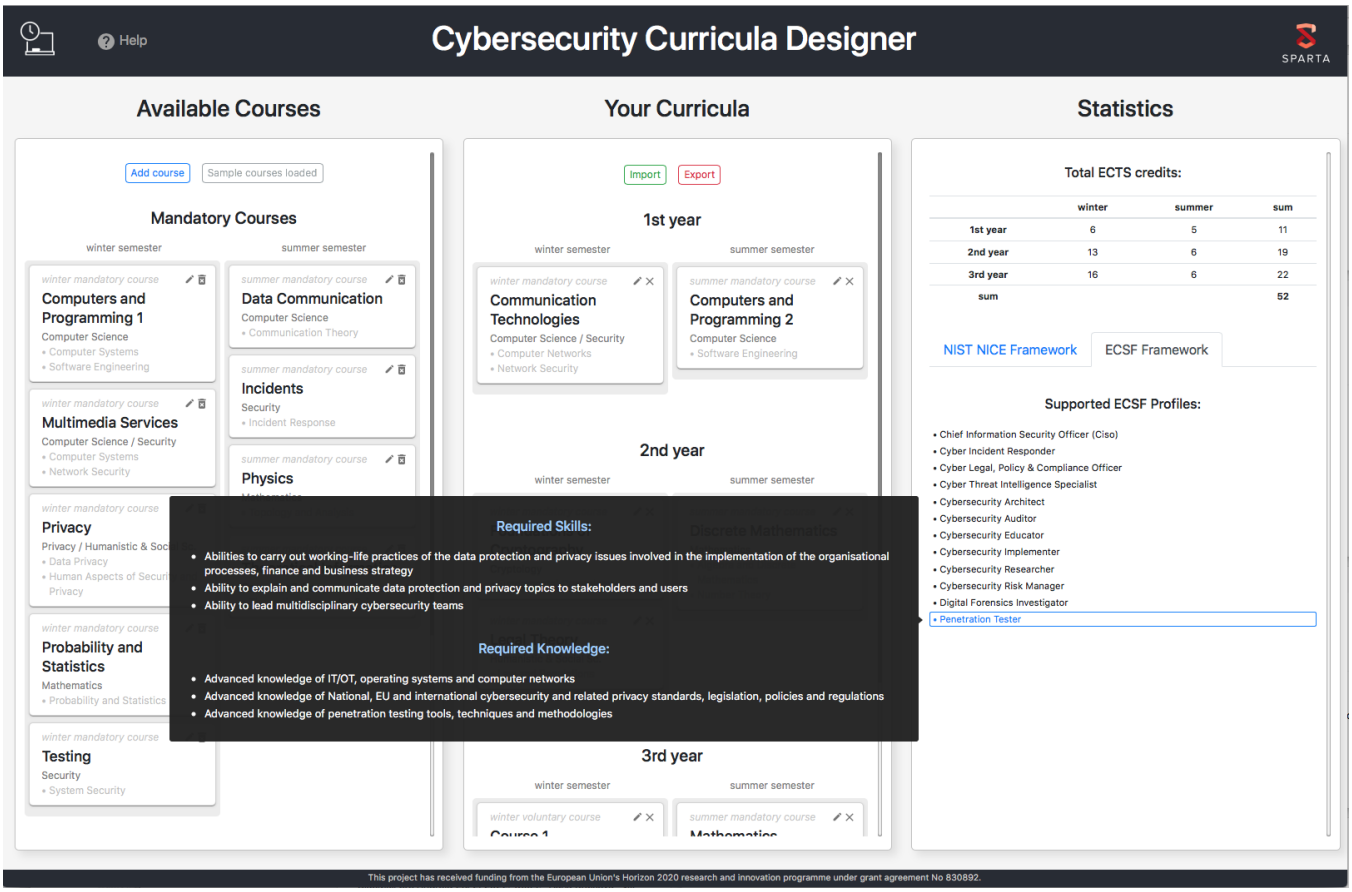

Figure 5: Lists of Knowledge and Skills for each ECSF Profile.

[8] CEN ICT Group. 2019. EN 16234-1 "e-Competence Framework (e-CF) standard. https://www.ecompetences.eu/get-the-e-cf/.
[9] Jan Hajny, Sara Ricci, Edmundas Piesarskas, and Marek Sikora. 2021. Cybersecurity Curricula Designer. In *The 16th International Conference on Availability, Reliability and Security* (Vienna, Austria) *(ARES 2021)*. Association for Computing Machinery, New York, NY, USA, Article 144, 7 pages. https://doi.org/10.1145/3465481.3469183
[10] NCSC. 2019. NCSC degree certification - Call for new applicants. https://www.ncsc.gov.uk/information/ncsc-degree-certification-call-new-applicants-0.
[11] NIST. 2020. NICE Framework Supplemental Material. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-supplemental-material.
[12] NIST. 2020. NIST Special Publication 800-181 Revision 1: Workforce Framework for Cybersecurity (NICE Framework). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.
[13] Australian Government Department of Education. 2017. Academic Centres of Cyber Security Excellence Program Guidelines. https://docs.education.gov.au/system/files/doc/other/accse_program_guidelines_february_2017_final.pdf.
[14] Awais Rashid, Howard Chivers, George Danezis, Emil Lupu Imperial, and Andrew Martin. 2019. The Cyber Security Body Of Knowledge. https://www.cybok.org/media/downloads/cybok_version_1.0.pdf.
[15] SPARTA. 2022. Cybersecurity Curricula Designer. https://www.sparta.eu/curricula-designer/.
[16] SPARTA. 2022. Cybersecurity Study Programs. https://www.sparta.eu/study-programs/.