SPARTA

European Cybersecurity Skills Framework

Training and education use case with SPARTA Curricula Designer

CONTACT

contact@sparta.eu

www.sparta.eu

This project has received funding from the European Union's Horizon 2020
research and innovation programme under grant agreement No 830892

Improving higher education using ECSF and SPARTA Curricula Designer...

Introduction

This use case provides recommendations on how ECSF can be used to shape education programmes that are linked with cybersecurity. As ECSF manifests the structure of high-level profiles from practitioners' point of view, including main tasks, relevant knowledge and skills, this can provide more focused approach for building specialized and comprehensive study programs, tailored to specific profiles, instead of covering cybersecurity in general.

Challenge

Education institutions compose their curricula considering the complete path – starting with the fundamental courses that are required for the student to learn as a basis for the next set of follow-on courses, which are often cybersecurity-specific. However, the selection of courses to be included in the cybersecurity curricula is up to the instituteion.

Each education institution has its own specific environment (determined by, e.g., infrastructure, equipment, expertise of teachers, composition of existing programs, etc.) and there is no universal way how the curriculum should be constructed.

Education providers differ in what concrete subdomain of cybersecurity they would like to focus on. Some providers are very technical, focusing on, e.g., computer science, some more social-oriented, focusing on legal and societal aspects. Therefore, the interoperability among the resulting study programs and a common language is currently a significant challenge.

Some academic programmes do not build skills and competencies that prepare students for specific work roles available on the job market. This poses a challenge for students which do not understand what are the occupational possibilities at the end of their studies.

Solution enabled by ECSF

The ECSF may contribute to the following activities that address challenges above:

- Evaluation: Description of profiles allows institutions to review their curricula in a structured and systematic manner, understanding the practitioners' point of view. This allows to understand for what profile institution is mainly targeting their graduates.

- Improvement: Can be done based on the evaluation exercise. This is especially important considering the set of knowledge / skills ascribed to specific profile.

- Focus: Education provided by universities may differ in the way they address core competencies. Some might be more focused on specific technological courses, some on law, others on forensics, etc. Having an ECSF to work with, they can map their core competencies onto various courses areas, important for defined profiles. This enables the institution to develop more effective targeted programs in house around the main competencies.

- Collaboration: ECSF gives the education providers the common language and vocabulary for describing their courses, creating joint programmes and allowing mobility of students.

While applying ECSF to cybersecurity education, the following approach is recommended:

- Courses in curricula can be classed as belonging to either Fundamental or Cyber Security categories. Fundamental courses are those that might not be directly linked to the ECSF, but which serve as a prerequisite for later studies. For example, Fundamental Cryptology is the prerequisite for Cryptanalysis or Advanced Cryptology; Number Theory is necessary for most intermediate and advanced computer related courses.

- Once the Fundamental courses are identified, the Cybersecurity courses can be proposed to address requirements of work roles the students are aiming to. Linking is achieved based on the content of individual courses, which can be linked to the profiles and finally to work roles. The concrete steps, as depicted in Fig. 1, are:

    a. 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.
    b. Education providers identify the necessary knowledge and skills for selected profiles. These requirements are defined by the ECSF, marked by blue arrows.
    c. 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.
    d. 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.

- Of course, the ECSF can be applied also in an exactly opposite way: first composing the curriculum from individual courses, analysing the knowledge and skills provided, using the ECSF to identify profiles and, finally, finding the work roles that are supported by the curriculum. This mapping reveals what exact knowledge and skills is already present in the curricula or, on the other side, what is missing and should be stressed or added to the courses. In this way, the ECSF helps to structure the curricula for a better fit with the expected profiles and job roles.

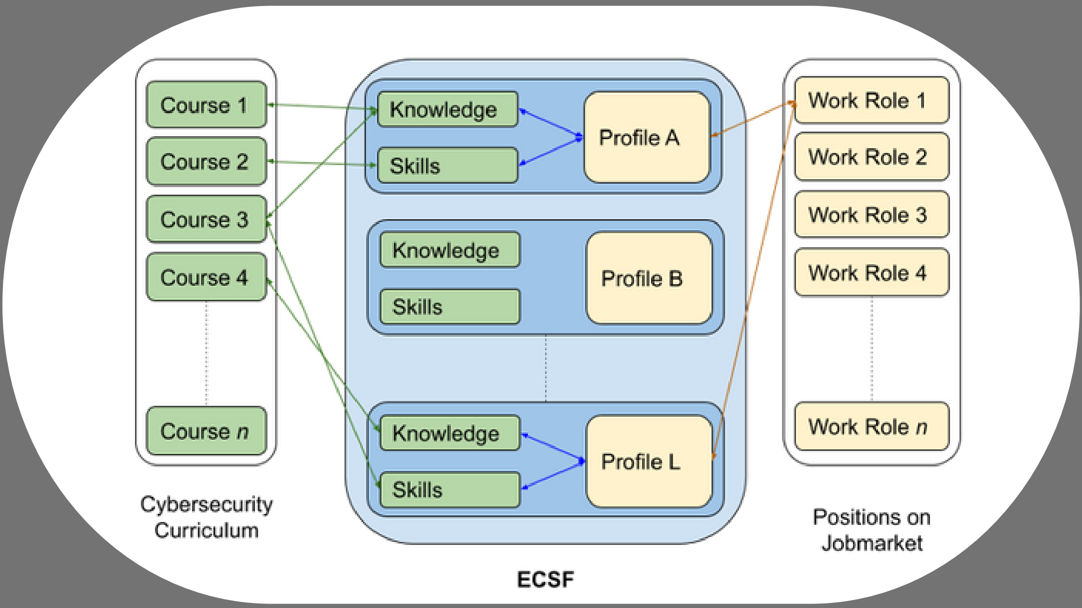
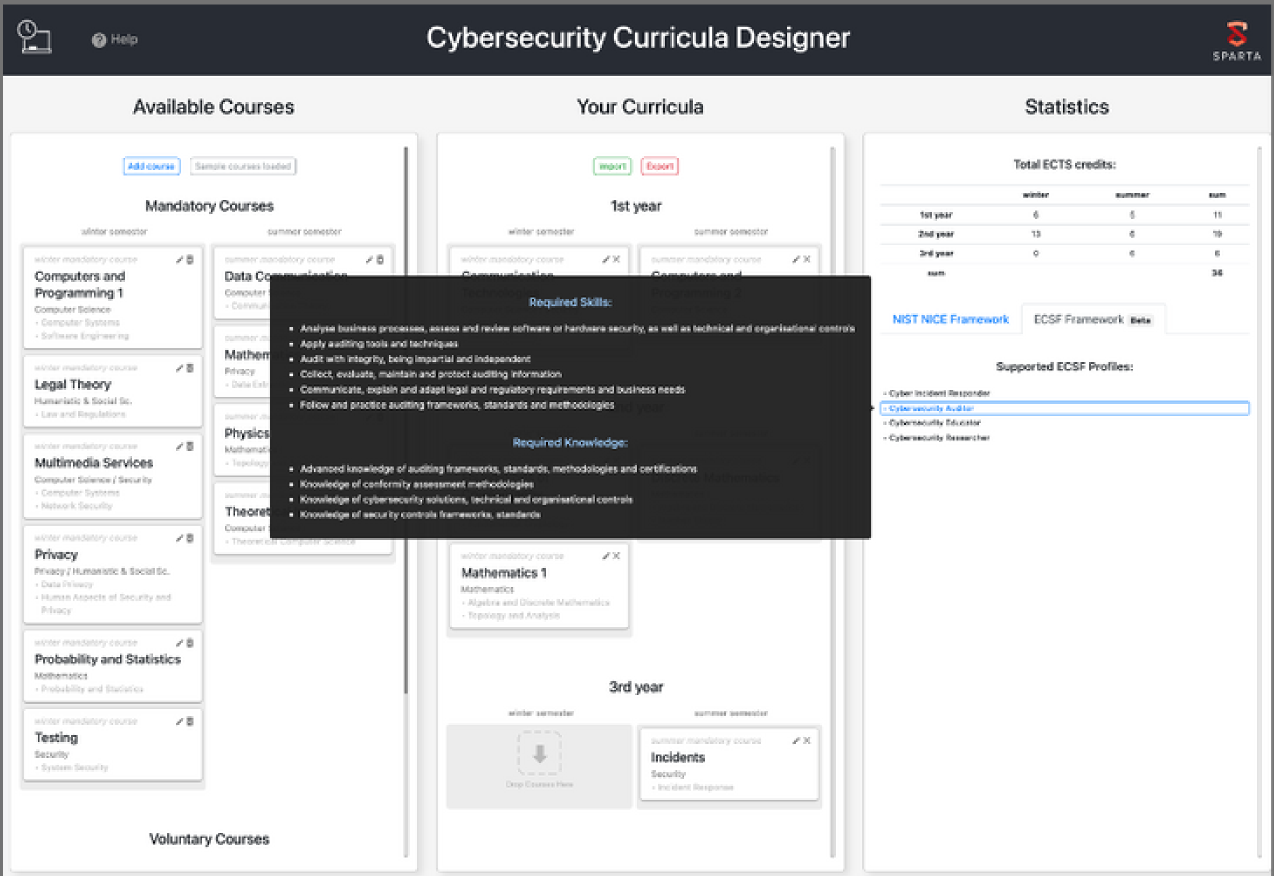


Fig. 1: Usage of European Cybersecurity Skills Framework by Education Providers

Result / added Value by SPARTA

SPARTA project used a cybersecurity skills framework to create a free tool called Cybersecurity Curricula Designer. It is a simple web application that helps education providers to create new study programs on cybersecurity and/or to analyze existing study programs according to their content and its reflection of cybersecurity jobs requirements.

The tool depicted in Fig. 2 allows study program administrators to compose their study program by dragging and dropping courses from the left section to the middle section. Courses, from which administrators develop the study programs, can be either pre-defined or custom. While composing the study program, the statistical data about its content is displayed in the right section. Besides other data, the information about what competencies and work roles are supported by the program are provided. By using the tool, it is easy to find out what content is missing in the study program and what specific work roles are best-suited for the graduates of the program. In this case, the cybersecurity skills framework is the core of the applications which allows linking the skills and knowledge with job roles.



Cybersecurity Curricula Designer

Available Courses

Mandatory Courses

winter semester

- winter mandatory course – Computers and Programming 1 – Computer Science – Computer Systems, Software Engineering
- winter mandatory course – Legal Theory – Humanistic & Social Sc. – Law and Regulations
- winter mandatory course – Multimedia Services – Computer Science / Security – Computer Systems, Network Security
- winter mandatory course – Privacy – Privacy / Humanistic & Social Sc. – Data Privacy, Human Aspects of Security and Privacy
- winter mandatory course – Probability and Statistics – Mathematics – Probability and Statistics
- winter mandatory course – Testing – Security – System Security

summer semester

- summer mandatory course – Data Communication
- summer mandatory course – Mathem…
- summer mandatory course – Physics
- summer mandatory course – Theoret… – Theoretical Computer Science

Voluntary Courses

Your Curricula

1st year

- winter mandatory course – Communication Technologies
- summer mandatory course – Computers and Programming 2
- winter mandatory course – Mathematics 1 – Mathematics – Algebra and Discrete Mathematics, Topology and Analysis

3rd year

- winter semester: Drop Courses Here
- summer mandatory course – Incidents – Security – Incident Response

Required Skills:

- Analyse business processes, assess and review software or hardware security, as well as technical and organisational controls
- Apply auditing tools and techniques
- Audit with integrity, being impartial and independent
- Collect, evaluate, maintain and protect auditing information
- Communicate, explain and adapt legal and regulatory requirements and business needs
- Follow and practice auditing frameworks, standards and methodologies

Required Knowledge:

- Advanced knowledge of auditing frameworks, standards, methodologies and certifications
- Knowledge of conformity assessment methodologies
- Knowledge of cybersecurity solutions, technical and organisational controls
- Knowledge of security controls frameworks, standards

Statistics

Total ECTS credits:

	winter	summer	sum
1st year	6	5	11
2nd year	13	6	19
3rd year	0	6	6
sum			36

NIST NICE Framework | ECSF Framework Beta

Supported ECSF Profiles:

- Cyber Incident Responder
- Cybersecurity Auditor
- Cybersecurity Educator
- Cybersecurity Researcher

Fig .2: SPARTA Curricula Designer

For further information see:

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

https://www.sparta.eu/curricula-designer/

HAJNÝ, J.; RICCI, S.; PIESARSKAS, E.; SIKORA, M. Cybersecurity Curricula Designer. In Proceedings of ARES 2021: The 16th International Conference on Availability, Reliability and Security. ACM, 2021. S. 1-7. ISBN: 978-1-4503-9051-4.

HAJNÝ, J.; RICCI, S.; PIESARSKAS, E.; LEVILLAIN, O.; GALLETTA, L.; DE NICOLA, R. Framework, Tools and Good Practices for Cybersecurity Curricula. IEEE Access, 2021, vol. 9, n. 1, pp. 94723-94747. ISSN: 2169-3536.