



Newsletter

January 2026

Federated Cybersecurity Lab

Federated Education is a paradigm for learning and collaboration. It envisions a decentralized network of educational institutions and learners working together to share resources, expertise, and best practices. The principles of federated education describe how one educational institution can share remote laboratories with other institutions. In this case, the education provider should ensure authentication, authorization, resource administration, etc. Learning management systems (e.g., Moodle) are designed to create, manage, deliver, and assess educational courses and learning and development programs. The courses are conducted online (or using blended learning approaches).

Developing a Federated Cybersecurity Lab based on the tools sandbox offers a few advantages and benefits. Intelligent technologies enable the creation of cybersecurity training material and simulations within the Federated Cybersecurity Lab. These simulations can be based on real-world cyber threats, attacks, and vulnerabilities. They also provide learners with hands-on experience identifying and mitigating security risks in a safe and controlled environment. Labs can facilitate experiential learning, allowing users to interact with cutting-edge security tools, technologies, and methods. Through practical exercises, labs, and scenarios, participants gain practical skills, problem-solving abilities, and critical thinking skills essential for effective cybersecurity practice.

Stakeholders and Their Goals

The Federated Security Lab involves two groups of stakeholders: learners and educators. Learners are the ones who will follow the CYBERCHALLENGE study program, take the courses, participate in the sandbox lab, and consider the CBL scenarios. The learners can be students (both undergraduate and graduate), post-graduate researchers and doctoral candidates, and non-formal learners from business and industry.

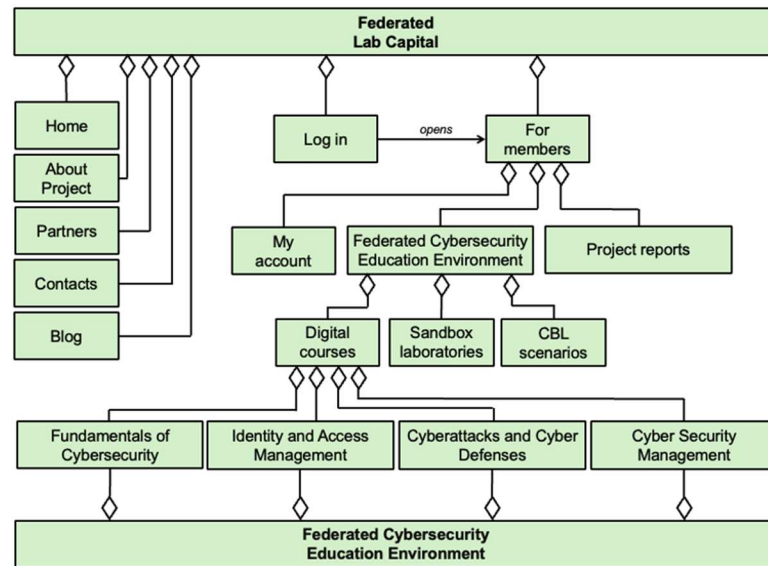
Perspective

Perspective of the Federated Lab Capital listed in Figure. The “Home” view presents the Federated Lab Capital landing page. The “About Project” view introduces the CYBERSECURITY project and its objectives, results, and targets. The “Partners” view describes the partners of the CYBERSECURITY project. The “Contacts” view introduces the coordinators and the key personnel contacts. The “Blog” view provides some means for communication.

To access the courses, the user (e.g., learner) needs to “Log In” to the Federated Lab Capital. She can choose two options: “Log in with Email” (if the capital administrator has created the account for her) or “Log in with Google” account. Once logged in to Federated Lab Capital, the user can access the “For members” view.



CYBERCHALLENGE - Challenges Solving in Cybersecurity Study Program No. 2024-1-LT01-KA220-HED-000252504



The “My account” view allows users to update their personal information and set and change their email address and password. The “Project reports” view displays the deliverables produced in the CYBERCHALLENGE project.

In the “Federated Cybersecurity Education Environment”, the user can choose among the digital courses, sandbox laboratories and CBL scenarios. This viewpoint leads to the course access, where the user can choose among “Fundamentals of Cybersecurity”, “Identity and Access Management”, “Cyberattacks and Cyber Defences” and “Cyber Security Management” courses. When accessing the courses, the user must follow the instructions (security, privacy restrictions, regulations and policies) specific to each referenced Federated cybersecurity education environment.

PROJECT COORDINATOR



PROJECT PARTNERS



<https://www.cyberchallenge-erasmus.eu/>

Kaunas University of Technology
Faculty of Informatics
Studentu str. 50, Kaunas, Lithuania