PROJECT COORDINATOR

kaunas university of technology

PROJECT PARTNERS

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

Funded by the European Union

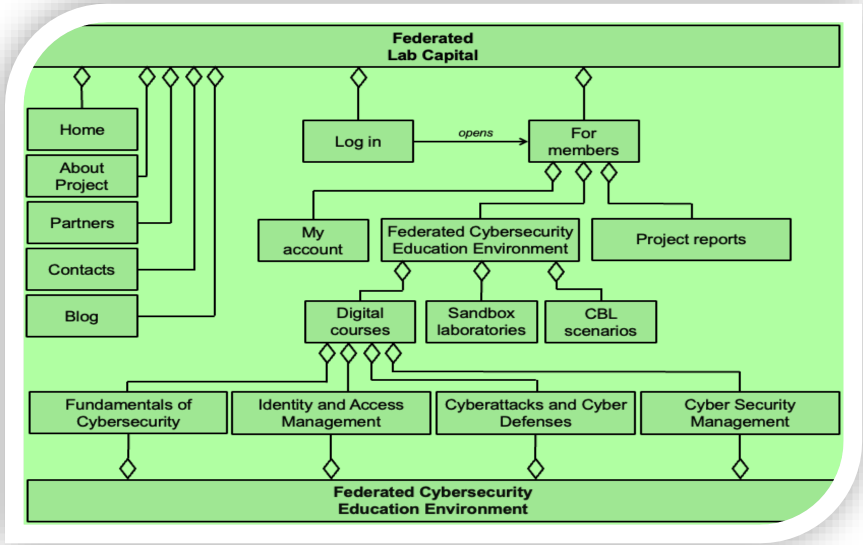
CYBERCHALLENGE Challenges Solving in Cybersecurity Study Program

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

Challenges Solving in Cybersecurity Study Program

CYBERCHALLENGE

***The aim of the project** is to increase the availability of digital content, technologies, and practices by developing a Cybersecurity curriculum based on the CBL methodology and Federated Cybersecurity lab based on tools sandbox.*


Federated Lab Capital
Home
About Project
Partners
Contacts
Blog
Log in
opens
For members
My account
Federated Cybersecurity Education Environment
Project reports
Digital courses
Sandbox laboratories
CBL scenarios
Fundamentals of Cybersecurity
Identity and Access Management
Cyberattacks and Cyber Defenses
Cyber Security Management
Federated Cybersecurity Education Environment

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

Project objectives

1. To increase the number of courses on Digital Cybersecurity curricular.

*2. To increase of using intelligence technologies in education by developing **Federated***

CYBERCHALLENGE

Challenges Solving in Cybersecurity Study Program

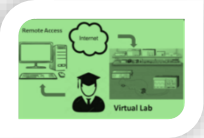
3. To increase learners' experience on CBL scenarios

Challenges for Cybersecurity study programme

With the increasing prevalence of cyber threats and the growing demand for cybersecurity professionals in institutions to accommodate a larger number of students and learners interested in pursuing cybersecurity education, by developing four distinct courses, educational institutions will cater to the diverse learning needs and interests of students and learners with different backgrounds, skill levels, and career aspirations in cybersecurity.

Federated Cyber Security Lab

Using intelligent technologies for the cybersecurity sector, particularly through the development of a Federated Cybersecurity Lab based on the tool sandbox, offers several significant advantages and benefits. Intelligent technologies enable the creation of realistic cybersecurity simulations within the Federated Cybersecurity Lab. These simulations in real-world cyber threats, attacks, and vulnerabilities, provide students and cybersecurity professionals with hands-on experience in identifying, analyzing, and mitigating cyber risks in a safe and controlled environment.



Challenge - based learning scenarios for studies in the lab and integration into study programme

By integrating CBL scenarios developed in collaboration with industry partners, students gain practical, real-world experience that prepares them for the demands of the workforce. CBL scenarios provide students with opportunities to develop critical thinking, problem-solving, and teamwork skills- qualities highly sought after by employers. Through hands-on experiences and collaboration with businesses, students will improve their experience on digital curricular settings and gain practical skills and knowledge that enhances their employability upon graduation.