Challenge-Based Learning in Cyber Security Education within a Federated Education Environment

Presenter - Algimantas Venčkauskas
Kauno technologijos universitetas

Partners
Tartu Ülikool · Universitatea Transilvania din Brașov · Universidade de Aveiro
ERASMUS+ Funded by the European Union.

Why Change Cybersecurity Education?

1

TRADITIONAL CYBERSECURITY LABS



- Follow predefined instructions
- Focus on tool usage
- Predictable outcomes
- Limited decision-making
- Instructor-centered approach

PROFESSIONAL CYBERSECURITY PRACTICE



- Ill-defined problems
- Multiple possible solutions
- Continuous investigation
- Critical decision-making
- Collaboration and reflection

KEY QUESTION: How can we bridge the gap between laboratory exercises and real-world cybersecurity practice?

CONSORTIUM

2

- KAUNAS UNIVERSITY OF TECHNOLOGY (Lithuania)
- UNIVERSITY OF TARTU (Estonia)
- UNIVERSITY OF AVEIRO (Portugal)
- TRANSLIVANIA UNIVERSITY OF BRAŞOV (Romania)

PROJECT OBJECTIVES

- Develop modern cybersecurity curricula
- Create Challenge-Based Learning scenarios scenarios
- Develop federated laboratories
- Support online and learning
- Strengthen international educational cooperation

CYBEREATURS

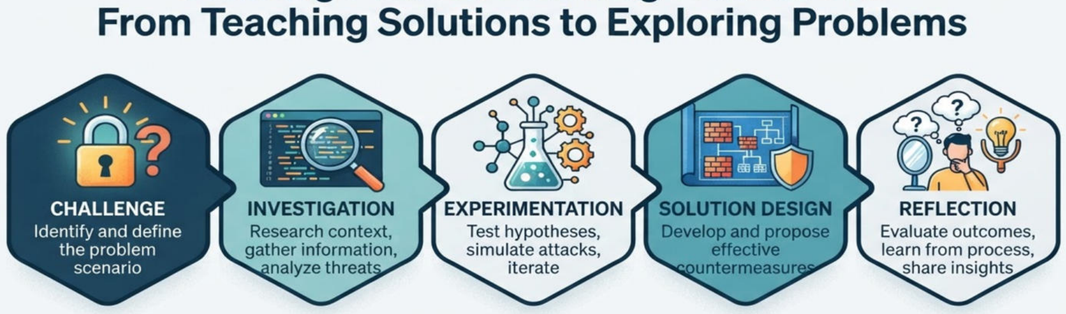
- Hybrid labls

THE CYBERCHALLENGE Project
ERASMUS+ Cooperation Project



Challenge-Based Learning Framework: From Teaching Solutions to Exploring Problems

3



Student Role:
- Active investigator
- Problem solver
- Decision maker

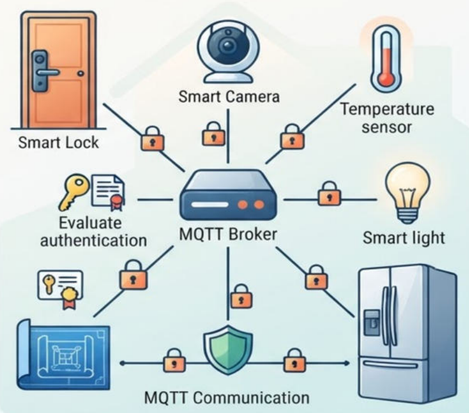
Teacher Role:
- Facilitator
- Mentor
- Learning designer

Example Cybersecurity Challenge IoT Security Challenge

4

Scenario
A smart home environment uses MQTT communication between IoT devices.

Student Tasks
- Identify security vulnerabilities
- Analyze attack surfaces
- Evaluate authentication mechanisms
- Implement secure communication
- Assess the impact of TLS protection
- Recommend a secure architecture





Learning Outcome
Students learn not only how to configure security but also why specific security decisions are necessary.

VIRTUAL LABORATORIES AS LEARNING ENABLERS

Why Virtual Laboratories?

5

Educational Benefits
- Safe experimentation
- Repeatable exercises
- Flexible access
- Remote participation
- Support for blended learning

Practical Applications
- Operating system security security
- Identity and access management
- Identioty and access management
- Cyberattacks and defenses
- IoT security laboratories
- Security management scenarios

Federated Learning Environment

Beyond a Single Institution

- Kauno technologijos universitetas
- Tartu Ülikool
- Universitatea Transilvania din Brașov
- Universidade de Aveiro

6

Federated Approach
Universities share:
- Learning resources
- Laboratory environments
- Educational expertise
- Challenge scenarios

Digital library
- Laboratory environments
- Educational expertise
- Varied security challenge

Benefits
- Resource optimization
- Wider variety of learning experiences
- Cross-institutional collaboration
- Increased educational sustainability

EDUCATIONAL RESOURCES DEVELOPED

Digital Cybersecurity Curriculum

7

FOUR COURSES (24 ECTS)
1. Fundamentals of Cybersecurity
2. Identity and Access Management
3. Cyberattacks and Cyber Defenses: Tools and Methods
4. Cyber Security Management

INTEGRATED COMPONENTS



Piloting

8

Participants



81
IT specialists and educators attended the pilot

Student Participation in Project Pilots

Study program courses	Federated CyberSecurity Lab	CBL (Challenge-Based Learning)
150 students	104 students	201 students

THREE COMPLEMENTARY DATA SOURCES FOR CBL PROJECT EVALUATION

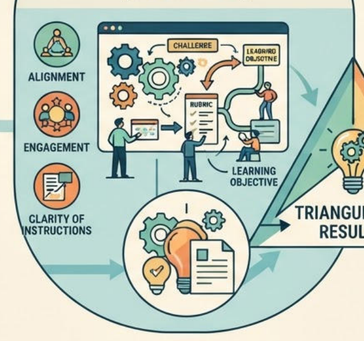
9

1. COURSE EVALUATION SURVEY (Moodle based)



Administered at semester end via Moodle. Focuses on students' overall evaluation of course structure and learning environment after CBL project.

2. CBL INTEGRATION EVALUATION SURVEY (Moodle based)



Administered at semester end via Moodle. Focuses specifically on design and implementation of the CBL project.

3. STANDARDIZED UNIVERSITY SATISFACTION SURVEY (institutional system)



Voluntary and anonymous questionnaire administered institutionally. Used for module quality assurance and improvement.

TRIANGULATED RESULTS

ASSESSING THE IMPACT OF CHALLENGE BASED LEARNING (CBL): A POSITIVE SHIFT

10

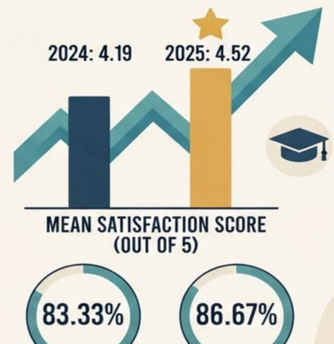
PERCEIVED ALIGNMENT & EDUCATIONAL VALUE



ENGAGEMENT & COGNITIVE IMPACT



OVERALL SATISFACTION CHANGE



PILOT EXPERIENCE AND EVALUATION: PRELIMINARY FINDINGS

11

PARTICIPANTS GENERALLY REPORTED POSITIVE PERCEPTIONS REGARDING:

Learning Materials
- Engaging Content
- Relevant Topics

Laboratory Environments
- Hands-on Labs
- Realistic Scenarios

Curriculum Integration
- Cohesive Structure
- Flow of Concepts

Practical Relevance
- Applicable Skills
- Industry Relevance

Variety of Learning Activities
- Interactive Exercises
- Diverse Formats

IMPORTANT NOTE
THE EVALUATION REPRESENTS FORMATIVE FEEDBACK OBTAINED DURING PILOT IMPLEMENTATION AND SHOULD NOT BE INTERPRETED AS CONCLUSIVE EVIDENCE OF LEARNING EFFECTIVENESS.

CYBERCHALLENGE

Challenges Solving in Cybersecurity Study Program

12

Find out more & apply
https://www.cyberchallenge-erasmus.eu/

Kaunas university of technology · Tartu Ülikool
Universitatea Transilvania din Brașov · Universidade de Aveiro

Poster created using MS Copilot, trybest.ai and canva.com