# Summary

CyberStart is a Nordic Baltic project aimed at addressing the underrepresentation of women in the cybersecurity workforce. Project participants will be offered training, mentorship, certification and career support to reskill and upskill in Cybersecurity. CyberStart seeks to enhance women's employability in a high-demand sector while contributing to regional cybersecurity resilience and gender equality.

# A New Beginning for Women in Cybersecurity

The goal of the CyberStart project is to reach unemployed or underemployed women and support them in gaining valuable skills for a career in cybersecurity. By motivating more women to join and complete the program, CyberStart aims to enhance their career prospects and strengthen their position in today's job market.

# Participants

The project aims to bring together at least 90 women - 60 from Latvia + Estonia and 30 from Finland.The project aims to train at least 100 women from Latvia, Estonia and Finland.

As the cybersecurity field is global in nature, a cross-country scale is necessary for the project to be fully successful. It not only encourages cooperation and connectivity, but also ensures that project participants are not limited to local job markets.

After completing the tailor-made online training program, participants will gain new, cyber-related qualifications and will be able to apply them in internships and entry job positions.

# Gains for women in tech

- **Increased employability**

The project will equip participants with skills and knowledge needed to continue their careers as freelancers, business owners, start-up founders in IT, particularly in the cybersecurity sector.

- **Decreased vulnerability in the IT sector**

Work in a digital economy evolves every day, placing at-risk groups that have limited access to education and reskilling. The project will remove this barrier for women, offering up-to-date and quality education.

- **Improved or developed cyberskills**

Participants will be provided with modules in network security, encryption, application security, risk and compliance, and other topics, ensuring a comprehensive understanding.

# Gains for society and the industry

- **Increased inclusivity and equality**

Currently, women are severely underrepresented in the field, but programs such as CyberStart help reach countries' and businesses' gender equality goals, as well as contribute to economic development in the region.

- **More available workforce**

In response to the military conflicts near the Baltic region and the increasing digitization of services, coupled with the rising opportunities for malicious attacks due to new technological trends, the demand for cybersecurity and IT specialists has surged in recent years. However, this demand has not been met with a corresponding increase in specialist availability. This project is designed to address and reduce this gap.

- **Investment in security and growth**

Quality cybersecurity education and training, as well as cross-border cooperation, are key to maintaining safety and preparing an effective response in case of risk. Increased participation in the ICT field will also stimulate economic growth.

# Timeline

| | |
|---|---|
| 1st registration phase | January 20 - February 20 |
| 2nd registration phase | February 20-23 |
| Program kick-off session | February 26 |
| Training program | March-May |

# Training program

After analyzing the EU Cybersecurity Strategy and National Cyber Security Centers' papers and reports and conducting interviews with 3 cybersecurity operational experts in the Baltic region in Phase 1, the retrieved insights will be used in developing a comprehensive **96-hour learning strategy involving 8 modules in Phase 3.**

1. **Intro to Cybersec & Digital Fundamentals**
   - Core concepts, roles, personal security, containers, VMs
2. **Network Security**
   - Concepts, devices, threats, IPS/IDS workshop
3. **Cryptography, Authentication & Identity and Access Management (IAM)**
   - Symmetric/asymmetric crypto, hashing, SSO, RBAC, authentication flows
4. **Application & Web Security**
   - OWASP Top 10, secure coding, API security, SSDLC, threat modeling
5. **Security Operations & Incident Response**
   - SOC workflows, SIEM, Level 1 SOC analyst skills
6. **Security Governance, Risk, Compliance & Privacy (GRC)**
   - Non-technical foundations, risk management, frameworks
7. **Attacker Mindset & Ethical Testing (Defender-focused)**
   - Fundamentals, OSINT, high-level offensive tactics
8. **Careers, Employability, Freelance Opportunities & Cybersecurity Entrepreneurship**
   - Process of building a cybersecurity business or product offering