wem cyber

WP2

CALL FOR SECONDMENT – 2026

Contact

coo.wemcyber@bilisimvadisi.com.tr

Funded by
the European Union

WP2

CALL FOR SECONDMENT - 2026

WEM Cyber
Widening Excellence and Mentoring In Cybersecurity

CALL: HORIZON-WIDERA-2024-TALENTS-03
TYPE OF ACTION: HORIZON-CSA
STARTING DATE: 1 JANUARY 2026
DURATION: 36 MONTHS
COORDINATOR: BILISIM VADISI TEKNOPARK YONETICI AS

DATE

May 2026 M5

WORK PACKAGE

WP2

TASK

Task 2.1

Funded by
the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Funded by
the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

WIDENING EXCELLENCE AND MENTORING IN CYBERSECURITY

WEM Cyber

Secondment 1

WEM Cyber (Widening Excellence and Mentoring in Cybersecurity) is a Horizon Europe funded project aiming to strengthen cybersecurity research capacity and increase women's participation in the sector across Europe. The project is coordinated by Bilişim Vadisi (Türkiye) and implemented by a consortium including Bogazici University (Türkiye), Vilnius Gediminas Technical University (Lithuania), University of Maribor (Slovenia), University of Pompeu Fabra (Spain), University of Toulouse (France), UBITECH (Greece), and Women4Cyber (Belgium). In addition, the project involves affiliated entities linked to Bilişim Vadisi, including Oninç- Cyberware (Türkiye), Cloudmetrik (Türkiye), Cyberwhiz (Türkiye), SphereTech (Türkiye), and SecroMix (Türkiye), which contribute technical expertise and support the implementation of project activities. Through structured academia–industry secondments, mentorship, and targeted training activities, WEM Cyber promotes cross-sector collaboration, supports the career development of women researchers and R&I personnel while contributes to strengthening Europe's cybersecurity ecosystem.

To clarify the organisation status within the project, please see the table below:

Organisation Type	Organisations
Academic Organisations: Academic Organisations can send eligible staff under the categories of Academic Staff / Researchers and Other R&I Staff. (They cannot send Non-academic Staff.)	• **University of Maribor** (Both Sending & Hosting) • **Bogazici University** (Both Sending & Hosting) • **Vilnius Gediminas Technical University** (Both Sending & Hosting) • **University of Toulouse** (Hosting Only) • **University of Pompeu Fabra** (Hosting Only)
Non-academic Organisations: Non-academic Organisations can send eligible staff only under the category of Non-academic Staff / Researchers. (They cannot send Academic Staff or Other R&I Staff.)	• **UBITECH** (Both Sending & Hosting) • **SecroMix** (Both Sending & Hosting) • **Cyberware** (Both Sending & Hosting) • **Cloudmetrik** (Both Sending & Hosting) • **SphereTech** (Sending Only) • **Cyberwhiz** (Sending Only)

Note: The call is **open to a closed group of organisations and their staff**, as defined in the project proposal. Therefore, only the organisations specifically identified in the proposal can act as sending or hosting partners under this call.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

CALL FOR SECONDMENT 1: 2026

ORGANISATION NAME	STAFF TYPE	POSITIONS	NUMBER OF SECONDEE
BOGAZICI UNIVERSITY	Non-Academic Staff (UBITECH, Cyberware, SphereTech, SecroMix, Cloudmetrik, CyberWhiz)	Cybersecurity Governance	4
UNIVERSITY OF MARIBOR	Non-Academic Staff (UBITECH, Cyberware, SphereTech, SecroMix, Cloudmetrik, CyberWhiz)	Human-Centred Cybersecurity and Privacy in Digital Platforms and Information Systems	1
		Cybersecurity and Privacy Risk Mitigation in Healthcare Data Breaches	1
	R&I Staff (BU and VT)	Cybersecurity Education, Training, and Skills Development for Human-Centred Security	1
UNIVERSITY OF POMPEU FABRA	Non-Academic Staff (UBITECH, Cyberware, SphereTech, SecroMix, Cloudmetrik, CyberWhiz)	Post-quantum cryptography; KEM combiners; PKI migration	1
	R&I Staff (BU, UM, and VT)	Post-quantum cryptography; PKI migration; PQ transition readiness	1
UNIVERSITY OF TOULOUSE	Non-Academic Staff (UBITECH, Cyberware, SphereTech, SecroMix, Cloudmetrik, CyberWhiz)	Social Engineering in the context of OSINT and AI	1
		Drones, Aerodynes and Geodata	1
VILNIUS GEDIMIAS TECHNICAL UNIVERSITY	Non-Academic Staff (UBITECH, Cyberware, SphereTech, SecroMix, Cloudmetrik, CyberWhiz)	Post-Quantum Cryptography and Quantum Key Distribution — Hybrid Architectures and Practical Migration	1 or 2
		Cyber Attack Detection — Methods, Gaps, and Practical Deployment	1 or 2
		Empirical Evaluation of EU AI Act Compliance in Cybersecurity AI Systems — Robustness, Fairness, Explainability, and Data Governance	1 or 2
		Cybersecurity of Dual-Use Unmanned Systems — UAV, UGV, and AUV Attack Surface Analysis and Defence	1 or 2
		Open — Proposed by the Secondee	1
	R&I Staff (BU, and UM)	AI-Augmented Digital Forensics and Incident Response	1 or 2
UBITECH	Academic Staff (BU, UM, and VT)	AI-driven Cybersecurity & Data Analytics Researcher	1

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

		Research & Innovation Associate	1
		Software & Systems Development Associate	1
ONINC ELEKTRONIK (CYBERWARE)	Academic Staff (BU, UM, and VT)	Automotive Cybersecurity for Software-Defined and Connected Vehicles	1
SPHERETECH	Academic Staff (BU, UM, and VT)	Product Owner	1

Important Note: This table was prepared based on pages 17–18 of the DoA. For final approval, please also check the DoA.

The call will include a total of **27 hosting opportunities**. Of these, **23 opportunities** will be opened for **Academic (5) / Non-Academic Researchers (18)**, while **4 opportunities** will be opened for **R&I Staff.** Researcher positions are structured as **academia–industry exchanges**. This means that industry partners can apply to researcher positions opened by academic organisations, while academic partners can apply to researcher positions opened by industry organisations. In this structure, the **researcher positions hosted by VT, BU, UM, UPF and UT** are open to eligible applicants from **industry partners, including UBITECH, Cyberware, SphereTech, SecroMix, Cloudmetrik and Cyberwhiz**. Similarly, the **researcher positions hosted by UBITECH, Cyberware and SphereTech** are open to eligible applicants from academic partners, **including BU, UM and VT**. R&I Staff positions are designed for **university staff** members who are defined as **R&I personnel**, such as administrative, managerial or technical staff supporting research and innovation activities. These staff members may apply to **R&I Staff positions** opened by **academic organisations**, in line with the eligible sending and hosting combinations defined in the table.

BOGAZICI UNIVERSITY

About Organisation:

Boğaziçi University, with roots dating back to 1863, is a leading public university in Istanbul, Türkiye, admitting highly selective and top-performing students nationwide. Its Management Information Systems Cybersecurity Center, established in 2016, serves as an interdisciplinary hub advancing digital security by integrating technical, managerial, and social science perspectives. The Center specializes in IT and cybersecurity governance, IT risk management, and information security and privacy management in emerging domains such as artificial intelligence and blockchain. Through international initiatives, including the EU-funded RECYPHER project, the Center contributes to research and innovation while bridging academia and industry through consultancy, applied research, and hands-on Cyber Camps.

Domains:

- Information Security Governance & Risk Management
- Security Policies, Standards & Compliance

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

- Asset Management & Data Classification
- Network Security & Architecture
- Incident Management & Response
- Business Continuity & Disaster Recovery
- AI & Emerging Technology Security

Location: *Türkiye*
Research Duration: *4 Months (Continuous)*

Researcher

Research Pathway: The secondment will take place in an interdisciplinary research environment focusing on cybersecurity from a business and governance perspective. The work will combine IT governance, risk management, and human factors to address current challenges in information security management.
Topic: C*ybersecurity Governance*
Research Objective: *The main objective is to analyse and develop approaches to improve cybersecurity governance and information security management by integrating business, technical, and human-centered perspectives.*
Number of Secondee: *4*
Candidate Profile: Candidates should have a background in cybersecurity, information systems, business administration, or related fields, with an interest in governance, risk management, and human factors in cybersecurity.
They are expected to have knowledge of information security governance, risk Technical Skills:

- Information Security Governance & Risk Management
- Security Policies, Standards & Compliance
- Network Security & Architecture
- GDPR Compliance & Data Protection Practices
- Incident Management & Response
- AI & Emerging Technology Security
- Business Continuity & Disaster Recovery
- Cybersecurity Ethics

Soft Skills:

- Problem-Solving & Critical Thinking
- Communication & Stakeholder Engagement
- Teamwork & Collaboration
- Ethical Judgement & Professional Responsibility
- Risk Communication & Security Awareness
- Time Management & Task Prioritisation
- Adaptability & Intercultural Communication

UNIVERSITY OF MARIBOR

About Organisation

University of Maribor

The University of Maribor is a leading research institution in Slovenia, recognized for its interdisciplinary expertise in cybersecurity, privacy, and information systems. Its research focuses on healthcare security, IoT and smart home environments, social networks, self-hosted software solutions, and human-centred cybersecurity, including security perception, privacy behaviour, and cybersecurity competences. The university also conducts research on cybersecurity education, skills development, privacy, trust, and security

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

perception in digital platforms. Through national and EU-funded projects, it contributes to applied cybersecurity research by developing security models and mitigation strategies for healthcare and IoT systems, while integrating technical, organizational, and behavioural perspectives.

Domains:

- Information Security Governance & Risk Management
- Security Policies, Standards & Compliance
- Cryptography & Data Protection
- Incident Management & Response
- AI & Emerging Technology Security
- Cybersecurity Ethics
- Privacy & Data Protection

Location: Slovenia

Research Duration: *No preferred secondment format (2+2 / 4 month continuous)*

Researcher 1

Research Pathway: Cybersecurity and privacy risks in digital platforms persist despite technical safeguards, largely due to human, organizational, and governance-related factors. Existing approaches insufficiently integrate user behaviour, security perception, privacy decision-making, and ethical considerations into security design.

Topic: *Human-Centred Cybersecurity and Privacy in Digital Platforms and Information Systems*

Research Objective: *To develop and validate user-cantered security and privacy models addressing trust, perception, and behaviour.*

Number of Secondee: 1

Candidate Profile: Background in cybersecurity or information systems; experience in privacy/data protection; knowledge of human-centred security and empirical research methods.

Technical Skills:

- Information Security Governance & Risk Management
- Security Policies, Standards & Compliance
- Privacy & Data Protection

Soft Skills:

- Problem-Solving & Critical Thinking
- Adaptability & Continuous Learning
- Intercultural Communication
- Presentation & Public Speaking Skills

Researcher 2

Research Pathway: Healthcare organizations increasingly face data breaches involving highly sensitive personal and medical data. Despite regulatory requirements and established security controls, breaches continue to occur due to a combination of technical vulnerabilities, inadequate governance, and human factors. Existing research often addresses technical defences in isolation, while insufficiently integrating organizational practices, risk management, and privacy protection into a holistic approach to breach prevention and mitigation.

Topic: Cybersecurity and Privacy Risk Mitigation in Healthcare Data Breaches

Research Objective: *To develop integrated frameworks for identifying, analysing, and mitigating healthcare data breach risks.*

Number of Secondee: 1

Candidate Profile: Background in cybersecurity or information systems; interest or experience in healthcare security, data protection, and regulatory compliance; knowledge of risk management and empirical research methods.

Technical Skills:

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

- Information Security Governance & Risk Management
- Security Policies, Standards & Compliance
- GDPR Compliance & Data Protection Practices
- Incident Management & Response

Soft Skills:

- Problem-Solving & Critical Thinking
- Adaptability & Continuous Learning
- Ethical Judgement & Professional Responsibility
- Intercultural Communication

R&I Staff 1

Research Pathway: Despite the growing importance of cybersecurity and privacy, significant gaps remain in user awareness, organisational training practices, and cybersecurity competences across sectors such as healthcare and digital platforms. Existing training initiatives are often fragmented, overly technical, or insufficiently tailored to diverse user groups, limiting their effectiveness in improving secure behaviour and decision-making. There is a need for structured, user-centred, and evidence-based training approaches that integrate behavioural insights, security awareness, and organisational needs.

The secondee will contribute to the design, development, and evaluation of cybersecurity education and training activities within the project, supporting the translation of research findings into accessible learning materials and capacity-building initiatives.

Topic: Cybersecurity Education, Training, and Skills Development for Human-Centred Security

Research Objective: To support the development and implementation of user-centred cybersecurity training frameworks and educational materials that enhance awareness, competences, and secure behaviour across different stakeholder groups.

Number of Secondees: 1

Candidate Profile: Candidates should have a background in education, social sciences, information systems, or a related field. Experience in training development, curriculum design, or capacity-building projects is desirable. Familiarity with cybersecurity or data protection topics from a non-technical perspective is an advantage. Candidates interested in translating research into practical learning and awareness solutions are encouraged to apply.

Technical Skills:

- Training & Curriculum Development
- Cybersecurity Awareness & Education Methods
- Knowledge Translation & Dissemination
- Data Protection & Ethical Awareness (basic understanding)
- Qualitative Evaluation & Impact Assessment

Soft Skills:

- Communication & Teaching Skills
- Creativity & Instructional Design Thinking
- Stakeholder Engagement & Facilitation
- Organisation & Project Coordination
- Critical Thinking & Problem-Solving
- Intercultural Communication

UNIVERSITY OF POMPEU FABRA
About Organisation

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

Pompeu Fabra University is a leading research university with strong expertise in advanced cryptography, cybersecurity, and privacy-preserving technologies. Its research activities focus on post-quantum cryptography, zero-knowledge proof systems, secure computation, blockchain technologies, and related cybersecurity applications. The university also contributes to cybersecurity training and inclusive STEM outreach, supporting the development of technical skills and broader participation in digital and security-related fields. Within the WEM Cyber context, Pompeu Fabra University brings high-level research capacity in cryptographic methods and privacy-enhancing technologies, offering secondees the opportunity to engage with cutting-edge research topics and contribute to innovation in secure and trustworthy digital systems.

Domains:

- Access Control & Identity Management
- Cryptography & Data Protection
- AI & Emerging Technology Security
- Privacy & Data Protection

Location: Spain

Research Duration: *No preferred secondment format (2+2 / 4 month continuous)*

Research 1

Research Pathway: Migrating public-key infrastructure from classical to quantum-resistant schemes requires hybrid constructions that remain secure even if one component is broken. The secondee will work on the design and evaluation of KEM combiners for hybrid PQ-classical deployments.

Topic: *Post-quantum cryptography; KEM combiners; PKI migration*

Research Objective: *To design and evaluate KEM combiners for secure hybrid post-quantum deployments.*

Number of Secondee: 1

Candidate Profile: Master's degree or equivalent experience in computer science, mathematics, or telecommunications; background in cryptography or information security; familiarity with PQC (e.g., lattice-based schemes) and programming skills in C/C++ or Rust.

Technical Skills:

- Security Policies, Standards & Compliance
- Cryptography & Data Protection
- Research Methodology & Academic Writing
- Privacy & Data Protection

Soft Skills:

- Problem-Solving & Critical Thinking
- Adaptability & Continuous Learning
- Intercultural Communication
- Presentation & Public Speaking Skills

R& I Staff 1

Research Pathway: Organisations across Europe will need to migrate their cryptographic infrastructure to quantum-resistant standards in the coming years, but there is a significant skills gap in understanding PQ schemes and their practical deployment. The secondee will gain hands-on experience with post-quantum cryptographic tools and migration strategies, contributing to the development of training materials and best-practice guides for enterprise PQ transition.

Topic: Post-quantum cryptography; PKI migration; PQ transition readiness

Research Objective: *To support the development of practical tools, guidelines, and training materials for enterprise-level PQ migration.*

Number of Secondee: 1

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

Candidate Profile: Bachelor's or master's degree in computer science, mathematics, telecommunications, or cybersecurity; basic knowledge of public-key cryptography; willingness to learn PQ schemes; programming skills (Python, C, or Rust); interest in policy and compliance frameworks.
Technical Skills:

- Security Policies, Standards & Compliance
- Cryptography & Data Protection
- Grant Writing & Proposal Development
- Project Management & Reporting (EU Projects)

Soft Skills:

- Communication & Stakeholder Engagement
- Adaptability & Continuous Learning
- Risk Communication & Security Awareness

UNIVERSITY OF TOULOUSE

About Organisation

Université de Toulouse, through the Institut de Recherche en Informatique de Toulouse, is one of France's major research actors in computer science and digital technologies. Established in 1990, IRIT is a Joint Research Unit of CNRS and Université de Toulouse, bringing together around 600 members and 100 external collaborators. The institute conducts research across data and computational sciences, with strategic application areas including artificial intelligence, cybersecurity, big data, smart cities, health, aerospace, and transportation. Within WEM Cyber, Université de Toulouse contributes strong expertise in data science, AI, privacy, personal data protection, IoT security, digital forensics, and cybersecurity, supported by extensive experience in European and international research projects.

Domains:

- Information Security Governance & Risk Management
- Security Policies, Standards & Compliance
- AI & Emerging Technology Security
- Cybersecurity Ethics
- Privacy & Data Protection
- privacy - social engineering

Location: France
Research Duration: *2 + 2 Months (Split Arrangement)*

Researcher 1
Research Pathway: OSINT – AI – Cybersecurity
Topic: Social Engineering in the context of OSINT and AI
Research Objective: To analyse social engineering risks in the context of OSINT and AI, focusing on the role of publicly available data, privacy and data protection challenges, cybersecurity ethics, and adversarial learning, and to contribute to research activities and a joint publication.
Number of Secondee: 1
Candidate Profile: The candidate should have a research background or strong interest in cybersecurity, AI, OSINT, privacy, data protection, and social engineering. The secondee is expected to contribute to research activities, data management, and the preparation of a joint publication formalising the collaboration.
Technical Skills:

- Data Management & FAIR Data Principles

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

- GDPR Compliance & Data Protection Practices
- Project Management & Reporting (EU Projects)
- Cybersecurity Ethics
- Privacy & Data Protection
- social engineering - adversarial learning

Soft Skills:

- Problem-Solving & Critical Thinking
- Creativity, Innovation & Vision
- Presentation & Public Speaking Skills

Researcher 2

Research Pathway: Drones, Aerodynes and Geodata

Topic: Security of embedded systems in drone and geodata-related applications

Research Objective: To analyse and address embedded systems security challenges in drone and geodata-related applications, including secure data collection, processing, modelling, and transmission, and to contribute to the development of a practical use case, prototype and/or joint publication.

Number of Secondee: 1

Candidate Profile: The candidate should have a research background or strong interest in embedded systems security, geodata, drone-related technologies, data modelling, privacy and data protection. The secondee is expected to contribute to the development of a complete use case, support the data modelling pipeline, and, where relevant, contribute to a prototype and/or joint publication.

Technical Skills:

- Data Management & FAIR Data Principles
- GDPR Compliance & Data Protection Practices
- Privacy & Data Protection
- Cybersecurity Ethics

Soft Skills:

- Analytical thinking
- Problem-solving skills
- Interdisciplinary collaboration
- Communication skills
- Research-oriented mindset
- Ability to work independently and contribute to joint research outputs

R&I Staff 1

Research Pathway:

Topic:

Research Objective:

Number of Secondees:

Candidate Profile:

Technical Skills:

- -

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

Soft Skills:

- -

VILNIUS GEDIMIAS TECHNICAL UNIVERSITY

About Organisation

Vilnius Gediminas Technical University is Lithuania's leading technical university and one of the country's largest research institutions, with strong expertise in engineering, informatics, electronics, cybersecurity, and emerging technologies. The university hosts the DIGI-DEFENSE Digital Defence Competency Centre, an applied R&D hub connecting academia, government, and industry in cybersecurity and defence technologies. Its research strengths include AI-driven threat detection, adversarial machine learning, federated learning, digital forensics, cyber incident investigation, zero-trust architecture, cyber threat intelligence, and the cybersecurity of cyber-physical systems. Vilnius Tech also provides advanced research infrastructure, including AI computing resources, edge AI laboratories, quantum key distribution equipment, digital forensics facilities, and cyber range environments for practical training and experimentation.

Domains:

- AI & Emerging Technology Security
- Cryptography & Data Protection (incl. Post-Quantum Cryptography and QKD)
- Incident Management & Response
- Digital Forensics & Cybercrime Investigation
- Network Security & Architecture
- OT/IoT Security & Zero Trust Architecture
- Security of Embedded & Electronic Systems
- Dual-Use Technology Security (Unmanned Systems)
- Privacy & Data Protection
- Cybersecurity Education & Skills Development

Location: Lithuania

Research Duration: No preferred secondment format (2+2 / 4 month continuous)

Researcher 1

Research Pathway: The transition toward quantum computing poses an existential threat to current public-key cryptographic infrastructure. Harvest-now-decrypt-later attacks — where adversaries collect encrypted data today to decrypt it once quantum computers mature — are already an operational concern for governments and critical infrastructure operators. Simultaneously, the deployment of Quantum Key Distribution (QKD) as a physically secure key exchange mechanism is transitioning from theory to practice, yet significant challenges remain in hybrid PQC–QKD architectures, integration with classical network stacks, and real-world performance characterisation.

Vilnius Tech is actively building QKD research capacity through its Alice & Bob device set and PQC-focused research team. The secondee will work alongside cryptography and security researchers at DIGI-DEFENSE to investigate practical aspects of post-quantum migration and quantum-secure communications, with access to both theoretical frameworks and hands-on hardware experimentation.

Topic: Post-Quantum Cryptography and Quantum Key Distribution — Hybrid Architectures and Practical Migration

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

Research Objective: To investigate and prototype hybrid PQC–QKD security architectures applicable to real-world communications infrastructure, with a focus on performance characterisation, integration challenges, and transition readiness assessment for organisations migrating away from classical cryptographic schemes.
Number of Secondee: 1-2
Candidate Profile: Candidates should have a background in computer science, mathematics, telecommunications, or information security, with interest or foundational knowledge in cryptography or quantum technologies. Familiarity with PQC schemes (lattice-based, code-based, etc.), programming in Python, C, or Rust, and interest in both theoretical and practical/experimental research is advantageous. Prior knowledge of QKD is beneficial but not required — the secondee will be embedded in an active learning environment with hardware access.
Technical Skills:

- Cryptography & Data Protection
- Security Policies, Standards & Compliance
- Network Security & Architecture
- Research Methodology & Academic Writing
- Privacy & Data Protection

Soft Skills:

- Problem-Solving & Critical Thinking
- Adaptability & Continuous Learning
- Creativity, Innovation & Vision
- Intercultural Communication
- Presentation & Public Speaking Skills

Researcher 2
Research Pathway: Cyberattacks are growing in both volume and sophistication — ransomware, supply chain compromises, advanced persistent threats, and AI-generated phishing campaigns are now routine rather than exceptional. Yet many organisations, particularly in public administration, healthcare, and critical infrastructure, still rely on signature-based or rule-based detection systems that struggle against novel and zero-day attacks. There is a pressing need for research that bridges the gap between state-of-the-art academic detection approaches — anomaly detection, behavioural analysis, graph-based network modelling, deception technologies — and practical deployment realities.
At Vilnius Tech's DIGI-DEFENSE Centre, the secondee will work within an active threat detection research environment, with access to real-world incident data, the AI hardware for model training, the Cyber Range for controlled attack simulation, and an experienced team whose members combine academic research with hands-on professional incident response backgrounds. The research environment is deliberately kept broad and adaptive — detection problems are explored across network traffic, endpoint behaviour, log analysis, and identity anomalies, allowing the secondee to contribute meaningfully regardless of their specific prior specialisation within cybersecurity.

Topic: Cyber Attack Detection — Methods, Gaps, and Practical Deployment
Research Objective: To survey, implement, and evaluate attack detection approaches relevant to the current threat landscape, identifying gaps between academic state-of-the-art and operational deployment, and contributing to at least one novel or improved detection mechanism validated against realistic attack scenarios in the Cyber Range environment.
Number of Secondee: 1-2
Candidate Profile: Candidates should have a background in cybersecurity, computer science, or information systems, with a genuine interest in how attacks work and how they are detected. Prior experience in any of the following is welcome but none is strictly required: network security, endpoint security, SIEM/SOC environments, penetration testing, CTF participation, or security research. Intellectual curiosity and motivation to engage with both technical and operational dimensions of detection are valued above any single specific skill.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

Technical Skills:

- Network Security & Architecture
- Incident Management & Response
- AI & Emerging Technology Security
- Security Policies, Standards & Compliance
- Research Methodology & Academic Writing

Soft Skills:

- Problem-Solving & Critical Thinking
- Adaptability & Continuous Learning
- Ethical Judgement & Professional Responsibility
- Intercultural Communication
- Presentation & Public Speaking Skills

Researcher 3

Research Pathway:

The EU AI Act — the world's first comprehensive binding regulation on artificial intelligence — entered into force in August 2024 and is now rolling out obligations across risk categories on a staggered timeline running through 2027. For organisations developing or deploying AI systems in security-relevant contexts — intrusion detection, fraud prevention, access control, biometric authentication, critical infrastructure monitoring — understanding precisely what the Act requires, when, and how those requirements translate into concrete technical and organisational measures is neither straightforward nor settled.

The intersection of AI security and AI regulation is a genuinely open research space. The Act introduces concepts like conformity assessment, technical documentation, human oversight requirements, and prohibited AI practices, but practical guidance on how these map onto real cybersecurity AI deployments remains scarce. Vilnius Tech has active AI-driven security systems in research and early deployment — including behavioural authentication, threat detection models, and federated learning approaches — that provide concrete objects of study for regulatory mapping. The secondee will contribute to building a structured understanding of the Act's obligations as they apply to security AI, identifying compliance gaps, and proposing implementation roadmaps — work that is directly useful to both the university's own R&D and to partner organisations navigating the regulatory transition.

First, robustness and reliability testing: the Act requires high-risk AI systems to be robust against errors, faults, and adversarial manipulation. The secondee will design and execute adversarial attack experiments — including white-box and black-box attacks (FGSM, PGD, Carlini-Wagner, model inversion) — against cybersecurity AI models to empirically characterise their robustness envelope and identify failure modes that would constitute Act-relevant technical deficiencies.

Second, fairness and accuracy-across-subgroups analysis: the Act mandates that high-risk AI systems maintain appropriate accuracy across different groups and operating conditions. In cybersecurity contexts this translates to questions such as: does a network intrusion detection model perform equally well across different network topologies, traffic profiles, or user behavioural patterns? Does a behavioural authentication system exhibit systematic bias against certain input distributions? The secondee will develop experimental protocols for subgroup performance analysis tailored to security AI deployment contexts, where protected attributes are not demographic but operational.

Third, explainability and human oversight evaluation: the Act requires that high-risk AI systems enable meaningful human oversight of their outputs. The secondee will experimentally compare explainability methods (SHAP, LIME, attention-based attribution, counterfactual explanations) applied to cybersecurity AI models, evaluating not just technical fidelity of explanations but their practical utility for a security analyst making an override decision — a question that requires user-centred experimental design alongside the ML experimentation.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

Fourth, data governance and training set documentation: the Act imposes requirements on training data quality, representativeness, and known limitations. The secondee will contribute to developing empirical data characterisation protocols — dataset shift detection, coverage analysis, label noise estimation — applicable to the threat datasets used in DIGI-DEFENSE research, producing reusable documentation artefacts that themselves constitute a research contribution.
The outputs of this research will be both scientific (experimental results, proposed evaluation frameworks, methodology papers) and practical (a structured compliance gap assessment and implementation roadmap applicable to real cybersecurity AI deployments).

Topic: Empirical Evaluation of EU AI Act Compliance in Cybersecurity AI Systems — Robustness, Fairness, Explainability, and Data Governance
Research Objective: To design and execute experimental evaluation protocols for assessing the compliance-relevant technical properties of AI systems used in cybersecurity contexts — including adversarial robustness, subgroup performance consistency, explainability utility, and training data quality — and to produce both scientific findings and practical compliance frameworks grounded in empirical evidence rather than theoretical mapping alone.
Number of Secondee: 1-2
Candidate Profile: Candidates should have a background in machine learning, AI, computer science, or cybersecurity, with hands-on experience in model training, evaluation, or experimentation. Familiarity with adversarial ML, XAI methods, or fairness evaluation frameworks is a strong advantage. Interest in regulatory and policy dimensions of AI is expected but prior legal knowledge is not required — the work is fundamentally scientific. Programming proficiency in Python and experience with ML frameworks (PyTorch, TensorFlow, scikit-learn) is expected. Candidates who are comfortable designing their own experiments, not just running existing code, are particularly encouraged.
Technical Skills:

- AI & Emerging Technology Security
- Security Policies, Standards & Compliance
- Privacy & Data Protection
- GDPR Compliance & Data Protection Practices
- Research Methodology & Academic Writing
- Data Management & FAIR Data Principles

Soft Skills:

- Problem-Solving & Critical Thinking
- Creativity, Innovation & Vision
- Communication & Stakeholder Engagement
- Ethical Judgement & Professional Responsibility
- Adaptability & Continuous Learning
- Intercultural Communication
- Presentation & Public Speaking Skills

Researcher 4

Research Pathway: Dual-use unmanned systems — autonomous ground vehicles (UGV), unmanned aerial vehicles (UAV), and autonomous underwater vehicles (AUV) — are increasingly central to both civilian applications (inspection, logistics, environmental monitoring) and defence operations (reconnaissance, logistics, contested environment navigation). These systems present a unique and underexplored cybersecurity challenge: they rely on a complex stack of sensors, real-time communication links, embedded AI decision systems, and command-and-control protocols — each of which represents a potential attack surface.
VILNIUS TECH launches a dedicated dual-use technology programme covering unmanned systems across all three domains. This programme is built on the university's existing strengths in electronics engineering (UAV/radar research published in Drones, Electronics — WoS SCIE), embedded AI (NVIDIA Jetson lab), and

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

cybersecurity (DIGI-DEFENSE). The secondee will work at this intersection — examining attack vectors, developing detection mechanisms, and contributing to secure-by-design principles for autonomous platforms.

Topic: Cybersecurity of Dual-Use Unmanned Systems — UAV, UGV, and AUV Attack Surface Analysis and Defence
Research Objective: To identify, characterise, and develop mitigations for cybersecurity vulnerabilities in dual-use unmanned systems, covering communication link security, sensor spoofing and jamming resilience, secure C2 protocols, and AI model integrity in autonomous decision-making pipelines.
Number of Secondee: *1-2*
Candidate Profile: Candidates should have a background in cybersecurity, computer science, electronics engineering, or a related field, with interest in embedded systems, autonomous platforms, or OT/IoT security. Experience with signal processing, communication protocols (MAVLink, DDS, ROS), or penetration testing is an asset. Candidates with a mix of software and hardware security curiosity are especially welcome, as the research environment bridges both.
Technical Skills:

- Network Security & Architecture
- OT/IoT Security & Zero Trust Architecture
- AI & Emerging Technology Security
- Cryptography & Data Protection
- Incident Management & Response
- Research Methodology & Academic Writing

Soft Skills:

- Problem-Solving & Critical Thinking
- Adaptability & Continuous Learning
- Creativity, Innovation & Vision
- Ethical Judgement & Professional Responsibility
- Intercultural Communication
- Presentation & Public Speaking Skills

Researcher 5 - Open Research Track

Research Pathway: VILNIUS TECH's DIGI-DEFENSE Centre is home to researchers who have worked across AI-driven threat detection, digital forensics, post-quantum cryptography, embedded systems security, unmanned systems, and cybersecurity education — spanning some of the most consequential open problems in the field. We recognise that the most productive research collaborations often begin not from a pre-defined topic but from a genuine meeting of curious minds.

This position is therefore intentionally open. If you have an idea in cybersecurity — a problem that keeps you up at night, a method you want to try, a gap in the literature you've identified, a threat model nobody has properly addressed — we want to hear it. We offer a research environment where your proposal will be taken seriously, discussed with experienced practitioners and academics, and shaped into a real research contribution. Lithuania is a small country that punches far above its weight in digital infrastructure, cybersecurity policy, and technical talent; it sits on NATO's eastern flank and deals with hybrid threats as an operational reality, not an abstraction. Living and working here for four months means engaging with a cybersecurity ecosystem that is genuinely motivated.

We are particularly — though not exclusively — interested in proposals touching on: AI security and adversarial robustness; quantum-safe communications; security of autonomous and unmanned systems; cyber-physical system resilience; digital forensics methodology; identity and authentication; or cybersecurity governance and compliance. But we will give serious consideration to any well-reasoned idea brought by a motivated researcher.

Topic: Open — Proposed by the Secondee

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

Research Objective: To be defined collaboratively between the secondee and the DIGI-DEFENSE research team based on the secondee's proposed research idea, with alignment to the Centre's active research areas and the WEM Cyber project's broader objectives.
Number of Secondee: *1*
Candidate Profile: Any background in cybersecurity or a closely related technical or interdisciplinary field is welcome. The key requirement is a concrete, well-articulated research idea or question that the candidate is genuinely motivated to pursue. Candidates should be able to describe their proposed topic, its significance, and a rough sense of the approach they would take. The secondee will have the opportunity to present their proposal to the DIGI-DEFENSE team at the start of the secondment and to refine it collaboratively.
Technical Skills:

- Any domain within cybersecurity relevant to the candidate's proposed topic
- Research Methodology & Academic Writing
- Problem-Solving & Critical Thinking (as a technical skill — the ability to frame and decompose research problems)

Soft Skills:

- Creativity, Innovation & Vision
- Communication & Stakeholder Engagement
- Problem-Solving & Critical Thinking
- Adaptability & Continuous Learning
- Ethical Judgement & Professional Responsibility
- Intercultural Communication
- Presentation & Public Speaking Skills

R&I Staff 1
Research Pathway: Modern cyber investigations increasingly rely on AI-assisted forensic tooling to cope with the volume, complexity, and speed of digital evidence. At the same time, AI systems themselves — including large language models and computer vision components — are becoming targets of adversarial manipulation, model poisoning, and data exfiltration, creating a new forensic discipline: AI forensics. VILNIUS TECH AI platform provides a high-capability environment for developing and testing AI-augmented forensic workflows and adversarial ML investigation techniques.
The secondee will work within DIGI-DEFENSE's forensics and incident response team, contributing to research on AI-enhanced digital investigation tools, forensic readiness frameworks for organisations deploying AI systems, and cross-border evidence handling procedures relevant to EU cybersecurity regulation.

Topic: AI-Augmented Digital Forensics and Incident Response
Research Objective: To develop and validate AI-assisted methodologies for digital forensic investigation, with a focus on scalable evidence analysis, AI system forensic readiness, and integration of ML tools into incident response workflows compliant with EU legal and regulatory frameworks.
Number of Secondees: 1-2
Candidate Profile: Candidates should have a background in cybersecurity, information systems, computer science, or digital forensics. Familiarity with forensic tools (e.g. Magnet, FTK, Belkasoft, EnCase), Python scripting, and interest in machine learning applications is advantageous. An understanding of legal and procedural dimensions of digital evidence (chain of custody, GDPR implications) is a plus. Candidates motivated to bridge technical forensic work with AI research are particularly encouraged.
Technical Skills:

- Incident Management & Response
- AI & Emerging Technology Security
- Security Policies, Standards & Compliance
- GDPR Compliance & Data Protection Practices

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

- Data Management & FAIR Data Principles
- Research Methodology & Academic Writing

Soft Skills:

- Problem-Solving & Critical Thinking
- Ethical Judgement & Professional Responsibility
- Risk Communication & Security Awareness
- Adaptability & Continuous Learning
- Communication & Stakeholder Engagement
- Time Management & Task Prioritisation
- Intercultural Communication

UBITECH

About Organisation

UBITECH has strong technical expertise in the design, development, integration, and deployment of advanced ICT solutions, combining applied research excellence with industrial-grade software engineering. Its core competencies include cloud computing, software engineering, 5G technologies, digital security, big data and analytics, cyber-physical systems, IoT, energy efficiency, and e/m-health systems. The company specializes in scalable, secure, and interoperable system architectures using modern software engineering approaches, including microservices, API-driven integration, DevOps practices, and advanced data management technologies. UBITECH also has extensive experience in cybersecurity and secure software development, applying encryption, authentication, digital signatures, penetration testing, and vulnerability assessment across mission-critical IT projects in finance, security, e-government, and industry.

Domains:

- Information Security Governance & Risk Management
- Asset Management & Data Classification
- Access Control & Identity Management
- Network Security & Architecture
- Cryptography & Data Protection
- Incident Management & Response
- Cloud Security
- AI & Emerging Technology Security
- Privacy & Data Protection

Location: Greece

Research Duration: *No preferred secondment format (2+2 / 4 month continuous)*

Researcher 1

Research Pathway: The secondee will support research and development activities in the area of cybersecurity and data-driven technologies, contributing to the design, development, and validation of innovative solutions. Activities may include data analysis, modelling, and the application of advanced techniques such as machine learning and automation, depending on project needs. The secondee will work with structured and unstructured datasets, support the development and integration of intelligent components, and contribute to system-level implementations within ongoing R&D and innovation projects. Tasks may also involve participation in pilot activities, testing, validation, and performance assessment of developed solutions in real or simulated environments.

Topic: *AI-driven Cybersecurity & Data Analytics Researcher*

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

Research Objective: *To design, develop, and validate data-driven and AI-based cybersecurity solutions.*
Number of Secondee: 1
Candidate Profile: Degree in Data Science, AI, Computer Science, or related field; experience in machine learning and data analysis; knowledge of Python and ML frameworks; interest in cybersecurity applications; strong analytical and problem-solving skills.
Technical Skills:

- Information Security Governance & Risk Management
- Security Policies, Standards & Compliance
- Access Control & Identity Management
- Cryptography & Data Protection
- Research Methodology & Academic Writing
- Data Management & FAIR Data Principles
- Asset Management & Data Classification
- Incident Management & Response
- Privacy & Data Protection

Soft Skills:

- Problem-Solving & Critical Thinking
- Adaptability & Continuous Learning
- Creativity, Innovation & Vision
- Ethical Judgement & Professional Responsibility
- Risk Communication & Security Awareness
- Behavioural Understanding & Trust Building
- Time Management & Task Prioritisation
- Intercultural Communication
- Presentation & Public Speaking Skills

Researcher 2
Research Pathway: The secondee will support research and innovation activities related to the design, development, and validation of digital and cybersecurity solutions. Activities may include contributing to technical development, analysis, and integration tasks, depending on project requirements. The secondee will collaborate with multidisciplinary teams and participate in testing, validation, and pilot activities, supporting the assessment and improvement of developed solutions.
Topic: Research & Innovation Associate
Research Objective: *To support the development, implementation, and validation of digital and cybersecurity systems.*
Number of Secondee: 1
Candidate Profile: Degree in Computer Science, Engineering, or related field; basic programming skills (e.g. Python, Java); interest in digital technologies or cybersecurity; analytical thinking and teamwork skills.
Technical Skills:

- Information Security Governance & Risk Management
- Security Policies, Standards & Compliance
- Access Control & Identity Management
- Cryptography & Data Protection
- Cloud Security
- Research Methodology & Academic Writing
- Data Management & FAIR Data Principles
- GDPR Compliance & Data Protection Practices
- Asset Management & Data Classification
- Incident Management & Response
- Privacy & Data Protection

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

Soft Skills:

- Problem-Solving & Critical Thinking
- Adaptability & Continuous Learning
- Creativity, Innovation & Vision
- Ethical Judgement & Professional Responsibility
- Risk Communication & Security Awareness
- Behavioural Understanding & Trust Building
- Time Management & Task Prioritisation
- Intercultural Communication
- Presentation & Public Speaking Skills

Researcher 3

Research Pathway: The secondee will contribute to the development and integration of software-based solutions within research and innovation projects. Activities may include supporting system implementation, integration of components, and optimisation of digital services, depending on project needs. The secondee will collaborate with technical teams to ensure interoperability and efficient operation of systems and will participate in testing and validation activities.

Topic: Software & Systems Development Associate

Research Objective: *To contribute to the development, integration, and optimisation of digital services and software systems.*

Number of Secondee: 1

Candidate Profile: Degree in Software Engineering, Computer Science, or related field; programming or software development skills; understanding of system integration and APIs (desirable); familiarity with data processing or application development; basic awareness of secure software development practices; interest in software development and system integration; problem-solving mindset and ability to work in multidisciplinary teams.

Technical Skills:

- Information Security Governance & Risk Management
- Security Policies, Standards & Compliance
- Cryptography & Data Protection
- Cloud Security
- Research Methodology & Academic Writing
- Data Management & FAIR Data Principles
- GDPR Compliance & Data Protection Practices
- Privacy & Data Protection
- Incident Management & Response
- Asset Management & Data Classification

Soft Skills:

- Communication & Stakeholder Engagement
- Problem-Solving & Critical Thinking
- Adaptability & Continuous Learning
- Creativity, Innovation & Vision
- Ethical Judgement & Professional Responsibility
- Risk Communication & Security Awareness
- Behavioural Understanding & Trust Building
- Time Management & Task Prioritisation
- Intercultural Communication
- Presentation & Public Speaking Skills

ONINC ELEKTRONIK (CYBERWARE)

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

About Organisation

Oninç / Cyberware specializes in the design and development of in-vehicle cybersecurity units and edge-connected automotive systems, with a focus on secure and scalable architectures across embedded devices, communication layers, and cloud-based platforms. Its expertise includes embedded cybersecurity, secure boot, firmware authentication and signing, hardware-backed key management, secure OTA updates, and intrusion and anomaly detection for in-vehicle networks. The organization works with automotive communication systems such as CAN, CAN FD, LIN, WiFi, Bluetooth, and GSM/LTE, while developing event-driven and streaming-based data pipelines for telemetry and security monitoring. Within WEM Cyber, Oninç / Cyberware offers secondees hands-on experience in secure system design, threat analysis, penetration testing, and applied automotive cybersecurity.

Domains:

- Access Control & Identity Management
- Network Security & Architecture
- Cryptography & Data Protection
- Cloud Security
- OT/IoT Security & Zero Trust Architecture
- Privacy & Data Protection

Location: *Türkiye*

Research Duration: *4 Months (Continuous)*

Researcher

Research Pathway: The transition to Software-Defined Vehicles (SDV) expands the automotive attack surface, requiring holistic cybersecurity frameworks to ensure system integrity, secure updates, and reliable communication across distributed components. In-vehicle networks such as CAN and CAN FD present inherent security vulnerabilities, creating a need for lightweight and scalable protection mechanisms that can be integrated without impacting system performance. Another key area is intrusion and anomaly detection in automotive systems, where data-driven approaches are explored to identify abnormal behavior in real time while maintaining low computational overhead and minimizing false positives. Additionally, secure embedded system design remains critical, focusing on implementing effective yet lightweight security solutions (e.g., secure boot, cryptography, HSM) in resource-constrained environments, while ensuring long-term maintainability. Depending on the secondee's expertise, additional topics may include secure edge-to-cloud communication, data integrity and transmission, OTA updates, hardware-based security, and telemetry-based anomaly detection in connected systems.

Topic: *Cybersecurity for Software-Defined Vehicles (SDV), In-vehicle network security (CAN / CAN FD), Intrusion detection and anomaly detection in automotive systems, Edge-to-cloud secure communication architectures, Secure embedded systems design for resource-constrained devices*

Research Objective: *To develop and evaluate secure architectures and detection mechanisms for in-vehicle and edge-connected systems.*

Number of Secondee: 1

Candidate Profile: The organization seeks to host a secondee at BSc, MSc, or PhD level in computer engineering, computer science, electrical and electronics engineering, cybersecurity, or related fields. The preferred profile includes candidates with an interest in cybersecurity for connected and software-based systems, particularly in cloud security, network security, data protection, and IoT/edge systems. Familiarity with software development and system-level thinking is expected; prior cybersecurity experience is beneficial but not mandatory. Candidates interested in applied research and real-world challenges across embedded systems, cloud platforms, and data analysis are especially encouraged.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

Technical Skills:

- Access Control & Identity Management
- Network Security & Architecture
- Cryptography & Data Protection
- Cloud Security
- OT/IoT Security & Zero Trust Architecture

Soft Skills:

- Communication & Stakeholder Engagement
- Leadership & Team Collaboration
- Problem-Solving & Critical Thinking
- Adaptability & Continuous Learning
- Intercultural Communication
- Presentation & Public Speaking Skills

SPHERETECH

About Organisation

SphereTech is a cybersecurity-focused company providing comprehensive security architectures, cloud security solutions, and integrated security ecosystems. Its services include the deployment, optimization, and continuous monitoring of security infrastructures, as well as professional implementation and operational support tailored to customer needs. Through its R&D activities, SphereTech develops in-house solutions such as Cylana, which focuses on third-party risk scoring and External Attack Surface Management, enabling organizations to proactively identify and mitigate external cybersecurity risks. The company combines expertise in cloud security, security integration, managed security, and cybersecurity solution design, offering secondees exposure to real-world security operations, applied R&D, and industry-oriented cybersecurity practices.

Domains:

- Information Security Governance & Risk Management
- Security Policies, Standards & Compliance
- Asset Management & Data Classification
- Access Control & Identity Management
- Incident Management & Response
- Supply Chain & Third-Party Security
- Cloud Security

Location: *Türkiye*

Research Duration: *2 + 2 Months (Split Arrangement)*

Researcher

Research Pathway / Description of Work:

- Gathered and analysed business requirements through structured sessions with stakeholders
- Conducted process analysis and created BPMN workflow documentation
- Prepared BRD, FDD, and UML diagrams
- Facilitated Agile/Scrum ceremonies and managed user stories in Jira
- Coordinated communication between business units and development teams throughout SDLC
- Wrote SQL queries on PostgreSQL for data analysis and requirement validation
- Developed test scenarios and coordinated UAT with business units

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

- Analysed API specifications and documented AWS based system integrations
- Created mock-ups and wireframes for UI/UX requirements visualization
- Identified process improvements using ELK stack data analysis
- Maintained comprehensive project documentation and regular status reports

Topic: *Product Owner*

Research Objective: *To support the development and management of a cybersecurity product by translating business and technical needs into actionable product requirements.*

Number of Secondee: 1

Candidate Profile: Background in a relevant technical field; knowledge of SQL, data analysis, and requirement analysis; interest in cybersecurity (especially EASM and cloud security); strong analytical thinking and communication skills.

Technical Skills:

- Information Security Governance & Risk Management
- Security Policies, Standards & Compliance
- Supply Chain & Third-Party Security
- GDPR Compliance & Data Protection Practices
- Project Management & Reporting (EU Projects)
- Asset Management & Data Classification
- Incident Management & Response

Soft Skills:

- Communication & Stakeholder Engagement
- Leadership & Team Collaboration
- Problem-Solving & Critical Thinking
- Risk Communication & Security Awareness
- Behavioural Understanding & Trust Building
- Time Management & Task Prioritisation

Secondee Profile

The secondee must be a staff member of a partner organisation acting as a sending organisation within the WEM Cyber consortium and must receive approval from the relevant decision-makers of the sending organisation for participation in the secondment. In addition, candidates should meet the following qualifications:

- A bachelor's degree (or equivalent) in related field, or equivalent professional experience; a master's degree is preferred.
- Demonstrated interest in relevant research and/or topics.
- Ability to work in a multidisciplinary and international research environment.
- Strong analytical and problem-solving skills.
- Preferably a strong academic background and performance in previous studies or research activities.
- Proficiency in English, both written and spoken, as all communication and collaboration will be conducted in English.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

- Personal qualities such as initiative, teamwork, communication skills, and the ability to work both independently and collaboratively with international project partners,
- Motivation and enthusiasm for interdisciplinary research and innovation activities.

Mobility Rules

Secondments will be organised through coordination between the sending organisation and the hosting organisation, considering the research objectives of the project and institutional timelines. The following rules apply:

1. Planned Start Date: Secondments are expected to begin in September, when most secondees will relocate to the hosting country.
2. Possible Postponement: The start date may be postponed for **up to two months if necessary**. This must be agreed upon by both the sending and hosting organisations. Such postponements are allowed but not encouraged.
3. Secondment Agreement: Each secondee will sign a **Secondment Agreement** before the mobility begins. This agreement will define the responsibilities, rights, and procedures for the secondee, the sending organisation, and the hosting organisation.
4. Responsibilities During the Secondment: **The hosting organisation** will support the secondee in daily research activities, workplace integration, and local coordination while **the sending organisation** will remain responsible for employment-related matters such as salary and administrative arrangements.
5. Duration of the Secondment: Each secondment will take **4 months in total**.
6. Flexible Mobility Structure: The secondment period may be organised in two separate periods of 2 months, with a break in between if required. This arrangement can be implemented based on the **secondee's request** and with the **approval of both the sending and hosting organisations**.

This structure ensures flexibility while maintaining alignment with the project's research objectives and institutional requirements.

Salary & Allowance

During the secondment period, all secondees will **remain employed by their sending organisations** and will continue to **receive their regular salary** through their existing payroll arrangements. No changes will be made to the employment contract or salary structure during the mobility period. The secondment budgets under the project, as stated in the Grant Agreement (GA), has been calculated based on all partners' PM flat rates, with a €1000 per month allowance increased, which is intended to support accommodation and general living expenses during the secondment period, in line with the project rules and internal procedures.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

The hosting organisation will not provide any additional salary to secondees.

Additional support

Mentorship Programme	Business mentor from Women4Cyber network 1–2 hours of guidance per month Career support and industry insights
Coaching Services	At least 4 coaching sessions Career planning, communication and confidence Leadership and decision-making support
Training Programmes	Tailored to self-assessment gaps 2–3 online training sessions Recorded and shared with all 3 cohorts
Cybersecurity Certifications	Up to €500 per participant Based on technical needs Can be obtained 6 months after return
Other R&I Certifications	Available for other R&I staff Same approach as researchers' secondments
Event Attendance	Workshop, conference or industry event Present research and expand networks

Besides the monetary benefits and the support given by the project partners during the Secondment, where they will have a dedicated tutor Secondees will receive mentoring, coaching and training to enhance their technical and soft skills. Additionally, Secondees will be provided the option of acquiring certifications related to cybersecurity or other R&I fields.

Funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101216854

wem cyber

Consortium

BİLİŞİM VADİSİ
VILNIUS TECH
UBITECH ubiquitous solutions
WOMEN 4CYBER
upf. Universitat Pompeu Fabra Barcelona
University of Maribor
Boğaziçi Üniversitesi 1863
Université de Toulouse
CyberWhiz
SecroMix #SeeWhat'sNext
CYBERWARE
SPHERETECH
<CloudMetrik>

Funded by
the European Union