Digital skills gap analysis for regional expert development

Umberto Morelli, Muhammad Imran
Fondazione Bruno Kessler

umorelli@fbk.eu
mimran@fbk.eu
https://www.fbk.eu

Content review

01 About us

The FBK Center for Cybersecurity activities and mission

02 Our role in MERIT

Main contribution

03 Past and current skill gaps

Leveraging the results of the recurrent analysis of market needs, state-of-the-art and innovative topics, technologies and application areas - focus on the CS domain

04 Gaps at the intersection of AI and CS domains

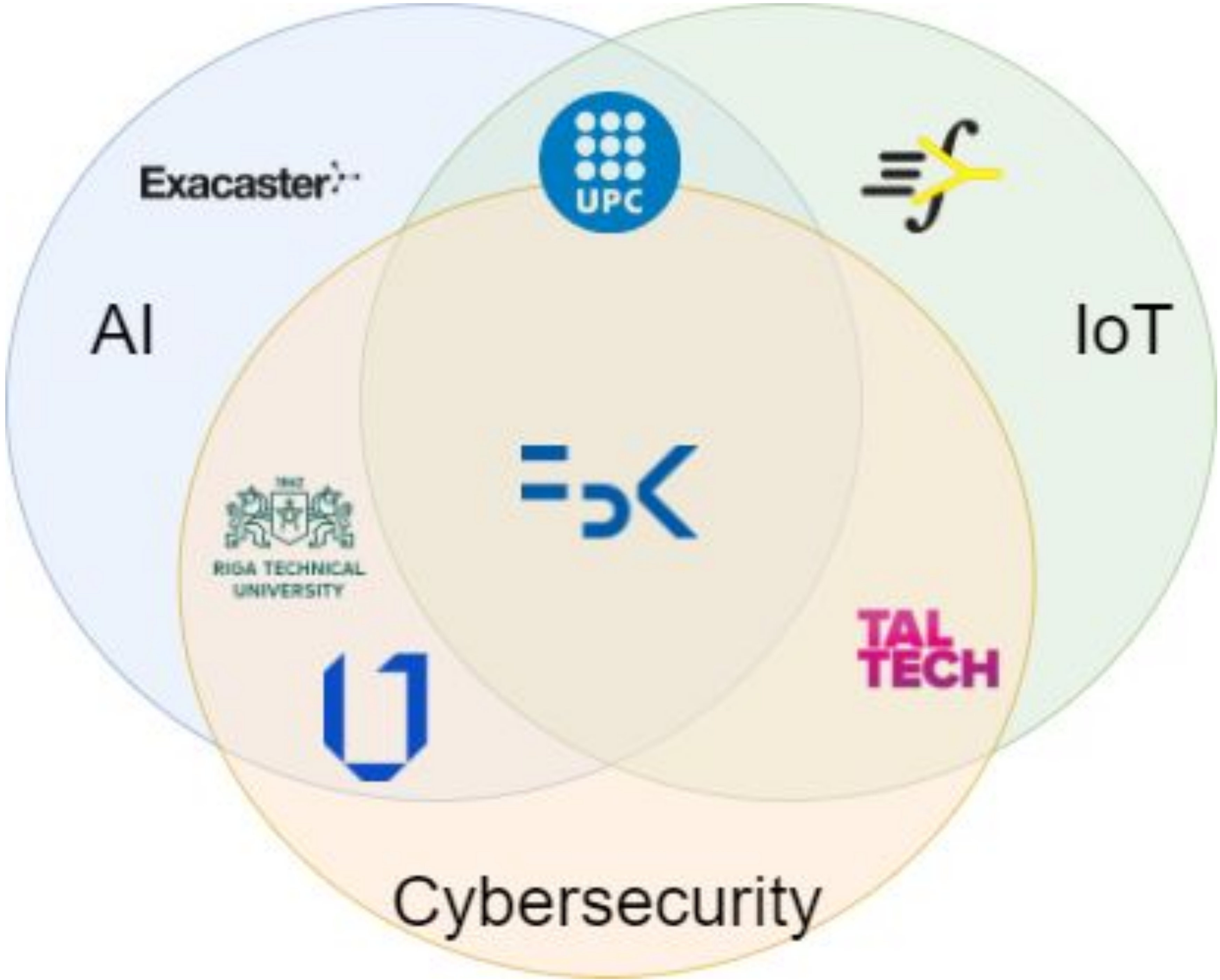
Job demand for outstanding specialized skills

The FBK Center for Cybersecurity

Advancing methodologies for security risk management in distributed and decentralized systems in 3 areas:

- Digital identity [Security&Trust research Unit].
- Distributed infrastructures [RISING research Unit].
- Applied cryptography [Aleph research Unit].

https://cs.fbk.eu



Our (main) role in MERIT

- Developing and pursuing a methodology to recurrently identify the most suitable topics, technologies and application areas in the AI, CS and IoT domains to design and update MERIT study programs.
- Increase the reputation of consortium universities, as leaders in AI, IoT and cybersecurity areas, thus becoming a close-by expert to the society and industry of digital competencies.

2nd Annual market and state of the art analysis for the AI, CS and IoT domains
Industry perspective

10 current research and statistics, reports and forecasts

- The EU Rewire project.
- The European Network and Information Security Agency (ENISA).
- The Italian Clusit.
- The World Economic Forum.
- (US) Splunk.
- The ACM and ScienceDirect research portals.

10 organizations

Operating in the fintech, robotics, AI and IoT domains, with marketing or more general IT services.

2nd Annual market and state of the art analysis for the AI, CS and IoT domains
List of topics, technologies and application areas

1. Monitoring of large-scale and possibly interconnected systems;
2. Machine learning with context-awareness;
3. Decision Intelligence;
4. Automation of preventive measures, and encrypting personal and sensitive data;
5. Predictive analytics;
6. Threat Modelling;
7. DevSecOps;
8. Phishing (prevention);
9. Zero Trust principles (Zero Trust Network Access - ZTNA);
10. AI cloud services and AIOps;
11. Ransomware (prevention);
12. User behavioural tracking;
13. Cloud-native tools that use machine learning to filter logs;
14. Proactive threat detection;
15. Automated incident response protocols;
16. Security information and Event Management (SIEM);
17. Vulnerability management for DevSecOps;
18. OS vulnerabilities;
19. The use of AI to detect vulnerabilities;
20. Privilege separation and least-privileged access, as well as using privileged access workstations (PAWs) for managing identity systems;
21. Identity-based segmentation, SD-WAN and Network Traffic Analysis.
22. Advanced authentication procedures (MFA, conditional AC, behavioural, passwordless);
23. Cloud computing, mobile application security, API management and SDKs;
24. Cyber Threat Intelligence and cyber deception;
25. Security Orchestration Automation and Response (SOAR).

2nd Annual analysis
CS topics, technologies and application areas to prioritize

01 | 11

Monitoring of large-scale and interconnected systems

Overseeing complex systems, networks, and applications to detect anomalies, performance issues, and security threats.

E.g., SIEM-Based Network Monitoring.

02 | 11

Threat Modeling

Structured approach to identifying and assessing potential threats to a system or application

E.g., Microsoft STRIDE framework.

2nd Annual analysis
CS topics, technologies and application areas to prioritize

03 | 11

Zero Trust

A multi-layered approach to CS based on three pillars:
- Verify explicitly;
- Use least-privilege access;
- Assume breach.

E.g., Microsoft Zero Trust strategy.

04 | 11

Risk Management and governance

Managing risks, mitigation strategies, compliance, and organizational policies, but also legal and ethical considerations.

E.g., ISO/IEC 27001 ISMS.

2nd Annual analysis
CS topics, technologies and application areas to prioritize

05 | 11

Machine learning with context-awareness

Leveraging ML techniques to adapt and make decisions based on contextual information.

E.g., contextual Anomaly Detection.

06 | 11

Security Orchestration Automation and Response (SOAR)

Coordinating security processes through automation and orchestration.

E.g., Threat Intelligence Playbooks.

07 | 11

Cloud computing, mobile application security, API management, and SDKs

Ensuring security across cloud services (more generally XaaS), mobile apps, APIs, and software development kits.

E.g., enforcing the OWASP Mobile Security Testing Guide.

08 | 11

AI-based cybersecurity systems

Using AI for threat detection, prevention, and response.

E.g., AI-Driven Threat Detection.

09 | 11

Penetration Testing

Ethical hacking to identify vulnerabilities in systems.

E.g., Web Application Penetration Testing via OWASP ZAP.

10 | 11

Advanced Authentication Procedures

Secure authentication methods, including multi-factor authentication (MFA), conditional access and behavioral authentication.

E.g., Multi-Factor Authentication (MFA).

11

Personal data protection

Safeguarding sensitive personal information from unauthorized access or disclosure.

| 11

E.g., Data Encryption at rest and in transit.

2nd Annual analysis

Mapping with the European Skills, Competences, Qualifications and Occupations (ESCO) classification

3770 results
(149 unique CS values)

1539 occupations
(881 CS-related)

2nd Annual analysis
Results for MERIT Universities - CS

	Cybersecurity Topic or Technology to be provided; Skill or Expertise (in specific application areas) to be developed	To prioritize
Fundamental knowledge	**Monitoring of large-scale and interconnected systems**: This involves overseeing complex systems, networks, and applications to detect anomalies, performance issues, and security threats. Understanding the principles of monitoring and how to analyze system behavior is crucial for cybersecurity professionals. (Ref. to **CS-Q1** in the following Scopus search and in Appendix A).	X*
	Threat Modeling: A structured approach to identifying and assessing potential threats to a system or application. It helps in designing secure systems by anticipating and addressing vulnerabilities early in the development process. (Ref. to **CS-Q2**).	X
	Zero Trust principles (Zero Trust Network Access - ZTNA): A security model that assumes no inherent trust within a network, requiring verification for every access attempt. Understanding Zero Trust architecture is foundational for securing modern networks. (Ref. to **CS-Q3**).	X
	Risk Management and governance: Managing risks, compliance, and organizational policies. Cybersecurity professionals need to understand risk assessment, mitigation strategies, and legal and ethical considerations. (Ref. to **CS-Q4**).	X

2nd Annual analysis
Results for MERIT Universities - CS

	Cybersecurity Topic or Technology to be provided; Skill or Expertise (in specific application areas) to be developed	To prioritize
Applied Knowledge	**Machine learning with context-awareness**: Leveraging machine learning techniques to adapt and make decisions based on contextual information. This skill is valuable for anomaly detection, threat prediction, and adaptive security measures. (Ref. to **CS-Q5**).	X*
	DevSecOps: Integrating security practices into the DevOps process, ensuring security is part of the software development lifecycle. Practical experience in implementing security controls within agile development environments is essential. (Ref. to **CS-Q6**).	
	Security Orchestration Automation and Response (SOAR): Coordinating security processes through automation and orchestration. This involves leveraging cyber threat intelligence and automated workflows to respond effectively to incidents. (Ref. to **CS-Q7**).	X*
	Cloud computing, mobile application security, API management, and SDKs: Ensuring security across cloud services (more generally XaaS), mobile apps, APIs, and software development kits. Practical knowledge of securing cloud environments and mobile applications is crucial. (Ref. to **CS-Q8**).	X
	Incident management: Handling security incidents promptly and effectively. Practical experience in incident response, including containment, eradication, and recovery, is essential. (Ref. to **CS-Q9**).	

2nd Annual analysis
Results for MERIT Universities - CS

	Cybersecurity Topic or Technology to be provided; Skill or Expertise (in specific application areas) to be developed	To prioritize
Applied Knowledge	**AI-based cybersecurity systems**: Utilizing artificial intelligence for threat detection, prevention, and response. Practical skills in implementing AI-driven security solutions are valuable. (Ref. to **CS-Q10**).	X
	Penetration Testing: Ethical hacking to identify vulnerabilities in systems. Practical experience in conducting security assessments and vulnerability testing is essential. (Ref. to **CS-Q11**).	X
	Secure communication protocols: Ensuring secure data transmission over networks. Practical knowledge of encryption, secure channels, and cryptographic protocols is necessary. (Ref. to **CS-Q12**).	
	Advanced Authentication Procedures: Implementing secure authentication methods, including multi-factor authentication (MFA), conditional access (AC), and behavioral authentication. Practical experience in configuring and managing authentication mechanisms is important. (Ref. to **CS-Q13**).	X*
	Personal data protection: Safeguarding sensitive personal information from unauthorized access or disclosure. Practical knowledge of data privacy laws, encryption, and access controls is critical. (Ref. to **CS-Q14**).	X

2nd Annual analysis
Results for MERIT Universities - CS

- Considering the **soft skills**, MERIT HEIs should prioritise for the future set of students:
  - Leadership: They should be able to lead when necessary.
  - Communication: Graduates should be able to communicate effectively in English.
  - Understanding Impact: They should understand the impact of proposed solutions.
  - Problem-Solving: Problem-solving in manufacturing engineering and management is emphasized.
  - Strategy Development: Proficiency in strategy development is expected.
  - Teamwork: They should work well in teams.
  - Critical Thinking: Graduates are expected to exhibit critical thinking.
  - Professional and Ethical Behavior: Adherence to professional and ethical behavior principles is expected.
  - Understanding Legal and Social Aspects: They should understand the legal and social aspects of system management.
  - Continuous Learning: All universities emphasize the importance of continuous learning.
  - Ethical Standards: Adherence to ethical standards is expected.
- Nonetheless, the remaining envisaged set of soft skills constitute an important wealth of experience that could support them both at work and in life:
  - Innovation: They should be able to create innovative solutions.
  - Justification: They should be able to justify their solutions.
  - Security Analysis: They should be able to analyse security weaknesses.
  - Proposing Solutions: They should have the ability to propose innovative and sustainable solutions.

3rd Annual analysis
Preliminary data

27 current research and statistics, reports and forecasts

From ENISA, ResearchGate, IBM, WEF, Forbes, CLUSIT, Gartner, McKinsey & Company, Splunk, The REWIRE EU project, Verizon and the World Economic Forum

14 respondents

From IT and non-IT related fields

Incident response (6/14)

Cyber Threat Intelligence (6/14)

AI-Based Tools (8/14)

Blockchain (7/14)

Healthcare security, financial services protection, supply chain security, regulatory compliance and cybersecurity of manufacturing and industrial sectors (i.e., supply chain resilience) - 2/14

2nd Annual analysis
CS-AI topics, technologies and application areas to prioritize

1. **Technical Skills:**
   - Machine Learning (ML) and Deep Learning (DL) frameworks (e.g., TensorFlow, PyTorch).
   - Knowledge of cybersecurity concepts like SOC operations, zero trust, and penetration testing.
   - Understanding of adversarial machine learning techniques.
   - Proficiency in programming languages (e.g., Python, R) for AI and cybersecurity tool development.
   - Knowledge of IoT protocols (e.g., MQTT, CoAP) and embedded systems.
2. **Analytical Skills:**
   - Data analysis for threat detection and performance optimization.
   - Predictive analytics and risk assessment.
   - Vulnerability management and prioritization.
3. **Soft Skills:**
   - Ethical decision-making for AI use.
   - Communication of complex AI findings to non-technical stakeholders.
   - Collaboration in cross-functional teams for cybersecurity incident response and IoT deployment.

2nd Annual analysis
CS-AI topics, technologies and application areas to prioritize

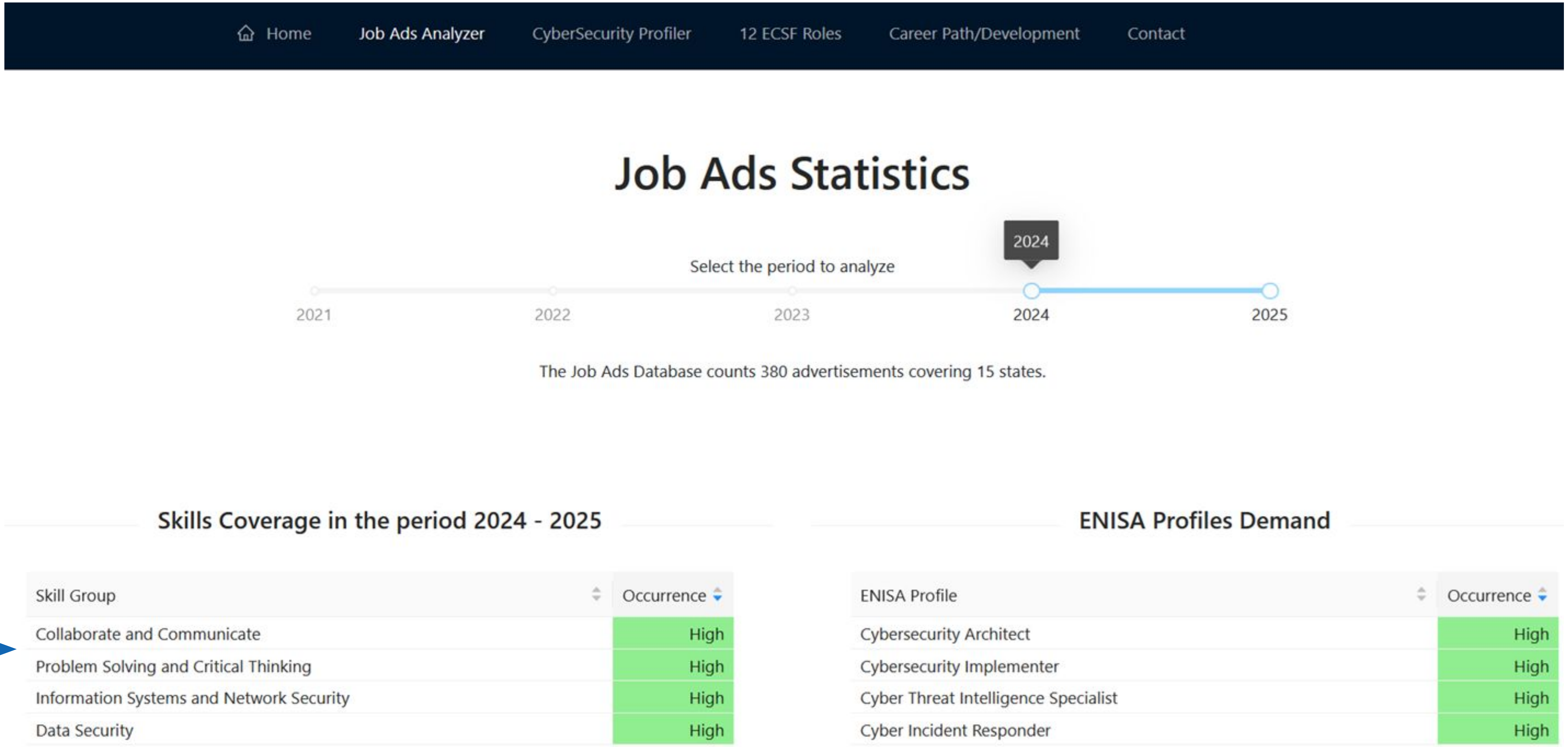
.

1. **AI-Powered Threat Detection**:
   - Predictive analytics, anomaly detection, malware recognition, and real-time intrusion prevention.
2. **Generative AI**:
   - Used in phishing simulation, automated security audits, and adversarial attack generation.
3. **AI for Incident Response**:
   - Tools for automating remediation and mitigating risks after breaches.
4. **Adversarial AI**:
   - Focus on securing AI systems from evasion attacks, data poisoning, and model exploitation.
5. **AI-driven SOC (Security Operations Center)**:
   - Enhancing log analysis, risk assessment, and alert prioritization.
6. **Explainable AI (XAI)**:
   - For transparency in automated decisions affecting cybersecurity measures.
7. **AI-enhanced Vulnerability Scanning**:
   - Automated scanning, prioritizing threats, and patching weak points.
8. **Quantum AI**:
   - Threat to current encryption methods; future cryptography research.
9. **Large Language Models (LLMs)**:
   - Fraud and social engineering defense, especially in text-based attacks.

2nd Annual analysis
CS-AI topics, technologies and application areas to prioritize

1. **AI Cybersecurity Specialist:**
    - Develop AI models for threat detection.
    - Automate incident responses using AI-driven tools.
    - Secure AI systems from adversarial attacks.
    - Conduct ethical hacking and penetration testing with AI.
2. **IoT Security Analyst:**
    - Implement AI-driven security frameworks for IoT networks.
    - Monitor device behavior and detect anomalies using AI.
    - Design encryption and access management protocols powered by AI.
    - Maintain the integrity of IoT device communications.
3. **AI Engineer for IoT Systems:**
    - Build Edge AI models for IoT applications.
    - Optimize IoT systems for predictive maintenance using AI analytics.
    - Develop and test AI-based digital twin simulations.
4. **AI Risk and Compliance Officer:**
    - Ensure AI models in cybersecurity adhere to ethical guidelines.
    - Design governance frameworks for AI applications in IoT and cybersecurity.
5. Mitigate risks associated with AI technologies.

How to stay in-the-loop



Job Ads Statistics

Select the period to analyze

The Job Ads Database counts 380 advertisements covering 15 states.

Skills Coverage in the period 2024 - 2025

Soft skills →

Skill Group	Occurrence
Collaborate and Communicate	High
Problem Solving and Critical Thinking	High
Information Systems and Network Security	High
Data Security	High

ENISA Profiles Demand

ENISA Profile	Occurrence
Cybersecurity Architect	High
Cybersecurity Implementer	High
Cyber Threat Intelligence Specialist	High
Cyber Incident Responder	High

From: https://cyberability-platform.informacni-bezpecnost.cz/job-ads-analyzer/statistics-job

How to stay in-the-loop

Merit D3.4 deliverable - available in April 2025 at https://digitalmerit.eu/deliverables/

https://digitalmerit.eu/news-events/

FONDAZIONE BRUNO KESSLER
CENTER FOR CYBERSECURITY

- https://st.fbk.eu/
- https://aleph.fbk.eu/
- https://rising.fbk.eu/

AI - Questionnaire

CS - Questionnaire

IoT - Questionnaire