

D.3.1 - Annual market and state of the art analysis in the context of IoT, AI and Cybersecurity: First year

Project Title: *Master of Science in Smart, Secure, Interconnected Systems*

Project Start Date: October 1st, 2022

Duration: 48 months

Call: DIGITAL-2021-SKILLS-01

Date of delivery: 31/03/2022

Topic: DIGITAL-2021-SKILLS-01-SPECIALISED

Dissemination Level: Public



Grant Agreement Number:	101083531
Project Title:	Master of Science in Smart, Secure, Interconnected Systems
Project Acronym:	MERIT
Document Number:	D3.1
Document Title:	Annual market and state of the art analysis in the context of IoT, AI and Cybersecurity: First year
Version:	2.0
Delivery Date:	16/07/2024
Lead Beneficiary:	FBK
Editor(s):	Umberto Morelli (FBK)
Authors:	Diego Sona, Federico Lanzi, Imran Muhammad, Salvatore Manfredi, Silvio Ranise, Umberto Morelli
Reviewers:	Òscar Franco Genís (CIT UPC), Egidijus Pilypas (Exacaster)
Keywords:	AI, Cybersecurity, IoT, Teaching topics and technologies, Research excellence, Industry needs
Status:	Final
Dissemination Level	Public
Project URL:	https://www.digitalmerit.eu/

Disclaimer: Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or European Health and Digital Executive Agency (HADEA). Neither the European Union nor the HADEA can be held responsible for them.



Revision History

Rev. No.	Description	Author	Date
0.1	First draft	Umberto Morelli, Salvatore Manfredi (FBK)	26.01.2023
0.2	Second draft	Diego Sona, Federico Lanzi, Imran Muhammad, Salvatore Manfredi, Silvio Ranise, Umberto Morelli (FBK)	23.03.2023
0.3	Content review	Egidijus Pilypas (EXACASTER), Oscar Franco (CIT-UPC)	27.03.2023
0.4	Content review	Simona Ramanauskaitė (VILNIUS-TECH)	29.03.2023
1.0	A final version based on v0.4 with several content and formatting improvements	Umberto Morelli, Salvatore Manfredi (FBK)	30.03.2023
2.0	Mapping of the results to the ESCO and e-CF frameworks: update of the <i>Executive Summary</i> (pg. 6), <i>Methodology</i> (Step 7, pg. 23-25), <i>Conclusions</i> (pg. 42) and addition of <i>Appendix C</i> (pg. 49)	Umberto Morelli, Muhammad Imran (FBK)	16.07.2024



Table of Contents

LIST OF FIGURES	5
LIST OF TABLES.....	5
EXECUTIVE SUMMARY	6
1 INTRODUCTION	7
2 METHODOLOGY	8
3 FINDINGS.....	26
3.1 CS Findings	26
3.2 IoT Findings.....	29
3.3 AI Findings	31
3.4 Industry needs	36
4 CONCLUSIONS	42
REFERENCES	44
APPENDIX A.....	46
APPENDIX B.....	47
APPENDIX C.....	49



List of Figures

Figure 1: methodology to investigate current state-of-the-art and forecasted topics, skills and technologies from both research and industry perspectives; and including Universities' needs.	8
Figure 2: technical skills needed by three of the four target groups in the study - from [18].	32
Figure 3: top cross-cutting, specialized skills of the future - from [14].	40
Figure 4: AI Ecosystem in industrial data space.	41

List of Tables

Table 1: MERIT Partners' areas of expertise.	9
Table 2: list of data sources, their field and scope.	10
Table 4: current and forecasted topics/skills.	16
Table 5: technologies associated with current and future industry needs.	18
Table 6: topics and skills with pertaining technologies.	21
Table 7: cybersecurity controls and relative profiles.	27
Table 8: cybersecurity controls mapping.	27
Table 9: skill gaps for skills needed for Data & AI jobs - from [16].	31



Executive Summary

This document presents the first version of the Deliverable 3.1 (D3.1) for MERIT Work Package 3 (WP3), including the analysis of market needs, state-of-the-art and innovative approaches, and technologies in Artificial Intelligence (AI), Cybersecurity (CS) and Internet of Things (IoT) domains. It provides the methodology to identify the topics and skills, structured as a seven steps process that leverages the available (best) expertise in the MERIT consortium; a first application of the methodology, with the output of each step; and how the AI, CS and IoT fields intertwine in domain-specific working positions. The results of the first application of the methodology are the following:

1. Definition of the areas of expertise of the MERIT Partners;
2. The skills to be developed in the context of study programs by MERIT Universities;
3. A carefully crafted set of data sources and keywords identified by MERIT Partners to investigate current and forecasted topics and skills in AI, CS and IoT;
4. A set of topics and skills identified from research, statistics, reports and forecasts that are crucial to define a study program capable of educating the next generation of experts in the fields of AI, CS, and IoT and their interplays;
5. A set of technologies derived from industry needs whose knowledge is a key enabler to make the skills of the study program operational;
6. A carefully defined mapping from topics to technologies that facilitates the exploitation of the skills developed during the study program;
7. A prioritized list of topics, skills and technologies that can be used as the basis to define a coherent and comprehensive study program coordinated among the Universities in the MERIT consortium. The list is mapped to the skills, knowledge and occupations associated with the EU ESCO and e-CF frameworks to highlight its applicability and potential in the European context.

The goals of the document are: (I) guide the design and upgrade of the MERIT master programme to support current and future industry needs with graduates highly specialized in the most relevant AI, CS and IoT topics; (II) reach a broader audience following the MERIT communication strategy, the participation of SMEs in the programme and future dissemination events; (III) increase the expertise of consortium members from both the research and industry perspectives.

The first edition of D3.1 is published in Month 6 (M6) and updated yearly (M18, 30 and a final version on M42) to reflect the evolving requirement landscape of the market and research dimensions.

The application of the strategy provides input to the design and upgrade of the study programs structure (MERIT WP4), which also investigates the future skillset needed for MERIT graduates, its development (WP5) and administration (WP6), together with all the related events (such as hackathons). In addition, to all the communication and dissemination activities prescribed by WP2.



1 Introduction

WP3 aims to provide the MERIT long-term strategy and identify the most relevant topics for the master programme and related activities, such as hackathons or public outreach events. It operates at three levels:

- Design of the master programme - feeding the identified topics, skills and technologies to WP4 for their teaching/support by tailoring the master programme's structure.
- Development of the programme material - understanding the expertise in the consortium to later distribute responsibilities over the preparation of courses and activities about identified topics, skills and technologies (WP5).
- Administration of the programme - with the possible upskilling of educators or SME employees on identified topics, skills and technologies (WP6).

In addition, WP3 coordinates with WP2 to advance digital skills among its identified target groups, with specific actions to communicate and disseminate the current and future most relevant topics, skills and technologies.

The following specific objectives have been defined for this WP:

- Increase the reputation of consortium universities as leaders in Artificial Intelligence (AI), Cybersecurity (CS) and Internet of Things (IoT) areas, thus becoming a close-by expert to the society and industry of digital competencies.
- Update the teaching staff skills through knowledge and synergy received from the collaboration of different stakeholders.
- Stimulate the growth of advanced digital skills in Europe by attracting additional target groups to choose AI, IoT and Cybersecurity master studies or individual courses to broaden and deepen the set of required skills to tame the challenges and complexity of current and next generation systems.

To fulfil these objectives, D3.1 provides:

- The methodology to leverage the consortium member expertise and investigate the most relevant topics, skills, and technologies in the context of AI, CS and IoT, from both market and research perspectives.
- The first application of the methodology to obtain a prioritised list of topics to provide WP4.

Organisation of the document

The document is organised as follows. Section 2 presents the seven-steps methodology to identify the skills and topics, and its first application. Section 3 provides the main findings from identified data sources and the specialised AI, AI-CS and AI-IoT roles. The deliverable concludes with Section 4, where a summary of the results and the link with other MERIT WPs are put forward.

2 Methodology

This Chapter describes the approach to investigating current and forecasted skills and topics. Figure 1 summarises the methodology steps (indicated as flag numbers) performed by the different Partners of the MERIT consortium. An output (a list or a table, inline or in the Appendix) corresponds to each step.

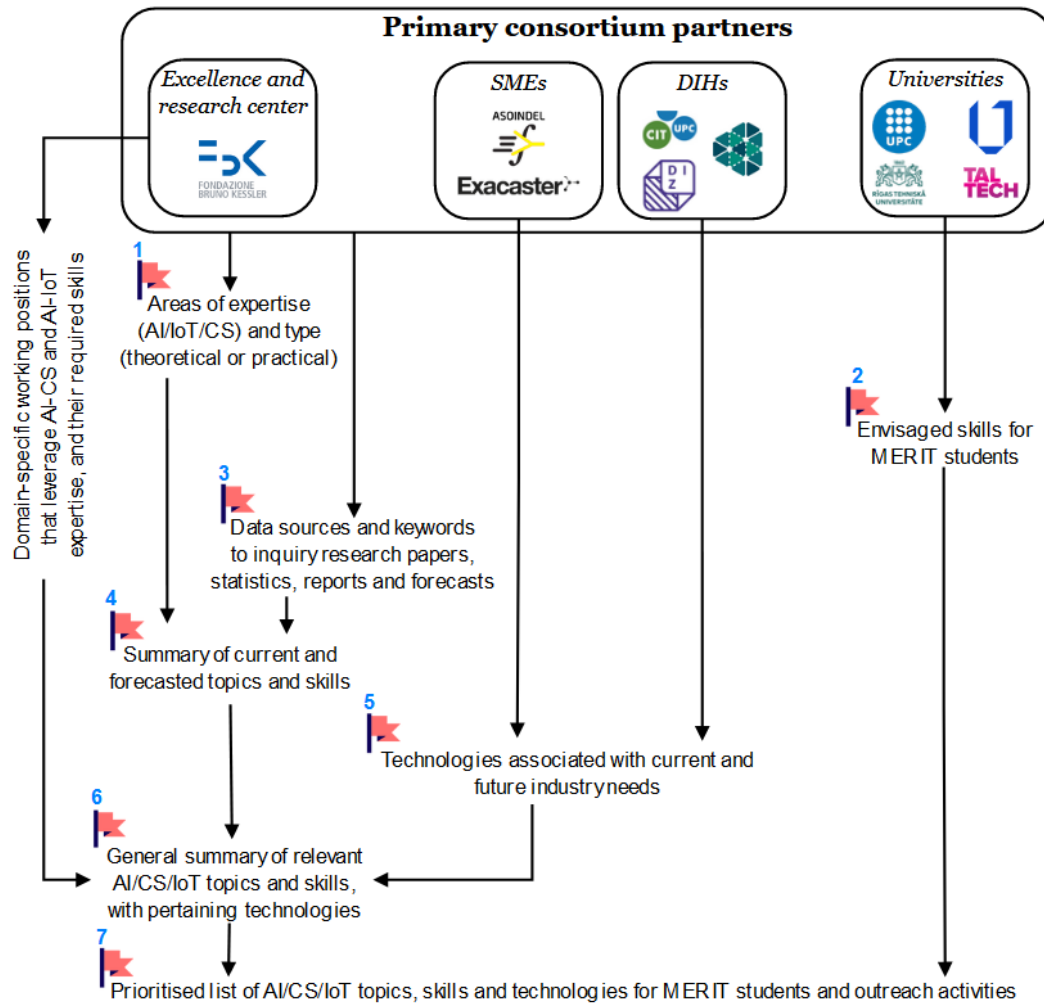


Figure 1: methodology to investigate current state-of-the-art and forecasted topics, skills and technologies from both research and industry perspectives; and including Universities' needs.

Figure 1 provides the MERIT consortium members: one Excellence and Research Centre (FBK), four Universities (UPC, Vilnius Tech, RTU, and TalTech), two SMEs (Exacaster and Asoindel), and three DIHs (Cit-UPC, DIZNE and SSMTTP). The following methodology takes advantage of FBK expertise to identify the domain-specific working positions (AI-CS and AI-IoT) and their required skills; and to generate the output at each step. In addition, it distributes the responsibilities according to the different areas of expertise (in general Universities and FBK to the state-of-the-art, SMEs and DIHs to industrial needs); and considers the specific Universities' needs to prioritise identified topics and skills.



Approach

To understand the relevant set of topics, skills and technologies for MERIT students (and a broader audience in accordance with future MERIT outreach and upskilling activities) the consortium developed a methodology inspired by the requirement elicitation process reported in [1]. We decided to:

- 1) Request each MERIT partner their **area of expertise** to focus contributions to the state-of-the-art investigation. The goal was to create three groups according to the declared expertise.

Step 1 intermediate data

Table 1 highlights how all three areas are covered from theoretical (**Research and Teaching**) and practical (**Prototyping and Laboratories**) perspectives, especially AI and IoT. Therefore, the competence of the consortium members in investigating (and later administering) the necessary topics/skills.

Table 1: MERIT Partners' areas of expertise.

Partners	AI Expertise	Cybersecurity expertise	IoT Expertise
	Research, Teaching, Prototyping, hosting of Laboratories		
FBK	R, T, P	R, T, P	R, T, P, L
UPC	P	T	R, T, P, L
Vilnius tech	R, T	R, T, L	R, T, L
RTU	R, T, P, L		R, T, P, L
TalTech	R, T	R, T	R, T, P, L
Exacaster	R, P		
Asoindel	R		T, P, L
DIZNE	R, T, P	R, T, P	R, T, P
SSMTP	T	T, L	
CIT-UPC	R		R

- 2) Request each University the set of **mandatory skills** they want their students to develop, to guide the investigation and later prioritise identified topics/skills in the MERIT programme.

Step 2 intermediate data

The following skill areas have been identified by requesting all consortium Universities the envisaged set of skills for their future MERIT students: VilniusTech provided the expected components and outcomes of different ICT study programs (with soft skills, foundational knowledge and applications); UPC provided a set of transversal competences; TalTech a set of hard skills, with a focus on management and economics; finally, RTU a set of soft and hard skills, with a focus on innovation and new technologies. Indeed, the identified skill set is quite heterogeneous and required a careful analysis to identify the essential competencies across the three main domains of focus of the MERIT project and keep the list of skill area not redundant as well as containing all aspects to meet the requirements of all four countries and institutions. To provide a coherent and homogeneous account, we have conducted a careful and deep analysis to define the following organised list of different needs. For better understanding and easier application, it was structured into several different areas too:



- Foundational knowledge.
 - Innovation and new technologies.
 - System, organisation and work improvement.
 - Digitalisation and digital transformation.
 - Economics and business.
 - Computer Science / CS Engineering.
 - Conduct research.
 - Applied knowledge.
 - (multi-disciplinary and real-world) Problem solving.
 - Focus on economics.
 - Demonstrate creativity.
 - Knowledge-based decisions and impact on business, society and the environment.
 - Focus on computer Science / CS Engineering.
 - Communication (inside and outside organisations).
 - Achieve high-level job positions.
 - Learn/work efficiently and independently.
- 3) Identify (as the consortium) the set of data sources and keywords to gather the most relevant documents in the context of AI, CS and IoT.

Step 3 intermediate data

Table 2 provides the agreed set of sources, the scope (Global, EU, or Regional), the domain (AI, CS, IoT), and if it has been used to query research papers, statistics, reports or forecasts.

Table 2: list of data sources, their field and scope.

Source with link	Scope	Field	Used as a source of		
			Research or Statistics	Reports	Forecasts
IEEEExplore	Global to Regional	AI/CS/IoT	V		
ResearchGate	Global to Regional	AI/CS/IoT	V		
Google Scholar	Global to Regional	AI/CS/IoT	V		
ENISA	EU	AI/CS/IoT	V	V	V
CLUSIT	Regional (IT)	AI/CS/IoT			
Gartner	Global	AI/CS/IoT			V
Web of Knowledge	Global	AI/CS/IoT	V		
Next Generation IoT	EU	IoT	V	V	V
EPoSS Association	EU	IoT	V	V	V
IEEE Innovation at Work	Global	AI/CS/IoT	V		
IEEE RAS	Global	AI	V		
ACM	Global	AI/CS/IoT	V		
LIKTA	Regional (LV)	AI/CS/IoT	V		
ScienceDirect	Global	AI/CS/IoT	V	V	V



This activity has been performed by requesting each consortium member to discuss and feed a table of trusted data sources, and a list of query keywords to be used when performing the investigation.

The following list provides the of unique keywords for investigating data sources:

- Cybersecurity
- IoT
- Machine learning
- Artificial intelligence
- Deep learning
- Data analytics
- Big data
- Automation
- Digital currencies / blockchain
- Computer science theoretical background - algorithms, data structures
- Cloud computing
- Robotics
- AR/VR
- Programming languages (C/C++/ Python/Java/R)
- Data management
- Business intelligence
- Data Science
- Data Engineering
- ML Ops
- Data Ops

4) Analyse identified research papers, statistics, reports, and forecasts according to reported expertise.

Step 4 intermediate data

Three tables have been developed to provide the name, year, link, scope (Regional/EU/Global), and a short summary of identified data. To narrow the research, data must be recent (at least from 2020) and in line with Universities' needs.

In the context of **CS**, the MERIT consortium highlights the following works:

- ENISA highlights in [2] the **12 typical cybersecurity professional role profiles**: CHIEF INFORMATION SECURITY OFFICER (CISO), CYBER INCIDENT RESPONDER, CYBER LEGAL, POLICY & COMPLIANCE OFFICER, CYBER THREAT INTELLIGENCE SPECIALIST, CYBERSECURITY- ARCHITECT, AUDITOR, EDUCATOR, IMPLEMENTER, RESEARCHER, RISK MANAGER; DIGITAL FORENSICS INVESTIGATOR, PENETRATION TESTER; along with their identified alternative titles, missions, deliverables and tasks, skills, knowledge, competences.
- In ENISA provides in [3] the 5 recommendations to address the EU cybersecurity skills shortage and gap: increase enrolments and eventually graduates in cybersecurity programmes; support a unified approach across government and industry; increase collaborations between Member States; promote analysis of the cybersecurity market needs and trends; and



support the promotion of the CyberHEAD¹ project (and its further evolution). The report also provides:

- The skill provided by all participating EU cybersecurity programmes according to topics taught at bachelor, master and post-graduate levels.
- Recommendation to prepare graduates for the cybersecurity workplace: organizations internships, industrial educators and cybersecurity certification preparation.
- **Top 7 certifications:** ISO 27001, CEH, CISM, CCNA Security, CySA+, CISSP and CompTIA Security+.
- EU initiatives to address the cybersecurity skills shortage and gap in the EU (and those adopted by member states).
- Recommendations to increase enrolment in cybersecurity programmes, a unified approach to cybersecurity skills (e.g., ECSF), and to understand job market and trends, and collaborate at EU level.
- Questions for EU HEIs (to be listed in CyberHEAD); and those new that may be considered. Value of CyberHEAD for students HEI and member states. CyberHEAD reply from some member states.

The 7 certifications cover various aspects of cybersecurity. These include network construction, management, and security, digital forensics, risk management, and incident response. From defence to penetration testing techniques for detecting vulnerabilities and validating a system's security.

Two of the listed certifications (CySA+ and CEH) require 2 to 5 years of cybersecurity industry experience. In its absence, they offer certifications at the entry level that satisfy the prerequisite.

While CompTIA (CySA+) offers Security+, which is already mentioned in the ENISA report, EC-Council (CEH) offers the Cyber Security Essentials Series, a series of free courses that cover network defence, ethical hacking, and digital forensics.

The latest development of AI allows for improving the accuracy of threat detection (both active and proactive), accelerating incident investigations, and improving the automation in response. Typical applications are:

1. Advanced threat detection (network, endpoint, and identity)
2. Improving authentication
3. Vulnerability assessment and threat response

Both applications 1 and 3 require investigating and correlating intelligence, for instance, via a threat intelligence platform.

This directly links the skills and knowledge provided by ENISA with the Cyber Threat Intelligence Specialist role. A less direct link exists between the Cyber Incident Responder and the Cybersecurity Risk Manager role.

Application 2 requires knowledge of the specific authentication and AC mechanisms and the implementation of risk-oriented access control rules. It is also important to correctly model user behavior and detect anomalies. A partial link exists between the set of skills and knowledge provided by ENISA with the Cybersecurity Architect role. Further, AI helps mitigate Cybersecurity related issues, Threat detection, Intrusion detection and prevention, Vulnerability management, and Fraud detection.

¹ Additional details are reported in <https://www.enisa.europa.eu/topics/education/cyberhead>. To be included in CyberHEAD, a (bachelor/master) cybersecurity program needs to be recognized at EU/EFTA level and 40% of modules need to address cybersecurity.



To anticipate the needs of the CS market and train the next generation of experts in the field, the MERIT consortium selected the following sources:

- ENISA provides in [4] the challenges, opportunities, research needs and priorities in 4 key-structural trends²: **hyperconnected world**, **intelligent systems**, cybersecurity in life sciences (**biotechnology**), and **computational security**.
- The 2022 edition of the CLUSIT report provides a focus article [5] that highlights the need for the following CS figures: **Cyber Security Engineer**, **OT Security Expert** and the **Security Governance Specialist**. Other articles highlight the need to protect **Operational Technology** architectures and **critical infrastructures**. The 2023 edition [6] highlights (considering the most significant cyberattacks globally in the past 4 years) the need for **Continuous Vulnerability Management** (also via PenTest-as-a-Service), **security-by-design** and Secure Software Development LifeCycle (**SSDLC**), adopt **SOC** and SOC-alike solutions for applications with respect to each element (exposed services, front end, middleware, mobile applications, IoT); review of outsourced processes and third-parties. In addition, a focus highlights the applicability and advantages (current and future ones) of Zero Trust and Zero Trust Architectures; and eleven possible use cases (from IIoT to 6G).
- Gartner provides in [7] the set of technologies piloted and to be deployed in 2023 by 400 midsize enterprises (MSEs)³, together with the value for the enterprise and key takeaways; in [8] it predicts that 10% of large enterprises will have a mature and measurable **Zero-Trust** program in place by 2026; in [9] it lists three factors influencing growth in security spending: **Remote Work**, **ZTNA** and **Cloud-Based Delivery Models**; in [10] it provides a set of trends that highlight the use of Zero-Trust, **third-party assessment** and **OT**. Additional trends associated with privacy are provided by Gartner in [11]: cloud data localisation (with respect to different applicable regulations), privacy-enhancing computation (PEC) in analytics, business intelligence and/or cloud computing; risks of AI-based data processing or the Hybrid Everything paradigm (in contrast to data minimisation), centralized privacy user experience (to tailor preference and for consent management).

In the context of **AI**, the MERIT consortium highlights the following works:

- Caiming Zhang and Yang Lu highlight in [12] how Artificial Intelligence (AI) can significantly impact the following areas i) agriculture, ii) autonomous driving, iii) education, iv) financial industry, v) governance, vi) intelligent robotics, vii) manufacturing, viii) medical, ix) retailing industry, and x) security.
- The roles and skills are based on LinkedIn data and the Microsoft Learn Career Path [13] are classified as follows: i) AI engineer, ii) AI Data analyst, iii) AI Data engineer, iv) AI Data scientist, v) AI Developer, vi) Robotics Engineer, vii) Digital transformation experts and viii) Functional consultant.
- The following technical skills are based on LinkedIn data e.g., Machine Learning, Deep Learning, Natural Language Processing (NLP), Computer Vision, Reinforcement Learning, Data Science and Analytics, Robotics and Automation, AI Ethics and Responsible AI, Cloud Computing, and familiarity with cloud-based platforms, such as AWS, Azure, and Google Cloud AI Project Management, Big Data, and Machine Learning Operations (MLOps), are needed.
- Sonia Malik highlights in [14] the top 16 essential soft skills need (e.g., Critical Thinking, Creativity, Emotional Intelligence - EQ - and Empathy) to focus on acquiring and improving to thrive in the future world of work.

² Identified with stakeholders and members of the research community.

³ I.e., those with greater than \$50 million and less than \$1 billion in revenue.



- The *Expert Group on Future Skills Needs* reports in [15] the skills gap (based on LinkedIn data) of typical skills needed for roles in data and AI jobs, as indicated by the *World Economic Forum* in [16]. The report identifies the fundamental high-level technical skills needed by AI experts but also considers skills needed for the deployment, management and regulation of AI, as well as the supplementary AI knowledge needed in the public sector, by educators, and by the citizens.
- Forbes asserts in [17] that there is a prediction of 97 million new jobs involving AI, created between 2022 and 2025. Colleges and universities have responded to this by creating new courses and educational programs focusing on the skills needed. Some of the skills are briefly described: programming, data science, AIOps, statistics & probability, communication & visualization.
- According to Gartner [18] AI usage increased from 35% in 2019 to 52% in 2021, however, data complexity and accessibility, difficulty measuring AI success, and lack of skills of staff remain the top barriers to AI implementation. This report defines the core and emerging roles and skills for technical professionals in the ML/AI space. The roles include data scientist, citizen data scientist, ML engineer, ML architect, model owner and model validator. These roles are a combination of key and emerging roles. Each role is deeply described in terms of responsibility and required skills (both technical and non-technical).

In the context of **IoT**, the MERIT consortium highlights the following works:

- John Soldatos from *Netcompany-Intrasoft* highlights in [19] the **5 factors contributing to the IoT skills shortage**:
 - IoT as a computing paradigm that includes different technology solutions, such as embedded systems, cloud computing, ML and CS. Therefore, it requires roles with multiple skills (technical or not) from different technology areas.
 - Complexity of IoT projects, that require multi-disciplinary profiles and different skillsets that go far beyond the basics of IoT systems.
 - Following the pace of IoT technology acceleration (e.g., integrating edge intelligence, federated learning, and tactile internet).
 - Skills shortage in IoT-related technologies, such as ML, AI, and CS.
 - Skills required to collaborate across the different stakeholders of IoT projects.

The report provides **four categories of IoT skills**, together with their subcategories and pertaining technologies and topics; that represent important and prominent IoT skills.

1. IoT Technical and Technological Skills: skills related to IoT technologies, including those required to develop, deploy, and operate IoT systems. It aims at providing a broad coverage of the very rich set of technologies that are currently associated with IoT systems.
 - IoT devices: sensors, actuators, DSP (Digital Signal Processing), FPGAs (Field Programmable Gate Array), the GPS (Global Positioning System), PLC (Programmable Logic Controllers), WSN (Wireless Sensor Networks), ad-hoc networks, RFID (Radio Frequency Identification) devices and more.
 - Smart objects: more complex devices (e.g., Cyber-Physical Systems and UAVs).
 - Networks and Connectivity: the most popular networking protocols and connectivity technologies for IoT systems such as Wi-Fi, Bluetooth and Low Power Wide Area Network (LPWAN) technologies. It also comprises various mobile networking technologies like 4G, Long Term Evolution (LTE), 5G and 6G networking technologies.
 - IoT protocols: protocols such as MQTT, Constrained Application Protocol (CoAP) and Data Distribution Service (DDS).



- Cloud/Edge/Mobile Computing for the development, deployment, and operation of non-trivial IoT systems, such as systems that integrate data and services from multiple distributed IoT devices.
 - IoT Analytics: analysis of IoT data using various technologies and techniques such as ML, DL (Deep Learning) and AI. Ranging from big data analytics to embedded machine learning and TinyML.
 - IoT Security, including for example skills relating to security processes (e.g., risk assessment, pen testing) and to secure operations of various types of IoT devices.
 - IoT Software Programming Skills: skills include for example programming in popular languages like Python, Java and JavaScript, as well as in other specialized skills for the programming of IoT devices e.g., robotics programming and Arduino programming.
 - IoT Development Methodologies: mainstream development infrastructures and methodologies that are commonly used by developers and deployers of IoT systems. For example, Development and Operations (DevOps), Data Operations (DataOps) and Machine Learning Operations (MLOps) infrastructures.
 - IoT Development and Deployment Tools.
2. Management and Marketing (in the real, of IoT product and service development) and Regulatory Skills (e.g., GDPR and ethics).
- Business, Management and Marketing Skills: A rather broad category that comprises various business, management and marketing skills which pertain to IoT products and services.
 - Legal and Regulatory Skills: skills that are required for developing, deploying, and operating enterprise-scale IoT products/services with commercial relevance. Includes skills associated with IoT Ethics, GDPR and other IoT/AI related regulations.
3. IoT End-Users and Operator 4.0 skills; with emphasis on industrial sectors.
- Industrial Automation Skills. Includes, for example, skills associated with the use of legacy automation systems and technologies (e.g., PLC, Supervisory Control and Data Acquisition - SCADA), as well as with popular industrial processes like quality control and production scheduling. It also includes skills linked to emerging digital tools for industrial automation like digital simulation and digital twins.
 - Asset Management Skills: asset programming, intelligent asset management, equipment maintenance, predictive maintenance and more. The EU-IoT framework includes a special sub-category for these asset management skills.
 - Visualization: IIoT applications need to understand and use visualizations of IoT data in industrial contexts. This subcategory is devoted to visualization skills, such as big data visualization, AR, MR, VR, design of ergonomic user journeys and more.
4. Social and Soft Skills to develop, deploy, operate, and use of IoT systems (e.g., teamwork, lifelong learning, and collaboration).
- Thinking Skills, such as critical thinking, analytical thinking, and complex problem solving.
 - Social Skills, such as teamwork, interpersonal skills, and professional ethics.
 - Personal Skills, such as lifelong learning, time management, people management and emotional intelligence.

The report also provides the results of **four questionnaires** (according to identified categories) with 183 different respondents.



Finally, it lists **six examples of skill profiles and their learning paths** (using the Udemy and the EU-IoT training resources catalogues): IoT Application Developer, IoT Network Engineer, IoT Data Analytics Expert, Embedded Systems Engineer, IoT Project Manager, IoT Product Manager.

Table 4 presents a summary of current and forecasted topics/skills in the three domains from the beforementioned sources.

Table 3: current and forecasted topics/skills.

Cybersecurity	AI	IoT
Communicate, present and report to relevant stakeholders		
Collaborate with other team members and colleagues		
Identify and solve cybersecurity-related issues	Big Data	Cloud/Edge/Mobile Computing
Automation and programmability (ref. to Appendix A)	Algorithm, Modeling	DevOps/DataOps/MLOps
Cloud computing	Machine Learning (ML)	Sensors & Actuators
Cryptography	Reinforcement Learning (RL)	Networking
Incident Management	Deep Reinforcement Learning (DRL)	Microcontrollers
Security Governance (ref. to Appendix A)	Natural Language Processing (NLP)	Embedded Systems
Security Training and Awareness (ref. to Appendix A)	Computer vision	Containerisation Technologies
Malware Threats	Federate Learning (FL)	Data Science
Network Fundamentals	Few shoots and meta learning	Machine Learning
Phishing (ref. to Appendix A)	Hybrid learning (Reinforcement, supervised unsupervised, operational research domain)	Data Visualization
Physical security controls (ref. to Appendix A)	Machine learning operations (Mops)	Project Management
Security Planning and Risk Management	Large Language Model (LLM)	Agile Development
Privacy	Cloud Computing e.g. AWS, Azure and Google Cloud	IoT protocols
Cybersecurity-related laws, regulations or legislations; and their requirements	Neuro Symbolic Learning	IoT security
Auditing	Edge Computing	Legal and Regulatory
Security controls	Common AI frameworks include Theano, TensorFlow, Caffe, Keras, and PyTorch	Industrial Automation



MERIT Deliverable



Co-funded by
the European Union



Cybersecurity	AI	IoT
Risk management	SQL, NoSQL, Python, Java, R, and Scala	
Techniques, Tactics and Procedures (TTPs)	ETL (extract, transform, and load) systems	
Providers of cybersecurity best practices according to technologies (applicable in EU and/or US); how to apply them in the ISO/OSI stack.	Automation and scripting	
Continuous vulnerability management	Big data tools e.g., Hadoops, Spark, Kafka, Flink, Cassandra, Hive, HBAs, Nifi, etc., and commercial tools like MongoDB, Presto, Elasticsearch, Google and BigQuery.	
Security by-design and Secure-software development lifecycle (SSDLC)	Data storage, Data Lakes, Data Warehouses, Data Mesh, distributed file systems, etc.	
Zero-Trust / ZTNA	Data visualization tools such as D3.js, Tableau, Power BI, BI tools such as Domo and Tableau.	
Cloud-based delivery models		
Third-party assessment	Data science tools (Python scripting, NumPy, scipy, matplotlib, scikit-learn, Jupiter notebooks, bash scripting, Linux environment.)	
Operational Technology	Parallel programming, ideally CUDA	
Critical infrastructures	Explainable artificial intelligence (XAI), OpenAI, Pandas, Numpy, NLP models	
Cloud data localisation (with respect to different applicable regulations)	Context awareness in ML	
Privacy-enhancing computation (PEC) in analytics	Ethical AI, AI project management	
Business intelligence		
Risks of AI-based data processing or the Hybrid Everything paradigm		



Cybersecurity	AI	IoT
Centralized privacy user experience (to tailor preference and for consent management)		

- Request partner SMEs to highlight their needs and, together with DIHs, inquire regional market needs via questionnaire in their network.

Step 5 intermediate data

A preliminary investigation in collaboration with WP4 over eleven companies linked with the Consortium, from different countries and representing different industry domains, highlights the following five knowledge blocs or skills as supported (hence, their demand in the industry).

- Cybersecurity and Data analytics (both indicated by 9 companies).
- Artificial Intelligence (indicated by 8).
- Machine Learning / Deep learning and critical thinking (both indicated by 7).

To have a general overview over industry needs, we decided to reviewing the following: Frost&Sullivan reports ([20], [21], [22]), Gartner forecasts ([7], [9] and [10]) and CLUSIT reports ([5] [6]) in the context of CS; Frost&Sullivan reports ([23] and [24]) in the context of AI and IoT ([25] and [26]). The Frost&Sullivan documents have been gathered by querying its domain-specific databases (considering their large experience in market analysis). In future editions of D3.1, we plan to expand the pool of industry to inquiry local industry needs and trends (leveraging the network of the consortium Partners).

Table 5 provides the set of technologies derived from this more general perspective, and if they pertain to specific contexts or relate to multiple areas (AI, CS or IoT). The reference for each technology is provided in line or in the context column (when the set of technologies are all extracted from that reference).

Table 4: technologies associated with current and future industry needs.

Technologies	Context	CS	AI	IoT
Human-computer-Interaction [4]	Any	X		X
New generations of mobile communications and data collection or processing methods (evolution from 5G to 6G) [4]		X		X
Symmetric key schemes at higher security levels [4]		X		
Post Quantum cryptographic systems; standards for new quantum resilient safe algorithms and protocols [4]		X		
Monitoring large-scale and possibly interconnected systems [4]		X		X
Biomimetic cybersecurity algorithms [4]		X		
Context awareness in machine learning (ML) to boost resiliency [4]		X	X	
Cyberbiosecurity [4]		X		
Privilege separation and least-privileged access, as well as using privileged access workstations (PAWs) for managing identity systems [6]		X		



Technologies	Context	CS	AI	IoT	
Multi-Factor-Authentication (MFA) and Conditional Access Control [6]		X	X		
Justin-Time (JIT) access and Just-Enough Access (JEA) administrator access [6]		X			
Extensive detection and response (XDR) -6 capabilities and modern cloud-native tools that use machine learning to separate noise from signals [6]		X	X		
Zero Trust principles [5] (Zero Trust Network Access - ZTNA) [7]		X		X	
Security controls and procedures in DevOps and application lifecycle processes [6]		X		X	
Security Orchestration Automation and Response (SOAR) [7]		X		X	
Endpoint Detection and Response (EDR) [7]		X			
Cloud Access Security Broker (CASBs) [7]		X		X	
Managed Detection & Response (MDR) [7]		X			
Network Detection and Response (NDR) [7]		X			
Distributed Cloud Systems [7]		X			
Hybrid Cloud Storage [7]		X			
Citizen Integrator Tools [7]		X			
NLP [7]		X			
Secure Access Service Edge (SASE) [7]		X		X	
Identity-based segmentation, SD-WAN and Network Traffic Analysis [7]		X			
AI cloud services and AIOps [7]		X		X	
Identity-based segmentation, SD-WAN and Network Traffic Analysis [7]		X		X	
API management PaaS [7]		X			
OS vulnerabilities [7]		X			
Ransomware (prevention) [7]		X		X	
Phishing (prevention) [7]		X		X	
SOC as a Service [7]		X		X	
Security information and Event Management (SIEM) [7]		X		X	
Identity-based security technologies [7]		X		X	
Smart mobile app: management of waste accounts, services and billing on the go		Waste recycling and circular economy [22]	X		
Detection of waste volumes or intelligent object recognition				X	X
Software to optimize routes, time and costs, to reduce emissions				X	X
Cloud-based remote services (and 5G networks)	X			X	



Technologies	Context	CS	AI	IoT
Decision Intelligence			X	
Asset health monitoring and management: real-time visualization of multiple data inputs		X	X	X
AI recycling robots: intelligent automated sorting			X	X
Digital Twin		X		X
SaaS business model		X	X	X
Predictive analytics: continual demand management and conservation	Waste recycling and circular economy [22] . AI [14]	X	X	X
Blockchain	Airport security technologies/mechanisms [21]. Waste recycling and circular economy [22]	X		
Disruption management	Airport security technologies/mechanisms [21]	X	X	
Operation Control Centre (OCC)		X	X	
Self-service technologies		X	X	X
Biometric verification, touchless ID, and Access Control		X	X	
User behavioural tracking		X	X	
Proactive threat detection		X	X	
Automated incident response protocols		X	X	
Automation of preventive measures, and encrypting personal and sensitive data		X	X	
Sensors (Lidar, Radar, image sensors)	IoT automotive [25]			X
Communication networks (V2V, V2X, V2I) and technologies (Bluetooth, Wi-Fi, RFID, UWB/Zigbee, WSNs, 4G LTE/5G, Lora, NB-IoT)		X		X
IoV Cloud Technologies				X
Machine learning			X	X
Data analytics			X	X
Object detection				X
Image processing algorithms			X	X
Multi-parameter sensing			X	X
Real-time data Management				X
Efficient communication between machine-machine and human-machine				X
Auto-steer and manoeuvrability			X	X
Error detection		X	X	X
Predictive maintenance			X	X
Remote monitoring and operability				X

Technologies	Context	CS	AI	IoT
Prediction of traffic conditions	IoT - Blockchain [26]		X	X
Limitations of resource-constrained devices				X
Securing large volumes of IoT devices		X		X
Blockchain-based solutions for IoT Device Identity				X
Communication & Reputation Management				X
Economy of Things and Data Brokerage				X
IoT Supply Chain Integrity Assurance		X		X
On-demand Asset Sharing Services				X
Secure & Autonomous Communication		X	X	X
5G-enabled Blockchain Services				X
Cybersecurity Assurance Services				X
Economy of Things				X
Blockchains for Secure IoT Firmware Updates		X		X
Compliance Verification of IoT Device Models		X		X
Cybersecurity through Monitoring of Device Traffic Patterns		X		X
Data management via databases (relational/not, Big Data repositories and processing engines)	AI [14]	X	X	
Data mining			X	

- 6) Generate a summary of required AI, CS and IoT technologies and skills/topics by considering both the state-of-the-art data (Step 4) and industrial needs (Step 5).

Step 6 intermediate data

Table 6 provides the topics and skills from Table 4, with at least one pertaining technology among Table 5 ones.

Table 5: topics and skills with pertaining technologies.

Topics/Skills	# of related technologies
Automation and programmability (ref. to Appendix A)	30
Network/ Network Fundamentals	22
Cybersecurity-related laws, regulations, or legislations; and their requirements	16
Physical security controls (ref. to Appendix A)	12
Security controls	12
Risk management	10
Cloud computing	8
Continuous vulnerability management	8
IoT security	5
Auditing	5



MERIT Deliverable



Co-funded by
the European Union



Topics/Skills	# of related technologies
Malware Threats	5
Incident Management	5
Cloud/Edge/Mobile Computing	4
Cloud-based delivery models	4
Operational Technology	4
Sensors & Actuators	3
Industrial Automation	3
risks of AI-based data processing or the Hybrid Everything paradigm	2
Big Data	3
Embedded Systems	2
IoT protocols	2
Identify and solve cybersecurity-related issues	2
Security by-design and Secure-software development lifecycle (SSDLC)	2
Security Training and Awareness (ref. to Appendix A)	2
Techniques, Tactics and Procedures (TTPs)	2
Big data tools (popular ones include Hadoop, MongoDB, and Kafka.)	1
Data storage	1
Data science tools (Python scripting, NumPy, scipy, matplotlib, scikit-learn, Jupyter notebooks, bash scripting, Linux environment.)	1
Data Visualization	1
business intelligence	1
Cloud data localisation (with respect to different applicable regulations)	1
Collaborate with other team members and colleagues	1
Communicate, present and report to relevant stakeholders	1
Cryptography	1
Centralized privacy user experience (to tailor preference, manage consent)	1
Phishing (ref. to Appendix A)	1
Security Governance (ref. to Appendix A)	1
Security Planning and Risk Management	1
SoC / SoC-alike solutions	1
Zero-Trust / ZTNA	1

- 7) Use the set of skills highlighted by consortium Universities to prioritize the set of topics that will be considered when creating/updating the MERIT programme.

Step 7 intermediate data

By merging the Table 6 topics/skills with the set of mandatory skills highlighted by the consortium Universities, the current topics/technologies that should be prioritised in the MERIT programme are:

- Automation and programmability.



- Network / Network fundamentals.
- Cybersecurity-related laws, regulations, or legislations; and their requirements.
- Physical security controls.
- Risk management.
- Cloud computing.
- Continuous vulnerability management.
- IoT security.
- Auditing.
- Identify and solve cybersecurity-related issues.
- Incident management.
- Security training and awareness.
- Collaborate with other team members and colleagues.
- Communicate, present and report to relevant stakeholders.
- Risk of AI-based data processing or the Hybrid Everything paradigm.
- Zero-Trust / ZTNA.
- Containerisation Technologies.
- Security by-design and Secure-software development lifecycle (SSDLC).
- Techniques, Tactics and Procedures (TTPs).
- Big data and Big data tools.
- Data storage, elaboration (data science tools), and visualisation.
- Operational Technology.

This list considers Table 6 topics with at least 5 pertaining technologies and additional topics deemed a priority according to the research/industry experience developed by the research and excellence centre.

To understand how the results of the methodology fit in the European skills and labour market, we assessed their adherence to the European Skills, Competences, Qualifications and Occupations (ESCO) [27] classification, and to the European e-Competence Framework (e-CF) [28].

To map which Skills, Knowledge and Occupations from ESCO the results relate to, we deployed and queried the ESCO database via the local API⁴. When using the 22 keywords from Step 7 with the *Full text search* API, we obtained 4560 results (3097 unique), which could be a *Concept*, a *Skill* or a *Knowledge* item in the ESCO classification, and it may be associated with zero or more occupations. We initially reviewed them to exclude those out of context and obtained a list of 1271 results. We then developed a script⁵ to:

- Query the ESCO database for each of the 1271 results (always using the *Full text search*).
- Fetch the related “essential for” occupations (if listed) and the ESCO identification code (if available); otherwise, fetch the parent in the hierarchy⁶ of the ESCO classification and its type (*Knowledge*, *Skill* or *Concept*).
 - In case of Transversal Knowledge items, duplicate parents (e.g., for cross-related knowledge), or if the result is classified as “obsolete” by ESCO, we manually queried

⁴ <https://esco.ec.europa.eu/en/use-esco/use-esco-services-api/esco-local-api>.

⁵ Available at https://digitalmerit.eu/wp-content/uploads/2024/07/MERIT_ESCO_code.zip.

⁶ For instance, the ESCO “Cloud technologies” item is listed as essential for 10 occupations and the parent in the hierarchy is “database and network design and administration”, which has a *Knowledge* code K0612. Ref. to <http://data.europa.eu/esco/skill/bd14968e-e409-45af-b362-3495ed7b10e0> for further details.



the online database to identify the parent or the alternative labels (to be queried and used in place of the original one⁷).

- Classify the results as being in the AI, CS and IoT domains.

The results of this mapping⁸ are 430 low-level items:

- 233 unique skills, 105 associated with the CS domain, 56 with AI, and 99 with IoT.
- 159 unique knowledge items, 60 in the CS domain, 70 in AI, and 40 in IoT.

To have a more general view of the set of skills and knowledge items associated with results, we can consider the parent items in the ESCO classification hierarchy (i.e., only the items holding a *Skill* or a *Knowledge* identification code). This provides:

- 71 unique skills, 21 associated with the CS domain, 45 to both AI and IoT ones.
- 33 unique knowledge items, 27 in the CS domain, 14 in both AI and IoT ones.

According to the ESCO classification, the knowledge of the topics, technologies and skills listed as Step 7 results would enable MERIT students to access more than 1200 possible occupations (771 related to the CS domain, 501 and 572 the AI and IoT ones - respectively).

It is worth highlighting that several ESCO results were linked to occupations across multiple domains, indicating the interdisciplinary nature of modern technological roles. Additionally, approximately 10% of keywords needed manual lookup, highlighting areas where automated systems can be improved.

Considering the e-CF framework, we manually mapped which framework roles can be associated with Step 7 skills, knowledge and technologies. We initially verified at which skill level (among the five available skill groups) we could map Step 7 results.

- Automation and programmability: B.1 (L1 to L3).
- Network / Network fundamentals: B.2 (L2, L3), B.6 (L3, L4).
- Cybersecurity-related laws, regulations, or legislations; and their requirements: D.1 (L4, L5), E.8 (L4).
- Risk management: A.1 (L4, L5), A.3 (L4, L5), D.1 (L4, L5), E3 (L2 to L4).
- Cloud computing: B.6 (L3, L4)
- Continuous vulnerability management: C.4 (L2 to L4).
- IoT security: B.6 (L3, L4).
- Auditing: E.3 (L3).
- Identify and solve cybersecurity-related issues: C.4 (L2 to L4), E.8 (L3).
- Incident management: C.4 (L2 to L4), E.8 (L2, L3).
- Security training and awareness: (D.3 L2, L3).
- Collaborate with other team members and colleagues: E.4 (L3, L4).
- Communicate, present and report to relevant stakeholders: A.3 (L4, L5), D.6 (L2 to L4), E.4 (L3, L4).
- Security by-design and Secure-software development lifecycle (SSDLC): B.1 (L1 to L3).
- Big data and Big data tools: D.7 (L2 to L5).
- Data storage, elaboration (data science tools), and visualisation: D.7 (L2 to L5).

⁷ E.g., we used “conduct web searches” in place of “search for information online”, indicated as obsolete.

⁸ Available at <https://digitalmerit.eu/wp-content/uploads/2024/07/ESCO-Mapping.zip>. Appendix C provides a synthesis of the algorithm.



- Operational Technology: B.6 (L3, L4).
- Zero-Trust / ZTNA: D.1 (L4, L5), E.8 (L2 to L4).

Those allow the partial coverage⁹ of the following e-CF roles:

- database administrator.
- developer.
- expert devops.
- digital media specialist.
- network specialist.
- systems administrator.
- systems architect.
- test specialist.
- scrum master.
- systems analyst.
- service manager.
- service support.
- technical specialist.
- information security manager.
- information security specialist.
- account manager.
- ict operations manager.
- project manager.
- quality assurance manager.
- data specialist.
- enterprise architect.
- business analyst.
- business information manager.
- chief information officer.
- digital transformation leader.

Unlike with the ESCO framework, not all concepts have a clear mapping. In particular, we did not find a direct correspondence for the following results:

- Physical security controls.
- Risk of AI-based data processing or the Hybrid Everything paradigm.
- Containerisation Technologies.
- Techniques, Tactics and Procedures (TTPs).

⁹ For instance, to cover all competences of the *database administrator* role, Step 7 results must have included also a map to B.2 (Component Integration) and D.10 (Information and Knowledge Management).



3 Findings

The following sections provide the main findings extracted from the documents reviewed as part of the methodology presented in Section 2 (Step 4), or the analysis of related topics/skills. Section 3.1 also introduces the domain-specific working positions that require both CS and AI expertise and the necessary skillset; similarly, Section 3.2 for IoT positions. Section 3.4 is finally dedicated to the industry needs extracted from reviewed documents. Additional findings are provided in Appendix A and Appendix B.

3.1 CS Findings

Following the ENISA report on the *Skills Framework Role Profiles* ([2]), the **Top 3 skills** needed by at least 3 of the 12 cybersecurity profiles are:

1. Communicate, present and report to relevant stakeholders (8 profiles).
2. Collaborate with other team members and colleagues (4 profiles).
3. Identify and solve cybersecurity-related issues (4 profiles).

The full list of needed skills can be found in Appendix A.

The **Top 13 topics** needed by at least 3 of the 12 cybersecurity profiles are:

1. Cybersecurity-related certifications (9 profiles).
2. Cybersecurity controls and solutions (6 profiles).
3. Cybersecurity standards, methodologies, and frameworks (6 profiles).
4. Computer networks security (5 profiles).
5. Cyber threats (5 profiles).
6. Cybersecurity recommendations and best practices (5 profiles).
7. Cybersecurity related laws, regulations and legislations (5 profiles).
8. Operating systems security (5 profiles).
9. Computer systems vulnerabilities (4 profiles).
10. Cybersecurity attack procedures (4 profiles).
11. Computer programming (3 profiles).
12. Cybersecurity-related technologies (3 profiles).
13. Legal, regulatory and legislative compliance requirements, recommendations and best (3 profiles).

In line with the first topic, the MERIT consortium investigated the knowledge modules required to apply for the Top 7 CS certifications reported by ENISA in [3]: ISO 27001, CEH, CISM, CCNA Security, CySA+, CISSP and CompTIA Security+ and the *Cyber Security Essentials Series* recommended as a CEH prerequisite.

The **Top 11 topics** covered by at least 4 of the 8 analysed certifications are:

1. Automation and programmability (4 certifications).
2. Cloud computing (6 certifications).
3. Cryptography (4 certifications).
4. Incident Management (6 certifications).
5. Security Governance (4 certifications).
6. Security Training and Awareness (5 certifications).
7. Malware Threats (4 certifications).
8. Network Fundamentals (4 certifications).
9. Phishing (5 certifications).
10. Physical security controls (4 certifications).
11. Security Planning and Risk Management (6 certifications).



The list of covered topics can be found in Appendix B.

The ENISA report [2] introduces the topic of "Cybersecurity controls and solutions". According to the European Cybersecurity Skills Framework (ECSF)¹⁰, the cybersecurity controls are covered by the profiles listed in Table 7. The security checks and their mention within the various certifications can be seen in Table 8.

Table 6: cybersecurity controls and relative profiles.

Role	Key knowledge	Notes
Chief Information Security Officer (CISO)	No	-
Cyber Incident Responder	No	Evaluate the resilience of the cybersecurity controls and mitigations actions taken after a cybersecurity or data breach incident
Cyber Legal, Policy & Compliance Officer	No	-
Cyber Threat Intelligence Specialist	Yes	-
Cybersecurity Architect	Yes	Monitoring, testing, and evaluating cybersecurity controls' effectiveness
Cybersecurity Educator	Yes	-
Cybersecurity Implementer	Yes	Implementing, monitoring and performance evaluation of the cybersecurity controls
Cybersecurity Researcher	No	Decompose and analyse systems to identify weaknesses and ineffective controls
Cybersecurity Risk Manager	Yes	Monitoring, testing and evaluating cybersecurity controls' effectiveness
Digital Forensics Investigator	No	-
Penetration Tester	No	Assess the effectiveness of security controls

Table 7: cybersecurity controls mapping.

	Physical	Digital	Security	Cloud	Testing/evaluation
ISO 27001			x		
EC-Essential	x		x		
CEH			x	x	
CISM					x
CCNA	x				
CySA+	x	x	x		
CISSP	x	x			x
Security+			x	x	

¹⁰ A tool to support the identification and articulation of tasks, competences, skills and knowledge associated with the roles of European cybersecurity professionals.



The same document also introduces the topic of "Cybersecurity standards, methodologies and frameworks", whose knowledge is required by 6 profiles. R3.5.1 of the REWIRE project lists the following topics (referring to each of them as standards, methodologies, and frameworks):

- Cybersecurity and privacy.
- Legal (frameworks for cybersecurity and data protection).
- Auditing.
- Security controls.
- Risk management.
- TTP (Tactics, Techniques and Procedures).

Students need to be acknowledged in current standards, methodologies, and frameworks. As each topic is covered by many different documents created by multiple agencies, we only report some of the available providers:

- EU-based
 - European Union.
 - ENISA.
 - ISO.
 - Regional cybersecurity agencies (e.g., German BSI, Italian AgID, French ANSSI).
- US-based
 - NIST.
 - ISACA.
 - Center for Internet Security.
 - HITRUST Alliance.

AI in Cyber Security

AI applied to Cybersecurity allows for improving the accuracy of threat detection (both active and proactive), accelerating incident investigations, and improving the automation in response. Common applications are:

1. Advanced threat detection (network, endpoint and identity)
 - a. Improve anti-phishing mechanisms and cybersecurity awareness with NLP to counter social engineering attacks, such as those that adopt AI-generated voice fakes and deep fakes.
 - b. Provide behavioural analytics.
2. Improving authentication
 - a. Dynamically evaluate the risk of authenticated users (e.g., as employed by Microsoft and IBM¹¹).
 - b. Support biometric authentication.
3. Vulnerability assessment and threat response
 - a. Analyse real-time data and prioritize vulnerabilities based on the risk score/level.

Roles of AI to mitigate Cybersecurity related issues.

The intersection between AI and CS expertise is particularly evident in the following activities:

1. Threat detection:
 - a. AI models can automatically recognize patterns in network traffic, emails, and other data that may indicate a security threat.

¹¹ As reported by Microsoft in <https://learn.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa> and IBM in https://www.ibm.com/docs/en/SS42VS_SHR/com.ibm.UBAapp.doc/c_Qapps_UBA_intro.html.



- b. They can also be used to identify malware and other malicious activities automatically.
2. Intrusion detection and prevention:
 - a. It's helpful for detection intrusions in real time and block or mitigate them automatically.
 - b. This helps prevent security breaches and minimize the damage they cause.
3. Anomaly detection:
 - a. Its help full to identify anomalies in data that might indicate a security threat, such as unusual user behaviour or a spike in network traffic.
4. Vulnerability management:
 - a. AI helpful in the process of identifying and fixing vulnerabilities in software and systems, reducing the risk of exploitation by malicious actors.
5. Fraud detection:
 - a. To identify fraudulent activities, such as phishing attacks, credit card fraud, and other types of financial scams.

Considering the CS roles presented by ENISA in [2], a link can be found between the *Cyber Threat Intelligence Specialist working position* and the *Threat detection* activity described above; hence, its set of skills and required knowledge. Similarly, the rest of the listed activities can be considered part of the *Cyber Incident Responder* role tasks.

3.2 IoT Findings

The following IoT skills profile identified by John Soldatos in [19], together with the learning path (a set of courses from the EU-IoT training catalogue and the Udemy training ecosystem), the additional courses (EU-IoT and Udemy, but also other ecosystems – such as courser, IBM and edX) and the application areas described in the *Strategic Research and Innovation Agenda 2023* [29] are:

1. IoT Application Developer.
 - a. Skills: Python, JavaScript, IoT & Cloud Computing, DevOps, Docker, Kubernetes, Sensors, WSN, Arduino, MQTT.
 - b. Learning path: Practical IoT Concepts-Devices, IoT Protocols & Servers DevOps; Introduction to IoT Programming with JavaScript; Exploring AWS IoT; Project - 2022: CI/CD with Jenkins Ansible Kubernetes; Arduino for Beginners - 2022 Complete Course.
 - c. Other relevant courses: Collaboration and Emotional Intelligence; I.T. Project Management for Beginners: A Step-by-Step Guide.
2. IoT Network Engineer.
 - a. Skills: Sensors & IoT Devices, LPWAN, 4G/5G/6G, Wi-Fi, Bluetooth, MQTT.
 - b. Learning path: Internet of Things (IoT) - Demystified using 3 IOT devices; 5G Masterclass: Architecture, NR RAN, Core and Call flows; The Ultimate WLAN and Wi-Fi Training Course; The Complete Bluetooth / IoT Design Course for iOS.
 - c. Other relevant courses: Collaboration and Emotional Intelligence; I.T. Project Management for Beginners: A Step-by-Step Guide.
3. IoT Data Analytics Expert.
 - a. Skills: Data Science, Machine Learning, TinyML, Sensors, WSN.
 - b. Learning path: Master Machine Learning and Data Science with Python; Intro to Embedded Machine; Sensors/Actuators/Data Visualization with Microcontrollers - IoT Dashboard with Arduino.
 - c. Other relevant courses: Statistics for Data Science and Business Analysis; Collaboration and Emotional Intelligence.
4. Embedded Systems Engineer.



- a. Skills: Embedded Systems, FPGA, Printed Circuit Board (PCB) Design, Sensors, Actuators, WSN.
 - b. Learning path: Mastering Microcontroller and Embedded Driver; Learn the Fundamentals of VHDL and FPGA Development; Sensors/Actuators/Data Visualization with Microcontrollers - IoT Dashboard with Arduino; Crash Course Electronics and PCB Design.
 - c. Other relevant courses: Arduino: Electronics circuit, PCB Design & IOT Programming; Collaboration and Emotional Intelligence.
5. IoT Project Manager.
- a. Skills: Data Science, Machine Learning, TinyML, Sensors, WSN.
 - b. Learning path: Master Machine Learning and Data Science with Python; Intro to Embedded Machine; Sensors/Actuators/Data Visualization with Microcontrollers - IoT Dashboard with Arduino.
 - c. Other relevant courses: Statistics for Data Science and Business Analysis; Collaboration and Emotional Intelligence.
6. IoT Product Manager.
- a. Skills: Product Management, Sensors, WSN, Cyber-Physical Systems.
 - b. Learning path: Agile PM 301 - Mastering Agile Project Management; Great Product Manager: Product Management by a Big Tech's PM; Complete Guide to Build IOT Things from Scratch to Market; Sensors/Actuators/Data Visualization with Microcontrollers - IoT Dashboard with Arduino.
 - c. Other relevant courses: Presentation Skills: Master Confident Presentations; Management Skills - Team Leadership Skills Masterclass 2022; Advanced Product Management: Vision, Strategy & Metrics.
7. IoT Hardware engineer.
- a. Service Architectures and Platforms for IoT: embedded systems, sensor networks, electronics.
 - b. Hardware: microcontrollers, System-on-a-Chip (SoC), I/O devices (sensors and actuators).
 - c. Programming Languages: C/C++, Python, Bash scripting, Assembler.
 - d. Communications Protocols: application protocols (e.g., AMQP, CoAP, DDS), hardware protocols (such as I2C, Serial).
 - e. Networks and Communications: Wi-Fi, NFC, Bluetooth, Low Power Networks, Power Line Communication (PLC).
 - f. Code management: source code management, Workflow Automation; collaboration and teamwork.
 - g. Collaboration and teamwork: analytical and Critical thinking abilities, communication skills, work and collaborate well with others.
8. IoT Communication engineer
- a. Service Architectures and Platforms for IoT: reference architectures for IoT, Cloud and Edge IoT Platforms, Distributed Systems, mobile applications, sensor networks.
 - b. Programming Languages: Python, Ruby, Java, Kotlin, Bash scripting, JavaScript, C/C++.
 - c. Communications Protocols: application protocols (Advanced Message Queuing Protocol (AMQP), Constrained Application Protocol (CoAP), Data Distribution Service (DDS), Message Queue Telemetry Transport (MQTT).
 - d. Cloud Technology: cloud environments (AWS, Azure, OpenStack).
 - e. Networks and Communications: cellular networks (2G-5G), Wi-Fi, NFC, Bluetooth, Bluetooth Low Energy (BLE), Low Power Networks (LoraWan, NBIoT), Zigbee, Z-Wave, 6LowPAN, Sigfox, Neul, Power Line Communication (PLC).



- f. Code management: source Code Management, Workflow Automation, Continuous Testing, Continuous Monitoring; collaboration and teamwork.
- g. Collaboration and teamwork: analytical and Critical thinking abilities, Communication skills.

Roles of AI to enable the IoT in Industrial Data Space (IDS) ecosystem.

1. Predictive Maintenance, to analyse sensor data from IoT devices to predict when Maintenance is required and suggest future actions to minimize downtime.
2. Predictive Analytics, to analyse data from IoT devices to predict future trends, such as demand for products or services, and to optimize decision-making processes.
3. Smart Home Automation, to be used to control and automate various devices in a smart home, such as lights, thermostats, and security systems, based on data collected from sensors and user behaviour patterns.
4. Intelligent Transportation, to be used in the transportation industry to optimize routes, reduce fuel consumption, and improve safety. To be used to analyse data from vehicle sensors to predict traffic patterns and suggest the most efficient way.
5. Industrial IoT, to be used in industrial settings to improve efficiency, reduce downtime, and increase safety. For example, AI algorithms can analyse data from sensors in manufacturing plants to identify potential problems and optimize production processes.
6. Healthcare IoT, to be used in healthcare to monitor patients, predict potential health problems, and improve patient outcomes. For example, AI algorithms can be used to analyse data from wearable devices to track vital signs and predict potential health issues.
7. Agricultural IoT, to be used in agriculture to help farmers reduce waste and enhance productivity ensuring high yields, profitability, and protection of the environment.

3.3 AI Findings

According to Gartner AI usage increased from 35% in 2019 to 52% in 2021 [18], and Forbes [17] asserts that there is a prediction of 97 million new jobs involving AI, created between 2022 and 2025. However, data complexity and accessibility, difficulty measuring AI success, and lack of skills of staff remain the top barriers to AI implementation. In line with this, the *Expert Group on Future Skills Needs* lists nine perceived barriers [15] to the adoption of new technologies among which the top three barriers involve skills gaps:

- Skills gaps in the local labour market.
- Inability to attract specialized talent.
- Skills gaps among organization's leadership.

According to the World Economic Forum Future report ([16]), that ranks the skills gap¹² (estimated on LinkedIn data) among the typical skills needed for roles in data and AI jobs, artificial Intelligence and related skills were found to have the largest skills gap among the sixteen skills listed (as reported in Table 9).

Table 8: skill gaps for skills needed for Data & AI jobs; 1 indicates full gap, 0 no gap. From [16].

Skill Gaps for Skills Needed for Data & AI Jobs	
Skills needed for Data & AI Jobs	Skill Gap
Artificial Intelligence	0.9
Natural Language Processing	0.89
Signal Processing	0.85

¹² I.e., the level of training and learning required between the previous and new role.



Skill Gaps for Skills Needed for Data & AI Jobs	
Data Science	0.81
Cloud Computing	0.73
Data Storage Technologies	0.59
Scientific Computing	0.59
Development Tools	0.27
Computer Networking	0.22
Management Consulting	0.15
Information Management	0.07

Hence, analysing the job market needs, Marr Bernard proposes in [17] the most valuable skills allowing to work with the automated, intelligent machines of the future:

- Programming
- Data science
- AIOps
- Statistics and probability
- Communication and visualization skills

In addition, Gartner tries to define in [18] the core roles (**data scientist, ML engineer, ML architect**) and emerging ones (**citizen data scientist, model owner, model validator**) for technical professions in AI. A survey was undertaken as part of the research. The survey had four sections, targeted at different groups likely to be affected by AI: users and innovators; educators; citizens; policy makers, legislators, and regulators. Results for the first three groups are given in the Figure 2.

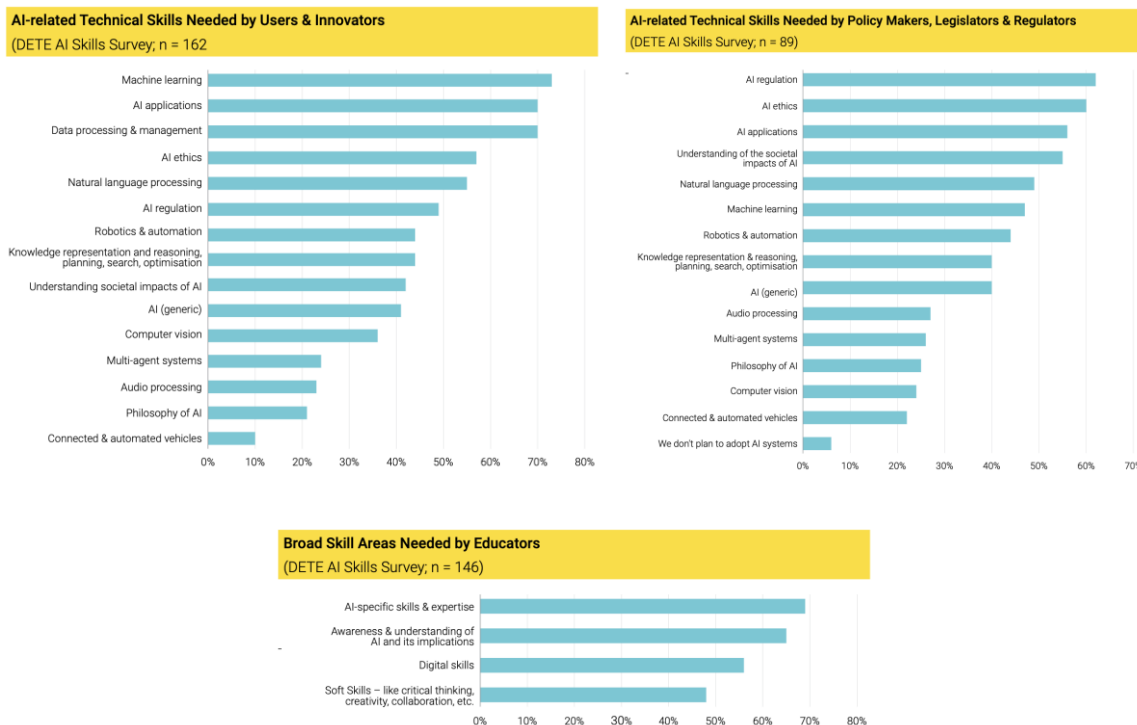


Figure 2: technical skills needed by three of the four target groups in the study - from [18].



The following Artificial Intelligence skills profile identified together with the learning path (a set of courses from training Microsoft learning paths and the Udemy training ecosystem) and additional courses (Udemy, but also other ecosystems – such as courser, IBM and edX) are:

Roles of AI in big data ecosystem.

1. AI engineer

a. Technical Skills:

- i. Programming language: (Python, R, Java, and C++), for designing and implementing models.
- ii. Big data Technologies: AI engineers Work with large amounts of data, so they are required to know Apache Spark, Hadoop, and MongoDB to manage it all.
- iii. Algorithms and Frameworks: Understanding of machine learning algorithms such as linear regression and Naive Bayes, as well as deep learning algorithms such as recurrent neural networks and generative adversarial networks, Reinforcement Learning (e.g., DQN, DDQN, POP) and being able to implement them with a framework.
- iv. AI frameworks: Theano, TensorFlow, Caffe, Keras, and PyTorch.
- v. Mathematics: linear algebra, probability, and statistics help to implement AI and machine learning models.

b. Soft Skills: collaboration and teamwork skills, Analytical abilities, Business knowledge and insight, Communication skills, Critical thinking abilities.

c. Learning Paths: boot camps, online courses, Bachelor, and master's degrees [30] [31].

2. Data analyst

a. Technical Skills: SQL, Statistics, Machine Learning, Data visualization.

b. Soft skills: critical thinking, effective communication, presentation skills, networking, and teamwork skills.

3. Data engineer

a. Technical Skills:

- i. Coding: languages including SQL, NoSQL, Python, Java, R, and Scala.
- ii. Relational and non-relational databases: databases rank among the most common solutions for data storage; familiarity with both relational and non-relational databases is essential.
- iii. ETL (extract, transform, and load) systems: common ETL tools include Xplenty, Stitch, Alooma, and Talend (ETL is the process by which you'll move data from databases and other sources into a single repository, like a data warehouse).
- iv. Data storage: as a designer of data solutions, knowledge of a data lake versus a data warehouse is an essential part of the job.
- v. Automation and scripting: automation is a necessary part of big data. Knowledge of writing scripts to automate repetitive tasks is compulsory.
- vi. Big data tools: tools and technologies are evolving and vary by company, but some popular ones include Hadoop, MongoDB, and Kafka.
- vii. Cloud computing: AWS, Azure, and Google Cloud is important for deploying, managing, and scaling AI solutions.

4. Data scientist

a. Technical Skills:



- i. Mathematics and Algorithmic: theoretical and practical knowledge of statistical analysis, statistical models, SPSS, business intelligence, cloud-based infrastructure, machine learning, predictive modelling, and optimization techniques. Algorithm design and complexity analysis, data mining, data warehousing or predictive modelling Solid command of probability (distributions, LLN, CLT, etc.).
- ii. Machine Learning Framework: experience with a major deep learning framework (PyTorch, TensorFlow, MXNet, etc.). Fundamentals of deep learning (layer details, back-propagation, etc.)
- iii. Language: python, R, Julia, or SAS, Kotlin, Tableau, Scala, Go or C++, Kaggle, BigQuery, Python, modern data platforms (Hadoop, Hive, Sqoop, HDFS)
- iv. Cloud Environment: AWS, Azure, OpenStack; software development and cloud platforms (e.g., AWS, GCP, Azure) debugging/profiling, “Google Looker”
- v. Databases, data sets, data science tools and data visualization: databases such as SQL or MongoDB, Spark and Hadoop, Excel, large-scale data sets, time series; data visualization tools such as D3.js, Tableau; Power BI, BI tools such as Domo, Tableau and visualizations for different audiences.
- vi. Data science tools: Python scripting, NumPy, scipy, matplotlib, scikit-learn, Jupiter notebooks, bash scripting, Linux environment.
- vii. Communication and Problem-solving skills:
 1. Communication skills: Excellent verbal and written communication skills and the ability to present technical data and approaches to both technical and non-technical audiences.
 2. Problem-solving and formulation skills: Understanding the unstructured problem, identifying specific research questions, and proposing data and model-driven solutions to create value for end-users and stakeholders.

5. AI Developer

- a. Technical Skills:
 - i. Language: C/C++, Parallel programming, ideally CUDA C/C++, software design, Python and Java.
 - ii. Mathematics and Algorithmic skills: Knowledge of vectors, matrices, and linear algebra Strong statistical and mathematical optimization linear/nonlinear integer programming.
 - iii. Machine learning and libraries Machine learning AI, Explainable artificial intelligence (XAI), OpenAI, Pandas, Numpy, NLP models.
 - iv. Cloud Technology AWS Serverless, Lambda, DynamoDB, API Gateway, Micro-service Architecture, Lex.
- b. Soft skills:
 - i. Problem solving skills, communication, and teamwork skills: excellent problem-solving ability, great team communication skills, passion for self-learning, and strong investigative; the ability to work collaboratively with partners, clients, and teams across multiple disciplines.
- c. Frameworks:
 - i. Scikit-Learn, Caffe, Comfortable with Agile/Scrum methodologies.
 - ii. Experience with game editor and commercial (Max, PhotoShop, Modo, etc.) plugins/modification.

6. DevOps engineer

- a. Technical Skills:



3.4 Industry needs

The following industry needs have been extracted from ENISA, Gartner and CLUSIT forecasts:

- ENISA highlights in [4] the following research focus (that we connect to future market needs):
 - Hyperconnected World: The redefinition of boundaries of human-computer interaction (**HCI**), and the concomitant cyber risks that are associated with this; Cybersecurity in the context of new generations of mobile communications and data collection or processing methods (evolution from 5G to **6G**).
 - Computational security: efficient implementation of **symmetric key schemes** at higher security levels, transition to the **Post Quantum** era of **cryptographic systems**, secure implementations of cryptographic systems are needed that resist **side channel attacks, standards for new quantum resilient safe algorithms and protocols**.
 - Intelligent systems: design of approaches for monitoring large-scale and possibly interconnected systems, exploration of **biomimetic cybersecurity algorithms**; Inclusion of **context awareness in machine learning (ML)** in order to boost resiliency.
 - Cyberbiosecurity: risks and the threat landscape in **biotechnology R&I**, risk management framework in the field of public health microbiology, **bio vulnerabilities** in the context of cyber, processes and routines throughout the life science fields that require cyber-interfaces and reliance on automation, cyberbiosecurity guides and standards.
- CLUSIT provides in [6] the following advice for enterprises in the context of cyber resilience:
 - Implement access restrictions by enforcing **privilege separation and least-privileged access**, as well as using privileged access workstations (**PAWs**) for managing identity systems.
 - Implement Multi-Factor-Authentication (**MFA**) and **Conditional Access Control**.
 - Employ privileged access management controls, such as **Justin-Time (JIT) access and Just-Enough Access (JEA) administrator access**.
 - Invest in extensive detection and response (**XDR**) capabilities and modern cloud-native tools that use machine learning to separate noise from signals.
 - Adopt **Zero Trust principles** (e.g., explicitly verify devices before allowing access to resources, continuously evaluate privileges and environment conditions, allow the minimum set of privileges); and implement security controls and procedures in DevOps and application lifecycle processes.
 - Every organisation should also identify and protect data according to the risk; and patch regularly.
- Gartner reports in [7] how the 400 respondents indicated Zero Trust Network Access (**ZTNA**) as a pilot security project (with high value for the enterprise); Security Orchestration Automation and Response (**SOAR** - high enterprise value), Endpoint Detection and Response (**EDR**) and Cloud Access Security Broker (CASBs) - both with medium enterprise value, and **XDR** (low enterprise value) as projects with expected deployment in 2023. The key takeaways interesting for MERIT are:
 - MSEs are responding to surging ransomware attacks by deploying **MDR**, Network Detection and Response (**NDR**), Endpoint Detection and Response (**EDR**) and Extended Detection and Response (**XDR**).
 - MSEs are prioritizing deployment of cloud and security technologies that strengthen infrastructure for remote and hybrid work. **Distributed Cloud Systems** and **Hybrid Cloud Storage** are also trending, prompting their prioritized deployment.



- While MSEs plan to deploy **Citizen Integrator Tools** by 2023, they are currently piloting Citizen Automation and Development Platforms (CADPs) to support low-code development environments for business users. By investing in lower-risk **citizen technologies**, MSEs aim to drive business-led IT and hyper automation while improving speed and agility.
- Despite advancements in **NLP** technologies, the complexity and ambiguity of the human language continues to be an obstacle for mainstream deployment.
- A growing number of **SD-WAN** and **SASE** vendors offer integrated Enhanced Internet capabilities, prompting MSEs to evaluate potential efficiencies. While 20% of MSEs have already deployed the technology, others are still evaluating how well it lives up to market hype.
- Despite indicating high-deployment risks for AI technologies, over 64% of the MSEs are either currently deploying or have already deployed **AI cloud services** and **AIOps**.
- Although MSEs identify 5G services as high value, inconsistent coverage and lack of supported devices prevent wider adoption. Instead, MSEs plan to deploy **identity-based segmentation**, **SD-WAN** and **Network Traffic Analysis** by 2023 for secure and consistent network coverage that enhances employee productivity.
- MSEs are recognizing the advantages of **API management PaaS** in supporting cloud platforms and automation. Talent shortages in specialized skills also preclude MSEs from hiring staff to support API management.

The following industry needs have been extracted from the Frost&Sullivan reports:

1. In the context of CS, the survey [20] highlights survey the **Top 3 cybersecurity concerns** (in France, Germany, Italy, Spain, and UK): system vulnerabilities, ransomware, and targeted phishing attacks. Almost half of interviewed enterprises (~100 in each country) declared to be **underprepared on the following topics**: Security Orchestration, Automation and Response (SOAR); SOC as a Service, Cloud Access Security Broker (CASB), Security Information and Event Management (SIEM). The **Top 5 most desired security additions** are (in order):
 - I. Security Orchestration, Automation, and Response
 - II. SOC as a Service
 - III. Cloud Access Security Broker
 - IV. Multi-Factor Authentication
 - V. Security Information and Event Management

In addition, among the key takeaways, it is important to highlight how:

- **zero trust frameworks and identity-based security technologies** have become the gold standard in 2022; in a world that has embraced remote working;
- more organisations consider partnering with firms providing **SOC as a service** to supplement in-house capabilities or push security improvement initiatives forward. This highlights the chronic, in-house shortage of experienced cybersecurity professionals.

2. In the context of CS - Waste Recycling and Circular Economy [22], which has also been selected in line with the EU Green Deal objectives, Frost & Sullivan reports the **technology areas** where the Top 20 digital practitioners operate: Smart Waste Recycling Bin Collection Systems (8); Smart Fleet Management and Logistics Solutions (7); Smart Waste Sorting and Recycling (4); Digital Resource Mapping, Cloud Computing, Connectivity, and Customer Interface Operations (10 - this is also the area expected to attract most revenue). The set of **developed/operated technologies** in the field are:
 - a. Fill-level sensors: detection of waste volumes or intelligent object recognition.
 - b. Smart trucks: in-vehicle software to optimize routes, time, and costs to reduce emissions.
 - c. Energy efficiency and performance monitoring: decision intelligence.



- d. Smart mobile apps: management of waste accounts, services, and billing on the go.
- e. AI recycling robots: intelligent automated sorting.
- f. Cloud-based remote services: fifth-generation network narrow range for massive IoT.
- g. Predictive analytics: continual demand management and conservation.
- h. Asset health monitoring and management: real-time visualization of multiple data inputs.
- i. Blockchain: aligns supply chain knowledge, visibility, and transparency.
- j. Digital twins: digital modelling of supply chain.
- k. Route optimization software minimizes windshield time and maximizes fleet capacities.
- l. Digital platforms: surveying, documentation, collaboration, logistics, and reporting.

The key Waste Recycling and Circular Economy trends are:

- I. Smart Bins: smart waste bins have sensors and/or camera-based visuals to monitor waste volumes and types, including intelligent object-recognition bins that automatically sort and compact cups, cans, and plastic bottles. The bins often connect to a platform that analyses real-time data to improve the efficiency of waste-related services and recycling grates.
 - a. Frost & Sullivan estimates that implementing smart waste containers can reduce waste collection companies' operational expenditure (OPEX) by 50%, while increasing service quality.
- II. Smart Trucks and Route Optimization Software: circular business models comprise activities and approaches aiming to support the transition toward resource efficiency and a circular economy.
- III. AI-based Material Sorting: the repair industry is seen as a crucial element to push the transformation toward a circular economy.
- IV. Cloud-based Enterprises: reverse logistics is becoming a crucial component of the well-organized, modern supply chain, moving goods back from the end user to the seller or manufacturer.
- V. Circular Management System for Building Materials — Building as Material Banks (BAMB): digital material passports and software platforms aim to reduce resource use in the construction industry.
- VI. Plastic Credits: the digital credit system is a possible solution to drive plastic reduction and fight global plastic pollution.

The following highlights are presented according to the Top 3 Strategic Imperatives in this sector:

- Stakeholders in the waste value chain are deploying technologies and solutions that enable cost-effectiveness and optimization.
- As smart technologies are still emerging, the digital waste management market is in the early development phase but will grow substantially during the forecast period (2021–2030).

Among the 3 growth opportunities, are of interest:

- Supply Chain Digital Sustainability (Environment, Communication, and Information tech): future-proofing economic development depends on supply chain innovations. Digital tools, such as blockchain, digital twins, and AI, can help companies increase the resilience of their supply chains. Physical and digital verification of raw materials at every stage in the value chain by digitizing. It is necessary to improve supply chain collaboration using innovative digital technologies, including uplifting technology capabilities of individual suppliers, to enable the sharing of meaningful data-based information with major stakeholders.



- SaaS Business Model: the digital marketplace uses cloud-based interactive platforms for on-demand waste management services.
 - Seek digital solutions that enable the development of innovative business models that cover end-to-end services based on customer requirements.
 - Analyse and understand customers need and interests to build sustainable operations with customized features depending on individual end-user profiles and expansion potential.
 - Incorporate flexibility in CAPEX and OPEX management, subscription-based features, and online self-service.
 - Enable interaction between customers (waste generators) and waste operators to gather and analyse important data to enhance operations and drive growth.
 - Adopt performance-based financial business models that encourage capital investments.
 - Focus on solutions that guarantee an open platform for change and are easily adaptable to changing market and customer needs.

- 3. In the context of CS - smart borders, Frost & Sullivan provides in [21] the following 3 takeaways:
 - I. To secure sustainable business operations during the recovery period (2021–2023), airports will need to reduce fixed costs, ensure an on-time and safe passenger experience, and improve staff and passenger safety.
 - II. Airports should look beyond automation and focus on improving operating efficiencies. In the next 5–10 years, biometrics, blockchain, disruption management, operation control centres, and self-service technologies are projected to gain traction.
 - III. Airports and airlines that invest now in modernizing their infrastructure to support seamless travel technology will be ahead of the curve, better able to handle periodic stressors from the ongoing pandemic (e.g., new variants) and ultimately recover faster.

The report also highlights the following trends:

- The COVID-19 pandemic has increased the focus on ensuring touchless/minimum physical touch for passengers. Biometric verification, touchless ID and access control, and user behavioural tracking are trends that will enable airlines to realize a touchless and secure passenger journey.
 - End-to-end cybertools for proactive threat detection, automated incident response protocols, automation of preventive measures, and encrypting personal and sensitive data (e.g., credit card information) are high-priority projects that are gaining significant traction across industries.
-
4. The following technologies are extracted from the Frost & Sullivan report in the context of IoT - Automotive [25]: sensors (Lidar, Radar, image sensors), Communication networks (V2V, V2X, V2I), Communications technologies (Bluetooth, Wi-Fi, RFID, UWB)/Zigbee, WSNs, 4G LTE/5G, Lora, NB-IoT), Vehicular Communication Networks, IoV Cloud Technologies, Machine learning, Data analytics, Object detection, Image processing algorithms, Accurate sensing of parameters, Location-based multi-parameter sensing, Real-time data Management, Efficient communication between machine-machine and human-machine, Auto-steer, manoeuvrability, Error detection, Predictive maintenance, Remote operability of system (automotive manufacturing), Remote monitoring Prediction of traffic conditions, and Intelligence functionality.



5. The following technologies are extracted from the Frost & Sullivan report in the context of IoT - Blockchain [26]: IoT deployment challenges of addressing memory and processor limitations, Securing large volumes of IoT devices, and Handling data velocity and volumes; Blockchain-based solutions for IoT Device Identity, Communication & Reputation Management, Economy of Things and Data Brokerage, IoT Supply Chain Integrity Assurance, On-demand Asset Sharing Services, Secure & Autonomous Communication, 5G-enabled Blockchain Services, Cybersecurity Assurance Services, and Economy of Things. Blockchains for Secure IoT Firmware Updates, Compliance Verification of IoT Device Models, and Cybersecurity through Monitoring of Device Traffic Patterns.

6. In context of AI, the World Economic Forum estimates in [16] that, **by 2025, 85 million jobs** may be displaced by a shift in the division of labour between humans and machines. In [14], *data and AI skills* are indicated as the essential digital skills required across all business disciplines. Figure 3 indicates them as requirement for the indicated set of specialised skills.

Specialized skill	Emerging job clusters
1. Product Marketing	Data and AI, People and Culture, Marketing, Product Development, Sales (5)
2. Digital Marketing	Content, Data and AI, Marketing, Product Development, Sales (5)
3. Software Development Life Cycle (SDLC)	Cloud Computing, Data and AI, Engineering, Marketing, Product Development (5)
4. Business Management	People and Culture, Marketing, Product Development, Sales (4)
5. Advertising	Content, Data and AI, Marketing, Sales (4)
6. Human Computer Interaction	Content, Engineering, Marketing, Product Development (4)
7. Development Tools	Cloud Computing, Data and AI, Engineering, Product Development (4)
8. Data Storage Technologies	Cloud Computing, Data and AI, Engineering, Product Development (4)
9. Computer Networking	Cloud Computing, Data and AI, Engineering, Sales (4)
10. Web Development	Cloud Computing, Content, Engineering, Marketing (4)
11. Management Consulting	Data and AI, People and Culture, Product Development (3)
12. Entrepreneurship	People and Culture, Marketing, Sales (3)
13. Artificial Intelligence	Cloud Computing, Data and AI, Engineering (3)
14. Data Science	Data and AI, Marketing, Product Development (3)
15. Retail Sales	People and Culture, Marketing, Sales (3)
16. Technical Support	Cloud Computing, Product Development, Sales (3)
17. Social Media	Content, Marketing, Sales (3)
18. Graphic Design	Content, Engineering, Marketing (3)
19. Information Management	Content, Data and AI, Marketing (3)

Figure 3: top cross-cutting, specialized skills of the future - from [14].

The authors indicate as key roles in the data ecosystem, including Industrial and Cyber domain:

- a. Data Engineering.
- b. Data Analytics.
- c. Data Scientists.

They also mention that roles growing in demand include data analysts, AI and machine learning specialists, robotics engineers, software and application developers, and digital transformation specialists. The following Figure 4 presents a comprehensive summary of the Artificial intelligence ecosystem in data space. At first, we highlighted application domains from manufacturing, education and health, where AI could have a significantly impact. Further, we highlighted the common ingredients to enable AI for the real-time deployment of a specific domain. Each role has some specific job requirements; further, we classify it as standard and specific skills needed for each role, along with future skills to address the complex challenges.

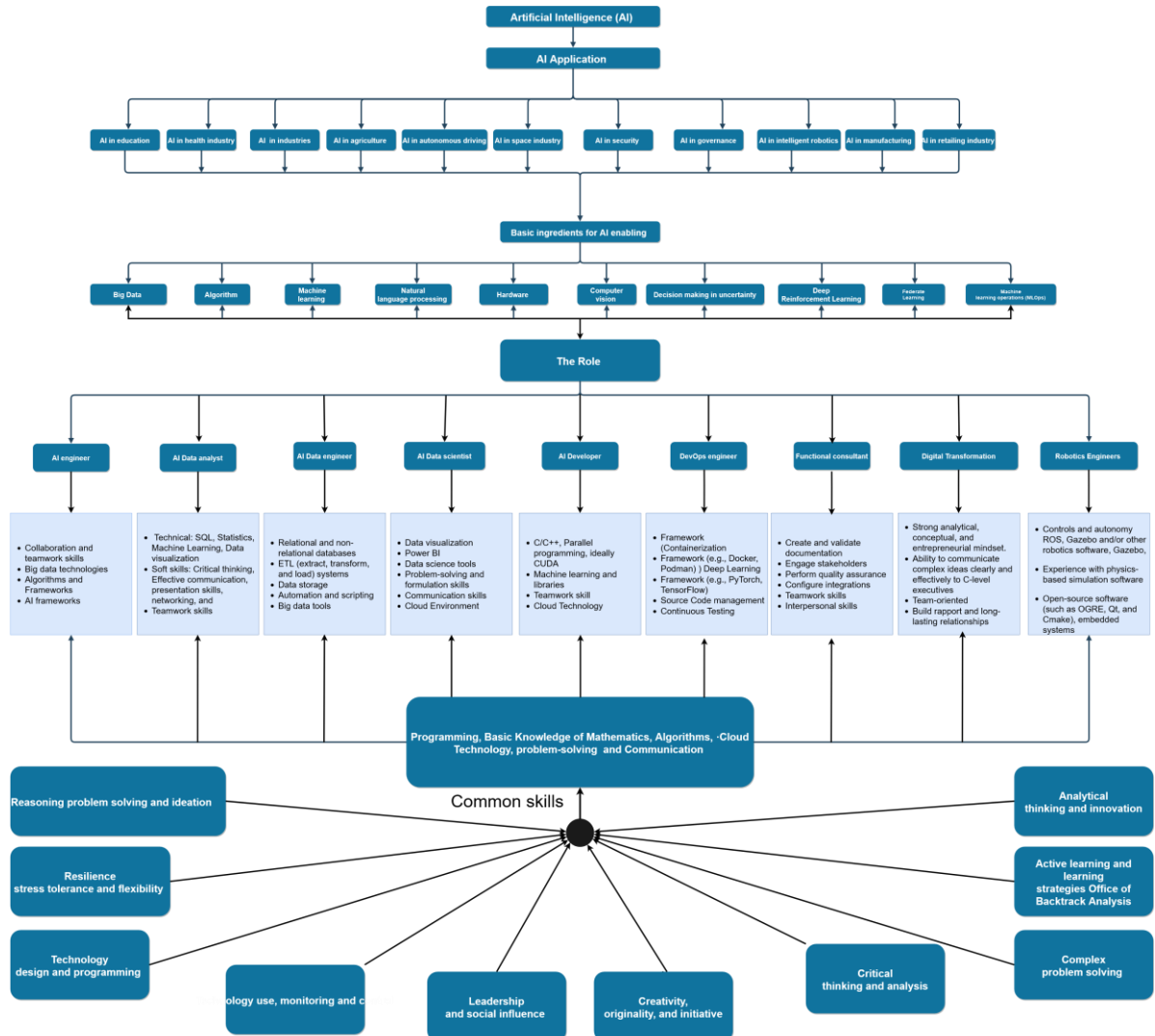


Figure 4: AI Ecosystem in industrial data space.



4 Conclusions

This document presents the methodology to identify and prioritize the most relevant topics and skills for the consortium Universities (to design/upgrade and administer the master programme), and for the MERIT communication and dissemination activities. Its first application provides seven results according to as many steps:

1. The definition of MERIT Partners' areas of expertise, that allowed focusing the effort in identifying the current and forecasted topics and skills in D3.1; and can also be used when preparing the material for the master programme (WP5), and for both the educators upskilling and their mobility between Universities (WP6).
2. The definition of the skills to be developed in the context of study programs by MERIT Universities, that allowed to include their specific needs in the procedure.
3. A carefully crafted set of data sources and keywords identified by MERIT Partners to investigate current and forecasted topics and skills in AI, CS and IoT. In future editions, we plan to improve this step with a topics trend analysis to investigate their relevance in time and better tailor the MERIT programme to be on the edge and in line with the market needs.
4. A set of 76 topics and skills identified from research, statistics, reports and forecasts that are crucial to define a study program capable of educating the next generation of experts in the fields of AI, CS, and IoT and their interplays.
5. A set of 84 technologies derived from industry needs whose knowledge is a key enabler to make the skills of the study program operational.
6. A carefully defined mapping from topics to technologies that facilitates the exploitation of the skills developed during the study program: 40 topics/skills - with 30 technologies connected with automation and programmability and 22 with Network / Network Fundamentals.
7. A prioritized list of 22 topics, skills and technologies that can be used as the basis to define a coherent and comprehensive study program coordinated among the Universities in the MERIT consortium.
 - a. Evaluating the list in the context of the ESCO [27] framework, we found that the acquisition of these knowledge, technologies and skills is linked with 233 unique skills and 159 knowledge items, spans multiple application scenarios (from finance to healthcare) and provides access to more than 1200 job positions. The combination of automated querying and manual investigation ensured comprehensive coverage and accuracy. Future work could focus on improving the algorithm to handle ambiguous cases better.
 - b. Considering the e-CF framework, we mapped Step 7 results to 12 e-CF competences and leveraging competences to 25 e-CF roles.

The following general insights can be derived from the first iteration of the methodology:

- A standardised approach to identify the professional roles is essential to determine current and future skill gaps: agencies like ENISA or research projects funded by the European Commission play a leading role in identifying and defining required skills (as they can have different names in different fields).
- All three areas share, from both the research and industry perspective, the need for both technical and soft skills.
- Acquiring expertise common to the three areas (AI, CS and IoT) opens to highly specialized professional figures, with wider career prospects: for instance, using AI in the context of Threat Intelligence (in a CS working role) or securing AI algorithms (in an "AI"-oriented role) can both share a substantial portion of expertise.



MERIT Deliverable



**Co-funded by
the European Union**



Additionally, advanced projects about digital skills like MERIT share the burden and responsibility to highlight and leverage the synergies of multiple domains (AI, CS and IoT); and cope with the current and future skill gaps by training and upskilling on the most relevant and needed topics.

To sum up, the first iteration of our methodology shows a considerable need for CS, AI and IoT experts in engineering (such as developers, architects, engineers) and management (such as project management, or figures in charge of data governance and AI ethics). From the MERIT project perspective, we see a lot of opportunities to have a huge synergy in all three areas that can be exploited by defining a common framework with hands-on experience. We regard this as essential for current and future professionals to cope with the growing skills shortage.



References

- [1] C. C. Didar Zowghi, "Requirements Elicitation: A Survey of Techniques, Approaches, and Tools," in *Engineering and Managing Software Requirements*, 2005.
- [2] ENISA, "European Cybersecurity Skills Framework Role Profiles," 2022.
- [3] ENISA, "Addressing Skills Shortage and Gap Through Higher Education," 2021.
- [4] ENISA, "RESEARCH AND INNOVATION BRIEF: Annual Report on Cybersecurity Research and Innovation," 2022.
- [5] CLUSIT, "Rapporto Clusit 2022," 2022.
- [6] CLUSIT, "Rapporto Clusit 2023," 2023.
- [7] Gartner, *2022-2024 Technology Adoption Roadmap for Midsize Enterprises*, 2022.
- [8] GARTNER, "Gartner Predicts 10% of Large Enterprises Will Have a Mature and Measurable Zero-Trust Program in Place by 2026," 2023. [Online]. Available: <https://www.gartner.com/en/newsroom/press-releases/2023-01-23-gartner-predicts-10-percent-of-large-enterprises-will-have-a-mature-and-measurable-zero-trust-program-in-place-by-2026>.
- [9] GARTNER, "Gartner Identifies Three Factors Influencing Growth in Security Spending," 2022. [Online]. Available: <https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i>.
- [10] GARTNER, "Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23," 2022.
- [11] GARTNER, "Gartner Identifies Top Five Trends in Privacy Through 2024," 2022.
- [12] C. Z. a. Y. Lu, "Study on artificial intelligence: The state of the art and future prospects," *Journal of Industrial Information Integration*, 2021.
- [13] Microsoft, "Learning paths and modules (queried with a specific subject and roles)," [Online]. Available: <https://learn.microsoft.com/en-us/training/browse/?roles=ai-engineer%2Cdata-engineer%2Cdata-scientist%2Cdeveloper%2Cfunctional-consultant&subjects=data-ai>.
- [14] S. Malik, "Top 3 Data Job Roles Explained : A Career Guide," 2021. [Online]. Available: <https://www.ibm.com/blogs/ibm-training/top-3-data-roles-a-career-guide/>.
- [15] Expert Group on Future Skills Needs, "AI Skills: A Preliminary Assessment of the Skills Needed for," 2022.
- [16] World Economic Forum, "The Future of Jobs Report," 2020.
- [17] B. Marr, "What Are The Most In-Demand AI Skills?," 2022. [Online]. Available: <https://www.forbes.com/sites/bernardmarr/2022/06/13/what-are-the-most-in-demand-ai-skills/?sh=37e038af249c>.
- [18] Gartner, "Roles and Skills to Support Advanced Analytics and AI Initiatives," 2022.
- [19] J. Soldatos, "The EU-IoT Framework for Internet of Things Skills: Closing the Talent Gap," 2023.
- [20] Frost & Sullivan, "European Cybersecurity Responsibility, Spending, and Posture: a Survey of Enterprise End Users Who Influence Cybersecurity Budgets.," 2022.



- [21] Frost & Sullivan, “Global Digital Smart Borders Growth Opportunities: defining Future Growth Strategies for Different Ports of Entry.,” 2022.
- [22] Frost & Sullivan, “Top 20 Companies Accelerating Digital Transformation in the Global Waste Recycling and Circular Economy Industry: new Era of Data-driven Operation and Industry Convergence will Optimize Waste Services and Close the Loop on Material Sourcing.,” 2022.
- [23] Frost & Sullivan, “Global Artificial Intelligence Growth Opportunities: transformative Mega Trends in AI Create ICT Growth.,” 2022.
- [24] Frost & Sullivan, “Enhancing European Customer Experience with Artificial Intelligence: AI Technologies Offer New Opportunities to Nurture Relationships and Enhance Customer Contact Effectiveness.”.
- [25] Frost & Sullivan, “Technology Convergence is Enabling the Automotive Internet of Things (IoT): advanced Communication Technologies will Revolutionize Automotive IoT.,” 2022.
- [26] Frost & Sullivan, “IoT Cybersecurity Analysis—Blockchain-enabled IoT Cybersecurity Market: implementing New Service Models through Distributed Ledger Technologies,” 2018.
- [27] The European Commission, “European Skills, Competences, Qualifications and Occupations (ESCO),” [Online]. Available: <https://esco.ec.europa.eu/en>.
- [28] European Committee for Standardization (CEN), “European e-Competence Framework (e-CF),” [Online]. Available: <https://ecfexplorer.itprofessionalism.org/>.
- [29] European Technology and Innovation Platform, “Strategic Research and Innovation Agenda 2023,” 2023.
- [30] Internet of Learning, “13 Best Artificial Intelligence Bootcamps,” 2023. [Online]. Available: <https://internetoflearning.org/bootcamps/best-artificial-intelligence-bootcamps/>.
- [31] Coursera, “What Is an AI Engineer? (And How to Become One),” 2022. [Online]. Available: <https://www.coursera.org/articles/ai-engineer>.
- [32] I. Campos, “What Does a Prompt Engineer Do?,” 2023. [Online]. Available: <https://medium.com/sopmac-ai/what-does-a-prompt-engineer-do-f00c6f2ad1ab>.
- [33] K. Cotterill, “Ethics and AI: Skills Needed,” 2018. [Online]. Available: <https://www.linkedin.com/pulse/ethics-ai-skills-needed-keith-cotterill>.



Appendix A

The following table lists the unique skills reported by ENISA in [2], together with the number of Cybersecurity profiles that requires them; skills only associated with one profile have been excluded.

UNIQUE SKILLS	# of Profiles
Communicate, present and report to relevant stakeholders	8
Collaborate with other team members and colleagues	4
Identify and solve cybersecurity-related issues	4
Decompose and analyse systems to identify weaknesses and ineffective controls	3
Collect, analyse and correlate cyber threat information originating from multiple sources	2
Communicate, coordinate and cooperate with internal and external stakeholders	2
Conduct technical analysis and reporting	2
Decompose and analyse systems to develop security and privacy requirements and identify effective solutions	2
Develop code, scripts and programmes	2
Motivate and encourage people	2



Appendix B

The following table details the intersections between each subject and the selected CS certification. The "x" indicates its presence in every exam outline. The exclamation point indicates extensive coverage.

Topic	Cov- ered by #	ISO 270 01	EC-Es- sen- tials	CE H	CISM	CCNA	CySA+	CISSP	Secu- rity+
Adversarial artificial intelligence (AI)*	1								x
Attacks, Threats, and Vulnerabilities	1								!
Authentication and authorization implementation	2							!	!
Automation and Programmability	4					x	x	x	x
Cloud Computing	6		x	!		x	x	x	!
Compliance and Assessment	3						x	x	x
Cryptography	4			x			x	x	x
Denial of Service	2	x		!					
Digital Forensics	3		x				x	x	
Enumeration	1			x					
Ethical Hacking	2		x	x					
Evading IDS, Firewalls, and Honeypots	1			!					
Foot Printing and Reconnaissance	1			x					
Hacking Mobile Platforms	1			!					
Hacking Web Applications	1			!					
Hacking Web Servers	1			!					
Hacking Wireless Networks	1			!					
Incident Management	6	x		x	!		x	x	!
Information Security Governance	4	x			x			x	x
Information Security Program, Training and Awareness	5	x		x	x		x	x	
IoT and OT Hacking	1			!					
IP Connectivity	1					!			
IP Services	1					x			
Malware Threats	4			!			x	x	x



MERIT Deliverable



Co-funded by
the European Union



Mobile security solutions implementation	1								!
Network Access	3					!	x	x	
Network Defence	2		x	!					
Network Fundamentals	4		x	x		!	x		
Phishing	5	x		x			x	x	x
Physical security controls	4		x				x	x	!
PKI implementation	2							x	!
Protocols implementation	1								!
Redundancy, Replication	2							x	!
Scanning Networks	3			x		x	x		
Secure network designs implementation	2							x	!
Secure wireless settings implementation	1								!
Security Fundamentals (Layer 2-3)	2		x			x			
Security Operations and Monitoring	3						!	x	!
Security Planning and Risk Management	6	x		x	!		!	!	x
Security solutions implementation	2							x	!
Session Hijacking	2			!			x		
Sniffing	1			!					
SQL Injection	1			!					
System Hacking	1			x					
Vulnerability Analysis	3			x			!	x	



Appendix C

The following is an abstract representation of the script created to query the ESCO database via the local API.

1. Define a function to read keywords from a file.
2. Define a function to determine the concept type based on the concept string.
3. Define a function to get the KLST (Knowledge, Skills, and Tasks) for a given keyword and group:
 - Send a request to a local server with the keyword.
 - Parse the response and extract the results.
 - For each result, check if it matches the keyword.
 - If it does, add any associated occupations to a global list.
 - Determine the type and parent of the keyword based on the result data.
 - Return a list containing the group, keyword, type, parent title, and parent code.
4. Initialize a dictionary to store occupations for different groups.
5. Get a list of all text files in the current directory.
6. For each file, read the keywords, get the KLST for each keyword, and write the results to a CSV file.
7. For each group in the occupations dictionary, write the occupations to a separate CSV file.