GreenPowerIT - Deliverable

Cartography of available training programs and requirements analysis for the development of new programs

This project has received funding from the European Union's Digital Europe program under **Grant Agreement No. 101083637**

Deliverable number :	D5.1
Due Date :	30/06/2023
Nature[1] :	R
Dissemination Level[1] :	PU
Work Package :	WP5
Lead Beneficiary :	INRIA
Contributing Beneficiaries :	UNIVERSITE DE LILLE ; CITC

[1] Nature: R = Report, P = Prototype, D = Demonstrator, O = Other

Dissemination Level
PU = Public
PP = Restricted to other program participants (including the Commission Services)
SEN = Restricted to a group specified by the consortium (including the Commission Services)
CO = Confidential, only for members of the consortium (including the Commission Services)

Co-funded by the European Union.

DOCUMENT HISTORY

Version	Date	Author	Description
0.1	26/06/2023	INRIA	Creation Deliverable template
0.2	21/07/2023	CITC, UNIV LILLE	Updates and completions
0.3	24/07/2023	CITC	Critical review and proofreading
0.4	27/07/2023	INRIA	Final edits for approval
1.0	28/07/2023	INRIA	Final version
1.1	06/11/2023	UNIV LILLE	Update final version

TABLE OF CONTENT

1 Introduction 8

1.1 Purpose and Scope of the Deliverable 8

2 Overview of the types of training on Artificial Intelligence, Cybersecurity, and Internet of Things 9

2.1 Type of IT engineering trainings programs 9

2.2 Type of specialized trainings in AI 10

2.2.1 Frugal AI 10

2.2.2 Frugal AI in Cybersecurity 10

2.2.3 Examples of use of Frugal AI in Cybersecurity 10

2.2.4 Challenges of the use of Frugal AI in Cybersecurity 11

2.2.5 Limitations of using frugal AI in cybersecurity 12

2.2.6 Real-world examples of using frugal AI in cybersecurity 12

2.2.7 Example of a program of AI training 13

2.2.8 Training Prototype for the EDIH 14

3 Regional Academic Mapping of Cybersecurity, AI and IoT Education 18

3.1 Unevenly distributed training offer for middle and senior management in the region of Hauts de France 18

3.1.1 Location of universities offering courses in the fields of cybersecurity, IoT, and AI 18

3.1.2 Typology and characteristics of university training offerings 19

3.1.3 University training offerings in the Hauts de France region 19

3.1.4 The employment needs of the region 23

3.2 A training offer for intermediate and senior management, with diversified levels of specialization and expertise 28

3.2.1 Generalist programs in Cybersecurity, AI, and/or IoT 29

3.2.2 Specialized programs in Cybersecurity, AI, and/or IoT 32

3.2.3 Specialized programs in AI for certain application areas 37

3.2.4 Career-oriented programs in Cybersecurity, AI, and/or IoT 38

3.2.5 Programs on the environment of Cybersecurity, AI, and IoT 40

3.3 The current training offer provides the business world with university or specialized courses that allow customized training to adapt to the specific needs of companies 41

3.3.1 Characteristics of the programs offered by these universities: Diverse programs for all types of audiences 41

3.3.2 University programs, specialized or customized, tailored to the needs 41

3.3.3 Programs aligned with the business world, technological and scientific developments, often linked to research 41

3.3.4 Prerequisites 42
3.4 Conclusion on academic offerings 42
4 Regional Private Trainings Mapping of Cybersecurity, AI and IoT Education 43
4.1 Key institutions and organizations offering private trainings Cybersecurity, AI and IoT Education 43
4.1.1 EDIH partners 43
4.1.2 Other organizations / Associations 44
4.1.3 Companies , other training organizations 45
4.2 Available Private Trainings Programs 46
4.2.1 Cybersecurity 47
4.2.2 Artificial Intelligence 47
4.3 Conclusion 48
5 Analysis of stakeholder's technological needs and requirements to build dedicated training programs not covered by the existing training programs offer 49
5.1 Local authorities 49
5.1.1 What is your current level of knowledge of the following technologies? 49
5.1.2 What training do you need? 50
5.1.3 Have you already identified specific training courses that meet your needs (in this area)? 50
5.1.4 Ideally, what format should the training take to adapt to the work context? 51
5.1.5 The availability of hours per months 51
5.2 SMEs 51
5.2.1 What is your current level of knowledge of the following technologies? 51
5.2.2 Which training have you already received? 52
5.2.3 What training do you need? 52
5.2.4 Have you already identified specific training courses that meet your needs (in this area)? 52
5.2.5 Ideally, what format should training take to adapt to the work context? 52
5.2.6 The availability of hours per months 53
5.3 Conclusion 53
5.3.1 Local authorities 53
5.3.2 SMEs 53
6 Conclusion 54

TABLE OF FIGURES

Figure 1 Map of the Universities offering courses in the fields of Cybersecurity, IoT and AI 18
Figure 2 Levels of training in the offerings 19
Figure 3 Location of Bachelor's degrees, training for intermediate management 20
Figure 4 Locations of other intermediate management level programs 21
Figure 5 Location of masters 21
Figure 6 Location of engineering programs 22
Figure 7 Number of recruitment projects in IT Professions in Hauts de France region 23
Figure 8 Number of recruitment projects in IT support technicians in Hauts de France region 24
Figure 9 Number of recruitment projects for IT engineers, R&D managers and IT project Managers in Hauts de France Region 25
Figure 10 Number of recruitment projects for IT engineers and administrative and maintenance managers in Hauts de France region 26
Figure 11 Distribution of the offerings according to the type of program 28
Figure 12 Generalist programs in Cybersecurity, AI, and/or IoT 30
Figure 13 Generalist programs for senior management in Cybersecurity, AI, and/or IoT 32
Figure 14 specialized programs for intermediate level in Cybersecurity, AI, and/or IoT 34
Figure 15 specialized programs for senior management level in Cybersecurity, AI, and/or IoT 36
Figure 16 Specialized programs in AI for certain application areas 37
Figure 17 Career-oriented programs in Cybersecurity, AI, and/or IoT 39
Figure 18 Programs on the environment of Cybersecurity, AI, and IoT 40
Figure 19 Level of knowledge of proposed technologies 49
Figure 20 Level of knowledge of proposed technologies 50
Figure 21 Training needs 50
Figure 22 Training format 51
Figure 23 Level of knowledge of proposed technologies 52
Figure 24 Training needs 52
Figure 25 Training format 53

TABLE OF REFERENCES

Ref 1 https://iotcluster.fr/index.php/en/homepage/ 43
Ref 2 https://www.inria-academy.fr/ 43
Ref 3 https://www.cma-hautsdefrance.fr/ 44
Ref 4 https://www.cnam-hauts-de-france.fr/presentation-du-cnam-hauts-de-france/ 44
Ref 5 https://www.afpi-acmformation.com/lafpi/ 44
Ref 6 https://www.skills4all.com/ 45
Ref 7 https://seela.io/ 45
Ref 8 https://adaliance.com/training/la-cyber-securite/ 45
Ref 9 https://www.ib-formation.fr/qui-sommes-nous/raisons-de-choisir-ib 45
Ref 10 https://www.m2iformation.fr/qui-sommes-nous/ 45
Ref 11 https://falconacademy.fr/ 45
Ref 12 https://www.proalterna-sarl.com/ 45
Ref 13 https://www.cesi.fr/ 45
Ref 14 https://e-catalyst.fr/ 45
Ref 15 https://www.institutmontaigne.org/initiatives/objectif-ia 46
Ref 16 https://simplon.co/ 46
Ref 17 https://www.lewagon.com/fr/about-us 46

ACRONYMS

Acronym	Description
EDIH	European Digital Innovation Hub
AI	Artificial Intelligence
IoT	Internet of Things

1 Introduction

1.1 Purpose and Scope of the Deliverable

The objectives of this workpackage are to design and implement multi-level training programs (beginner-intermediate-expert) to enhance the technological skills of the stakeholders of the EDIH (European Digital Innovation Hub).

• Develop dedicated training programs (5 days) to address the specific needs of projects requiring advanced technological knowledge and/or skills.

• Establish a quality label "EDIH Skills and Training" to enable project stakeholders to identify available dedicated training programs at their regional level to meet their technological training needs.

• Foster synergies between the stakeholders of the EDIH and the consortium.

The proposed method for the work package is as follows:

- Analysis of Skills Needs: This stage will involve identifying the skills and training needs for the EDIH project based on the objectives to be achieved, the technologies to be utilized, and the profiles required for project implementation. This analysis will enable the creation of a skills mapping, identifying gaps and specific training requirements.
- Development of a Training Program: Based on the results of the skills needs analysis, the aim is to design a tailored training program for the various profiles required for the EDIH project. The program may include online courses, in-person training sessions, or practical workshops to allow participants to enhance their knowledge and skills according to the identified needs.
- Identification of Training Partners: It is essential to identify the most relevant training partners for the specific needs of the EDIH project. These partners could be academic institutions, professional training organizations, research centers, or specialized companies in the fields of IT, AI, and cybersecurity.
- Implementation of the Training Program: This step involves the concrete implementation of the training program, organizing training sessions, ensuring participant involvement, and monitoring learners' progress throughout the training.

The objective of this deliverable is to map and identify all the regional training offerings in IoT, cybersecurity, and Artificial Intelligence, and to analyze this offering in relation to the needs of local authorities and regional businesses. This will allow us to subsequently target the implementation of training actions more effectively within the territory.

2 Overview of the types of training on Artificial Intelligence, Cybersecurity, and Internet of Things

2.1 Type of IT engineering trainings programs

Several training programs can be beneficial based on the specific needs identified for the EDIH Hauts-de-France project. Among the most relevant ones, we can mention:

• Software and Application Development Training: This training can help educate engineers capable of designing, developing, and maintaining software and applications for businesses in various sectors.

• Artificial Intelligence Training: This training can enable engineers to develop intelligent systems for industrial, medical, financial, and other applications.

• Cybersecurity Training: This training can equip engineers with specialization in information systems security and protection of sensitive data against cyber-attacks.

• IT Project Management Training: This training can prepare engineers to efficiently manage complex IT projects while adhering to budgets and timelines.

• Computer Networks Training: This training can educate engineers specialized in designing and maintaining computer networks for businesses.

• Blockchain Training: This training can enable engineers to design and develop blockchain applications for companies in different sectors.

• Big Data Training: This training can equip engineers to manage and analyze large datasets for businesses in various industries.

• Cloud Computing Training: This training can prepare engineers to design, implement, and manage Cloud infrastructures for businesses.

• Internet of Things (IoT) Training: This training can help engineers develop IoT systems for companies in various sectors.

• Virtual and Augmented Reality Training: This training can prepare engineers to design and develop virtual and augmented reality applications for businesses in different industries.

• Advanced Programming Training: This training can provide engineers with strong technical expertise in programming for complex applications across different sectors.

• Information Security Management Training: This training can prepare engineers with skills in information security management for businesses, including risk identification, prevention of breaches, and crisis management in case of incidents.

These training programs can contribute to the development of skilled and versatile engineers in key areas of IT, AI, and cybersecurity to meet the needs of the EDIH Hauts-de-France project.

2.2 Type of specialized trainings in AI

2.2.1 Frugal AI

Frugal AI is a branch of artificial intelligence that focuses on developing AI models that are simpler, lighter, and less energy-intensive than traditional AI models. This approach centers on optimizing AI performance using limited computing resources.

Frugal AI is particularly useful for applications that require AI capabilities on mobile devices or connected objects such as smartwatches, smartphones, IoT sensors, etc. Frugal AI models enable developers to create AI applications that can operate on these devices with limited resources in terms of memory, computing power, and storage.

Techniques used to develop frugal AI models include model compression, quantization of model weights, the use of lossless compression algorithms, data dimensionality reduction, and online learning techniques.

Frugal AI offers several advantages, including more efficient resource utilization, lower energy consumption, reduced data storage and processing costs, and decreased latency.

However, frugal AI may have limitations in terms of precision and the complexity of tasks it can perform compared to more complex AI models. Therefore, frugal AI is often used in combination with traditional AI models to provide comprehensive and balanced solutions for AI problems.

2.2.2 Frugal AI in Cybersecurity

Frugal AI is an approach to artificial intelligence that aims to develop efficient algorithms with limited computing resources. This approach is particularly relevant for environments where computing resources are constrained, such as mobile devices, IoT sensors, low-power networks, and cost-effective cloud infrastructures.

Regarding cybersecurity, frugal AI can be useful for detecting threats and malicious attacks in resource-limited environments. For instance, frugal machine learning algorithms can be used to detect phishing attacks or hacking attempts in low-power networks like wireless sensor networks or IoT devices. By employing efficient and frugal algorithms, limited computing resources can be utilized more effectively to enhance security.

Moreover, frugal AI can also enhance the security of mobile applications by enabling faster and more efficient analysis of security data without consuming excessive computing resources. Lastly, by using frugal AI to analyze security data, businesses can reduce cybersecurity costs while improving their effectiveness.

2.2.3 Examples of use of Frugal AI in Cybersecurity

Frugal AI can be used in various domains related to cybersecurity, notably for:

• Phishing Attack Detection: Frugal machine learning algorithms can be used to detect phishing emails by analyzing common characteristics of such emails. These algorithms can identify phishing emails even on resource-limited mobile devices.

• IoT Network Threat Detection: Frugal machine learning algorithms can be employed to detect threats on IoT networks, such as wireless sensor networks. They can identify malicious behaviors on the network, such as suspicious data packet transmissions.

• Mobile App Vulnerability Analysis: Frugal AI can be used to analyze the vulnerability of mobile applications by detecting malicious behaviors in these apps. Frugal machine learning algorithms can identify applications that request excessive permissions or access sensitive data.

• Anomaly Detection on Networks: Frugal AI can be used to detect anomalies on networks, such as hacking attempts or malicious behaviors. Frugal machine learning algorithms can detect these anomalies even on low-power networks.

• Low-Bandwidth Network Security Management: Frugal machine learning algorithms can be used to detect anomalies on low-bandwidth networks, such as satellite networks. They can help identify DDoS attacks, man-in-the-middle attacks, port scans, and other types of attacks.

• Malware Detection: Frugal AI can be employed to detect malware by analyzing program behaviors. Frugal machine learning algorithms can identify malicious programs even on resource-limited mobile devices.

• Enhanced Security for Low-Cost Cloud Infrastructures: Frugal machine learning algorithms can be used to detect anomalies in low-cost cloud infrastructures. They can help identify malicious behaviors, hacking attempts, and suspicious activities on cloud servers.

• Embedded System Vulnerability Management: Frugal AI can be used to detect vulnerabilities in embedded systems, such as industrial control systems. Frugal machine learning algorithms can identify security flaws in embedded systems and enhance their security.

By utilizing frugal AI in these applications, businesses can improve their security without investing in costly computing resources. Furthermore, the use of frugal AI can reduce false alerts and enhance threat detection efficiency. In summary, frugal AI is a highly promising approach for cybersecurity, as it enables more effective utilization of limited resources to improve security. The applications of frugal AI in cybersecurity are numerous and continue to develop as new security challenges arise.

2.2.4 Challenges of the use of Frugal AI in Cybersecurity

There are several challenges to overcome for the use of frugal AI in cybersecurity, such as:

• Adaptation to New Threats: Cybercriminals constantly develop new methods to bypass existing security measures. Frugal machine learning algorithms must be able to quickly adapt to new threats and detect malicious behaviors before they cause damage.

• Privacy Protection: The use of frugal AI for cybersecurity may involve the collection and analysis of large amounts of data. It is crucial to ensure that users' privacy is protected and that data is not misused.

• System Complexity: Computer networks and security systems are becoming increasingly complex, making it challenging to detect anomalies and malicious behaviors. Frugal machine learning algorithms need to adapt to this complexity and provide accurate results.

• Data Availability: Machine learning algorithms require data for training. In many cases, the data needed to train the algorithms may not be available or may not be of sufficient quality.

• Interpretability of Results: The results produced by frugal machine learning algorithms can be difficult to interpret. It is essential to understand how the results were obtained and to justify the decisions based on these results.

In conclusion, the use of frugal AI in cybersecurity can help address many challenges, but there are still obstacles to overcome to maximize its potential.

2.2.5 Limitations of using frugal AI in cybersecurity

• Lack of Data: Machine learning algorithms require data for training, but in some cases, the data may be insufficient, of poor quality, or not representative of the real situation. This can make training the algorithms more challenging and limit their accuracy.

• Complexity of Environments: Computer networks and security systems can be highly complex, with different architectures and protocols, which can make it difficult to adapt frugal machine learning algorithms to these environments.

• Resource Requirements: Machine learning algorithms may require significant resources, such as storage, processing, and communication capabilities. Resources can be limited in environments with cost or power constraints, which can limit the feasibility of using frugal AI.

• Complexity of Result Interpretation: The results produced by machine learning algorithms can be difficult to interpret, as the models used by the algorithms can be very complex. This can make it challenging to understand the reasons for a particular result.

• AI-Related Security Challenges: AI can also present security challenges in itself, as it may be vulnerable to attacks, such as adversarial attacks or data falsification attacks.

In summary, the use of frugal AI in cybersecurity still presents challenges and limitations that must be taken into account. However, despite these limitations, frugal AI remains a promising approach for cybersecurity, as it allows maximizing the utilization of limited resources while improving system security.

2.2.6 Real-world examples of using frugal AI in cybersecurity

• Anomaly Detection: Frugal machine learning algorithms can be used to detect anomalies in security data. For instance, a cybersecurity company utilizes a frugal machine learning algorithm to identify malicious behaviors in network connections by monitoring incoming and outgoing data flows and alerting administrators of any anomalies.

• Malware Detection: Frugal machine learning algorithms can also be employed to detect malware. For example, a security provider uses a frugal machine learning algorithm to analyze suspicious files for malicious behavior.

• Phishing Attack Prevention: Frugal machine learning algorithms can be used to prevent phishing attacks. For instance, a cybersecurity firm leverages a frugal machine learning algorithm to analyze incoming emails for signs of phishing, considering features such as sender's address, message content, and attachments.

• Fraud Detection: Frugal machine learning algorithms can also be applied to detect fraud. For example, a financial services company employs a frugal machine learning algorithm to identify fraudulent transactions by analyzing spending patterns and user behavior.

In these examples, frugal AI showcases its capability in enhancing cybersecurity measures efficiently, even with limited computing resources.

2.2.7 Example of a program of AI training

Introduction

• Presentation of Artificial Intelligence (AI) and cybersecurity

• Importance of AI and cybersecurity in the current context

Artificial Intelligence in cybersecurity

• Various applications of AI in cybersecurity (malware detection, attack detection, etc.)

• Advantages of using AI in cybersecurity (speed, precision, etc.)

• Current limitations of AI in cybersecurity

Risks associated with the use of Artificial Intelligence in cybersecurity

• Risks of false positives and false negatives

• Risks of bias and discrimination

• Security risks related to AI (adversarial attacks, etc.)

Frugal Artificial Intelligence in cybersecurity

• Presentation of frugal AI and its characteristics

• Advantages of using frugal AI in cybersecurity (reduced energy consumption, local data processing, etc.)

• Challenges and limitations of frugal AI in cybersecurity

Federated Learning in Cybersecurity

• Presentation of federated learning and its functioning

• Applications of federated learning in cybersecurity (malware detection, attack detection, etc.)

• Advantages of using federated learning in cybersecurity (privacy protection, collaboration between different stakeholders, etc.)

• Limits and challenges of federated learning in cybersecurity

Conclusion

• Summary of the key points covered in the course

• Perspectives and future challenges for the use of AI and federated learning in cybersecurity.

2.2.8 Training Prototype for the EDIH

2.2.8.1 Cybersecurity

2.2.8.1.1 Beginner Level

• Introduction to Cybersecurity: This training will enable engineers to grasp the fundamental principles of cybersecurity, including common threats and risks, best security practices, as well as key tools and protection techniques.

• Information Systems Security: This training will help engineers understand the core concepts of information systems security, including defense mechanisms, security standards, and protective tools.

2.2.8.1.2 Intermediate Level

• Computer Security Incident Management: This training will equip engineers with skills in detecting, analyzing, and managing computer security incidents, including investigation procedures, coordination with stakeholders, and communication of findings.

• Network Security: This training will enable engineers to comprehend the basics of network security, including communication protocols, firewall design and implementation, intrusion detection, and protection against denial-of-service attacks.

2.2.8.1.3 Advanced Level

• Application Security: This training will empower engineers to grasp the major security challenges related to web and mobile applications, including common vulnerabilities, secure coding practices, and intrusion testing techniques.

• Data Security: This training will enable engineers to understand the primary security challenges concerning data management, including cryptography, key management, privacy protection, and regulatory compliance

2.2.8.2 Artificial Intelligence (AI)

2.2.8.2.1 Beginner Level

• Introduction to AI: This training will enable engineers to grasp the basic principles of AI, including different types of machine learning algorithms, natural language processing techniques, computer vision, as well as the most common applications.

• Databases and Machine Learning: This training will help engineers understand how data is used to train machine learning models, including data manipulation, normalization and data transformation, as well as feature selection.

2.2.8.2.2 Intermediate Level

• Deep Learning: This training will enable engineers to understand the principles of deep learning, including neural networks, deep network architectures, backpropagation, as well as optimization techniques.

• Advanced Natural Language Processing: This training will enable engineers to understand advanced natural language processing techniques, including speech recognition, machine translation, text generation, as well as sentiment analysis.

2.2.8.2.3 Advanced Level

• Reinforcement Learning: This training will enable engineers to understand the principles of reinforcement learning, including policies, value functions, search algorithms, as well as applications in robotics and games.

• AI Ethics: This training will help engineers understand the ethical issues related to AI, including transparency, accountability, fairness, as well as social, economic, and political implications

2.2.8.3 Complementarity of AI & Cybersecurity

2.2.8.3.1 Beginner Level

• Introduction to Cybersecurity: This training will enable engineers to grasp the basic principles of cybersecurity, including common threats, vulnerabilities, security attacks, as well as prevention and protection measures.

• Basics of AI for Cybersecurity: This training will enable engineers to understand the principles of AI applied to cybersecurity, including machine learning techniques, anomaly detection algorithms, recommendation systems, and real-time monitoring.

2.2.8.3.2 Intermediate Level

• AI Security: This training will enable engineers to understand the security threats and risks related to AI, including data manipulation, model attacks, data confidentiality and integrity, as well as algorithm robustness.

• Advanced Cybersecurity with AI: This training will enable engineers to understand advanced cybersecurity techniques with AI, including fraud detection, identity and access management, user behavior analysis, and automated security incident response.

2.2.8.3.3 Advanced Level

• Ethics and Cybersecurity: This training will enable engineers to understand the ethical issues related to AI and cybersecurity, including transparency, accountability, fairness, as well as social, economic, and political implications.

• Security of Intelligent Systems: This training will enable engineers to understand advanced security techniques for intelligent systems, including secure architectures, confidentiality and privacy protection mechanisms, as well as certification and compliance approaches.

The goal of these integrated training programs (in cybersecurity and AI) is to help EDIH engineers acquire advanced skills in cybersecurity and AI and understand the synergies between these two domains to ensure robust and resilient security

2.2.8.4 Internet of Things (IoT)

2.2.8.4.1 Beginner Level

• Introduction to IoT: This training will enable engineers to understand the basic principles of IoT, including architectures, communication protocols, sensors, actuators, and security protocols. • IoT Application Development: This training will enable engineers to understand the basics of IoT application development, including programming languages, development platforms, and application development tools.

2.2.8.4.2 Intermediate Level

• IoT Security: This training will enable engineers to understand the security risks and threats related to IoT, including device vulnerabilities, network attacks, denial-of-service attacks, man-in-the-middle attacks, as well as security measures to protect them.

• IoT Data Analytics: This training will enable engineers to understand the basics of IoT data analytics, including machine learning techniques, forecasting models, real-time data analysis, and data visualization tools.

2.2.8.4.3 Advanced Level

• IoT Architecture: This training will enable engineers to understand advanced architectures for IoT systems, including distributed processing systems, real-time data processing systems, and security architectures.

• Industrial IoT: This training will enable engineers to understand the applications of IoT in industry, including machine monitoring, predictive maintenance, production quality, as well as supply chain and logistics management systems

2.2.8.5 Linking AI, Cybersecurity, and IoT

2.2.8.5.1 Beginner Level

• Fundamentals of IT, Cybersecurity, and AI: This training will enable engineers to understand the basic concepts of IT, cybersecurity, and AI, including architectures, protocols, programming languages, security models, and machine learning models.

• Basic Tools and Technologies: This training will enable engineers to understand the basic tools and technologies used in IT, cybersecurity, and AI, including operating systems, databases, networks, software development tools, intrusion detection tools, and data analysis tools.

2.2.8.5.2 Intermediate Level

• AI Security: This training will enable engineers to understand the risks and threats related to AI security, including algorithm vulnerabilities, adversarial attacks, privacy protection, and security measures to protect AI systems.

• Advanced Data Analysis: This training will enable engineers to understand advanced data analysis techniques, including machine learning techniques, forecasting models, real-time data analysis, and advanced data visualization tools.

2.2.8.5.3 Advanced Level

• IT, Cybersecurity, and AI Security Architecture: This training will enable engineers to understand advanced security architectures for IT, cybersecurity, and AI systems, including distributed processing systems, real-time data processing systems, and advanced security architectures.

• Advanced IT, Cybersecurity, and AI Projects: This training will enable engineers to work on advanced projects in the fields of IT, cybersecurity, and AI, including the development of advanced security systems, real-time data analysis, image recognition, and predictive modeling

2.2.8.6 Criteria for Classifying the Proposed Training Levels

To define the classification of each level of the proposed trainings, the following criteria can be used:

• Beginner Level: This category of training is aimed at those who have little or no prior knowledge in the field. Beginner-level trainings should cover the basic concepts and fundamental tools necessary to understand the domain.

• Intermediate Level: This category of training is aimed at those who have basic knowledge in the field and wish to deepen their skills. Intermediate-level trainings should cover more advanced and technical topics.

• Advanced Level: This category of training is aimed at those who have professional experience in the field and wish to develop advanced skills. Advanced-level trainings should cover specialized and technical subjects.

Additional criteria that can be used to define the training levels may include:

• Complexity of Covered Topics: The topics covered in each level of training may vary in terms of complexity and difficulty.

• Depth of Acquired Knowledge: The training levels may also vary in terms of the depth of acquired knowledge. Beginner levels may be more superficial, while advanced levels may focus on more specialized and in-depth subjects.

• Level of Practice: The training levels can also vary in terms of practice and practical experience gained. Beginner levels may focus on basic exercises, while advanced levels may involve complex projects and real-world use cases.

By using these criteria, it is possible to define appropriate training levels for different target audiences and ensure that the proposed trainings meet the needs of each level.

3 Regional Academic Mapping of Cybersecurity, AI and IoT Education

3.1 Unevenly distributed training offer for middle and senior management in the region of Hauts de France

3.1.1 Location of universities offering courses in the fields of cybersecurity, IoT, and AI

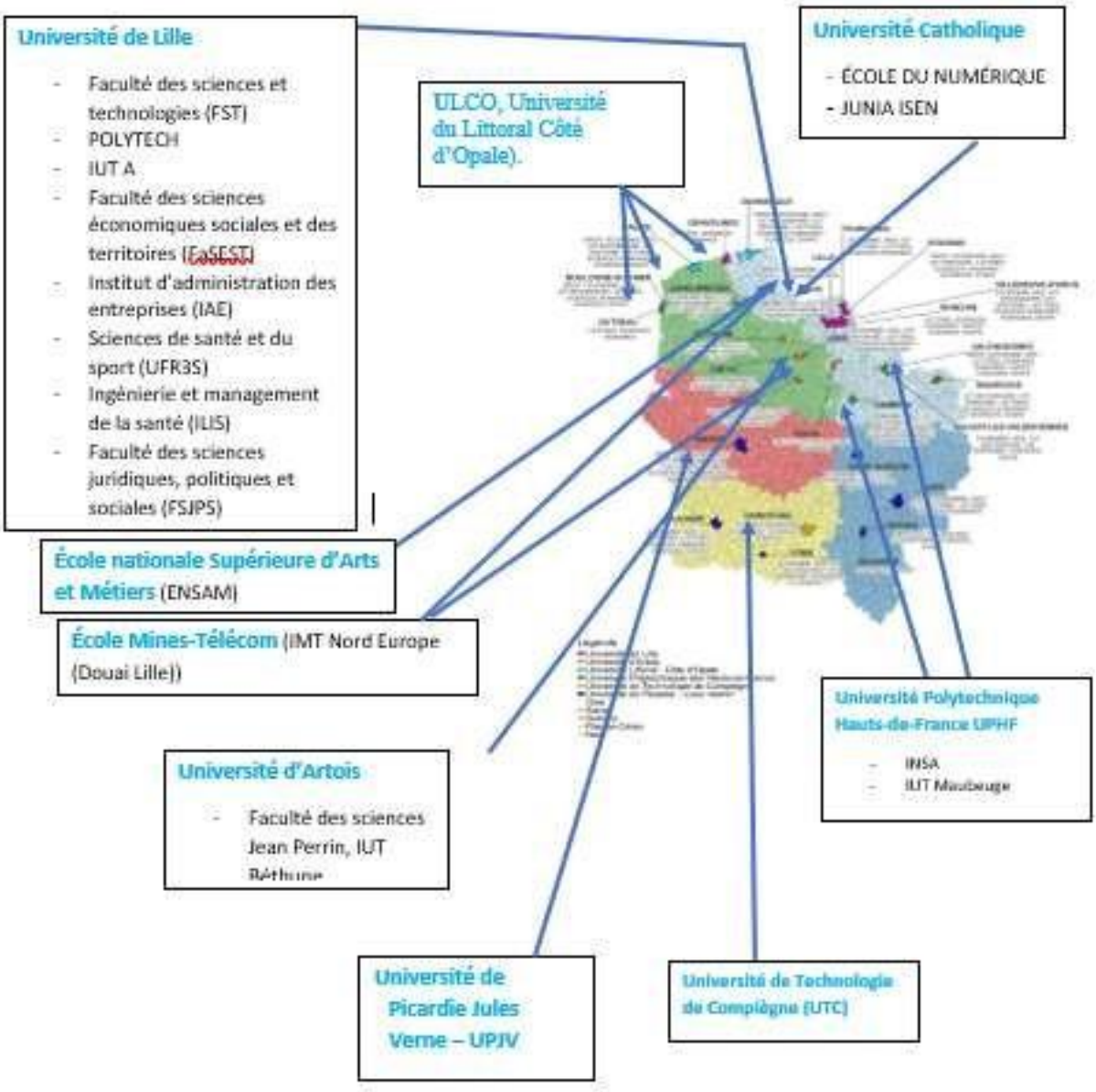

Figure 1 Map of the Universities offering courses in the fields of Cybersecurity, IoT and AI

3.1.2 Typology and characteristics of university training offerings

Universities offer courses in the fields of cybersecurity, IoT, and AI:

- Academic programs such as the Diploma of Scientific and Technical University Studies (DEUST), the University Bachelor of Technology (BUT), the Bachelor's degree and the Professional Bachelor's degree, the Master's degree and the Engineering degree, and specialized Master's degrees. These programs are:
  - Organized into competency-based blocks,
  - Providing opportunities for company internships,
  - Taught by industry professionals.

- Specific job-oriented programs that align with the region's needs:
  - Certifying programs: University Diploma (DU), University Certificate (CU), Professional Certificate, organized into competency-based blocks,
  - Qualifying or short, highly specialized programs, focused on specific industries, available in a catalog or tailored to address identified and highly specific economic demands

3.1.3 University training offerings in the Hauts de France region

The universities in the Hauts de France region offer 65 courses in these 3 fields

Trainings	Number of programs
Licences	10
Licences professionnelles	2
DEUST	1
CU	3
Certificat professionnel	1
DU	3
Offres courtes	3
BUT	7
Masters	26
Ingénieurs	7
Mastères	2

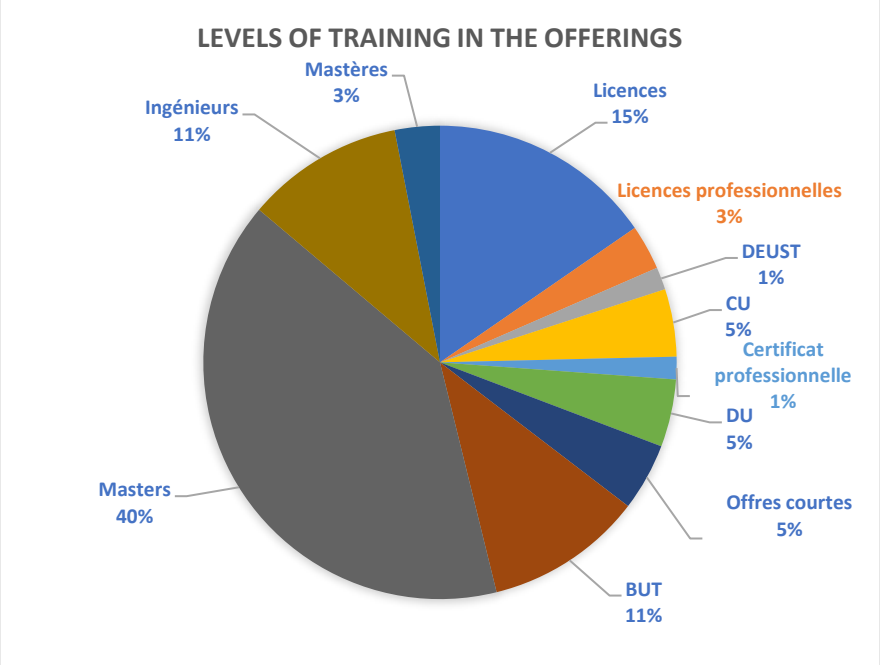

Figure 2 Levels of training in the offerings

- 54% of the cybersecurity, AI, and IoT training offerings in the Hauts de France region are designed for senior executives (from Bachelor's +5 to Bachelor's +6 level).
- 30% are aimed at middle management (from Bachelor's +2 to Bachelor's +3 level).

- 16% consist of highly specialized, job-oriented programs, varying in duration from a few days to 1 year, targeting both middle management and senior executive levels.
- 95% of the courses are certifying programs.

3.1.3.1 Intermediate management training programs

3.1.3.1.1 Bachelor's degrees (10)

Location of Bachelor's degree	Nb of programs
Université de Lille, 6 à la FST et 1 à l'ENSAM (LILLE)	7
Université Catholique ÉCOLE DU NUMÉRIQUE (LILLE)	1
Université d'Artois Faculté des sciences Jean Perrin (Lens)	1
UPHF INSA (Valenciennes)	1

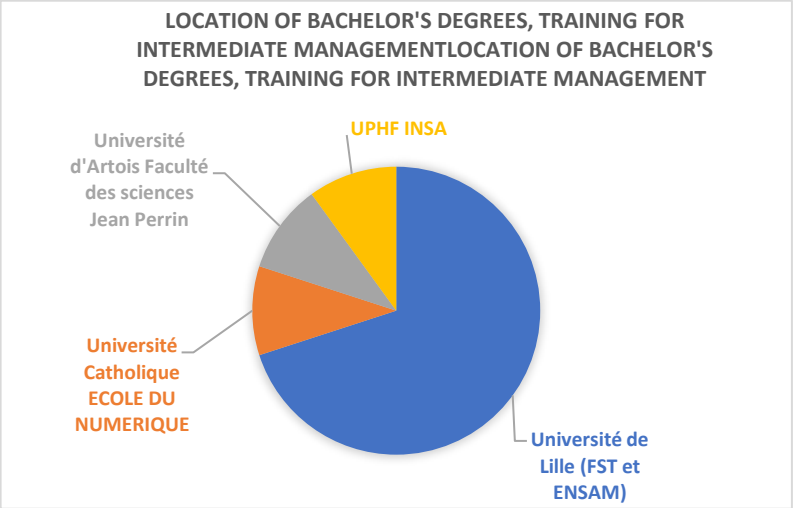

Figure 3 Location of Bachelor's degrees, training for intermediate management

The training offer for intermediate management at the bachelor's degree level (10 bachelor's degrees The range of training courses for middle managers at bachelor's level (10 bachelor's degrees in cybersecurity, AI and IoT) is mainly concentrated in the regional metropolis, with 6 bachelor's degrees for the University of Lille's FST, 1 for ENSAM and 1 for the Catholic University.

The other bachelor's degrees are located in Valenciennes (l'INSA Hauts-de-France, UPHF) and Lens (University of Artois, Jean Perrin Faculty of Science).

3.1.3.1.2 Other intermediate management level programs (10)

The other intermediate management level programs in cybersecurity, AI, and IoT are Professional Bachelor's degrees, University Technology Bachelor's degrees (BUT), and University Diploma of Scientific and Technical Studies (DEUST)

The other intermediate management level programs are half located in the Lille metropolis, while the rest are distributed across the Hauts de France region, with 2 in Maubeuge, 1 in Amiens, and 1 in Béthune.

Licences professionnelles	Nbre de parcours
UPHF INSA	1
UPJV Institut Universitaire de Technologie d'Amiens	1

BUT	Nbre de parcours
Université de Lille (IUT)	4
UPHF (IUT Maubeuge)	2
Université d'Artois (IUT Béthune)	1

DEUST	Nbre de parcours
Université de Lille (FST)	1

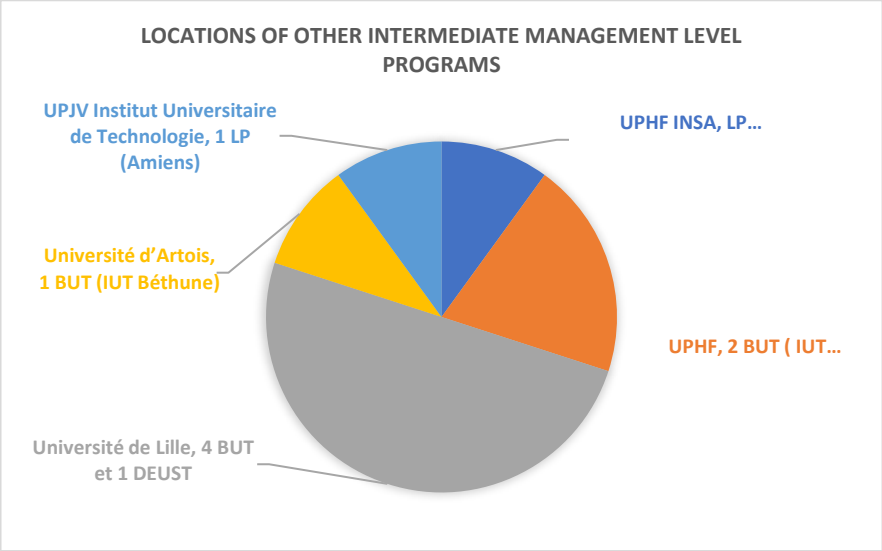

Figure 4 Locations of other intermediate management level programs

Half of the other middle management training courses are in the Lille metropolitan area, while the others are spread across the Hauts de France region: 2 in Maubeuge, 1 in Amiens and 1 in Béthune.

3.1.3.2 Senior management training programs

3.1.3.2.1 Masters (26)

Masters	Nb of programs
Université de Lille	18
Université d'Artois (LENS)	1
Université catholique (LILLE)	2
UPHF (VALENCIENNES)	2
UPJV (AMIENS)	1
ULCO (CALAIS)	2

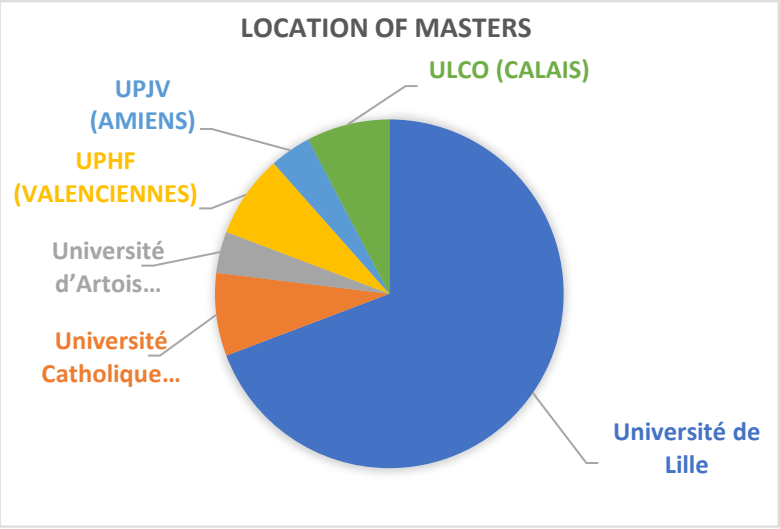

Figure 5 Location of masters

20/26 master's degrees in cybersecurity, AI and IoT are located in Lille: 17 are prepared at the University of Lille (10 for the FST + 1 at the FSJPS, 1 at the FaSEST + 3 at the IAE + 2 at the ILIS), 1 at the ENSAM site in Lille and 2 at the Catholic University, in the digital school.

UPHF INSA, located in Valenciennes, and the University of Littoral Côte d'Opale-ULCO, situated in Calais, each offer 2 masters. The offerings are complemented by 1 master each at Amiens (University of Picardy Jules Verne - UPJV) and Lens (University of Artois, Jean Perrin Faculty of Science).

3.1.3.2.2 Engineering programs (7) and specialized master's programs (2)

Engineers	Nb of programs
Junia ISEN, Université catholique de Lille.	3
Polytech, Université de Lille	2
IMT Nord Europe (Lille)	1
l'INSA Hauts-de-France, UPHF (Valenciennes)	1

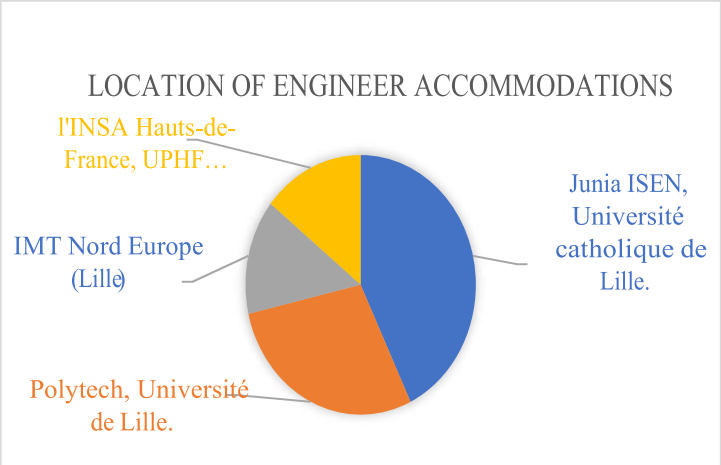

Figure 6 Location of engineering programs

6 /7 engineering courses in cybersecurity, AI and IoT are prepared in 3 engineering schools in Lille (2 courses for Polytech from the University of LILLE, 1 for IMT Nord Europe Lille, then 3 for Junia ISEN from the Catholic University. The seventh engineering course is offered by UPHF's INSA Hauts de France in Valenciennes.

The offer is completed by 2 post-engineering courses (specialised Masters), one offered by ENSAM and the other by IMT, all located in the Lille metropolitan area.

3.1.3.2.3 Shorter, highly specialized, job-oriented programs, ranging from intermediate management to senior management level

3 University Diplomas (DU): 2 from the University of Lille (University of Lille FSJPS + UFR3S), 1 from the Catholic University of Lille (FGES – School of Digital Technologies),

- 1 Professional Certificate from the University of Lille IMT Nord Europe (Lille),
- 3 University Certificates (CU) from the University of Artois (Lens),
- 3 short programs from UTC (Compiègne).

These programs, varying in duration from a few days to 1 year, highly specialized, and ranging from intermediate management to senior management level, are mostly located in the Lille metropolis, while the rest are distributed across the Hauts de France region (3 in Lens and 3 in Compiègne).

3.1.3.3 Intermediate conclusion

It can be observed that the training offerings in cybersecurity, AI, and IoT are unevenly distributed across the region. They are primarily concentrated in the Lille area.

These data need to be cross-referenced with the locations of companies operating in these sectors of cybersecurity, AI, and IoT, as well as their skill requirements. To do this, we will rely on the data from the "BMO" (Besoin en Main-d'œuvre) surveys conducted by Pôle emploi, which, although not highly specific, will provide us with an indication.

3.1.4 The employment needs of the region

3.1.4.1 Intermediate management job needs in the 'IT professions' in the Hauts de France region according to Pôle emploi's BMO

According to Pôle emploi's BMO, the number of recruitment projects in 2023 for IT study and development technicians in the departments of the Hauts-de-France region is concentrated in the Nord department. It accounts for 89% of the jobs, and 82% of the jobs are located in the employment areas of Lille, Roubaix, and Tourcoing (92% of the jobs in the Nord department).

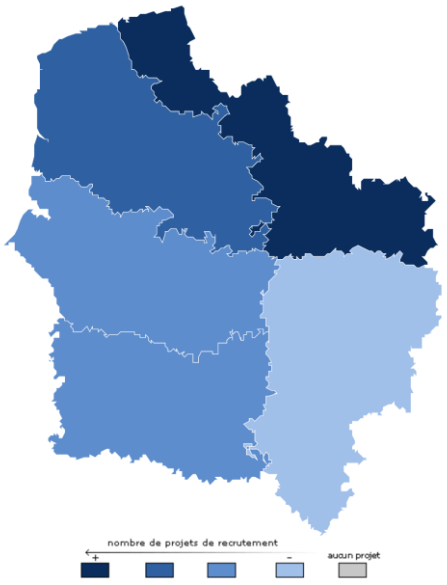

Figure 7 Number of recruitment projects in IT Professions in Hauts de France region

Department	Recruitment projects	%	Difficulties to recruit	Seasonal jobs
Nord 59	790	89	83,50 %	3,80 %
Pas-de-Calais 62	50	6	100,00 %	0,00 %
Somme 80	30	3	33,30 %	0,00 %
Oise 60	20	2	50,00 %	0,00 %
Aisne 02	10	1	100,00 %	0,00 %
Total	890	100	82,00 %	3,40 %

Employment area	Recruitment projects	%	Difficulties to recruit
LILLE	580	73	81,00 %

VERSANT N-EST ROUB.TOURC.	150	19	100,00 %
DOUAI	20	3	100,00 %
CAMBRESIS	10	1	100,00 %
VALENCIENNES	10	1	100,00 %
DUNKERQUE	10	1	100,00 %
SAMBRE AVESNOIS	10	1	0,00 %
FLANDRE LYS	0	0	-
Total	790	100	83,50 %

3.1.4.2 Intermediate management job needs in IT user support technicians in the Hauts de France region according to Pôle emploi's BMO

The recruitment projects for IT user support technicians in the departments of the Hauts-de-France region in 2023 are concentrated in the Nord department (82%), particularly in the employment areas of Lille, Roubaix, and Tourcoing (77% of the jobs in the region and 94% of the jobs in the Nord department).

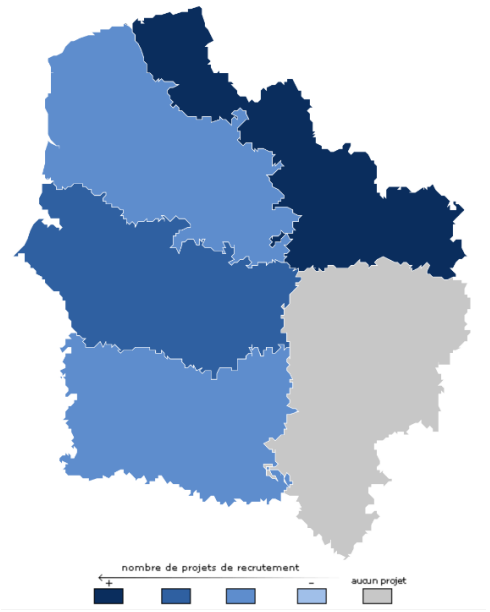

Figure 8 Number of recruitment projects in IT support technicians in Hauts de France region

Department	Recruitment projects	%	Difficulties to recruit	Seasonal jobs
Nord 59	490	82	75,50 %	6,10 %
Somme 80	70	12	28,60 %	0,00 %
Pas-de-Calais 62	30	5	66,70 %	0,00 %
Oise 60	10	2	100,00 %	0,00 %

Aisne 02	0	0	-	-
Total	600	100	70,00 %	5,00 %

Employment area	Recruitment projects	%	Difficulties to recruit
LILLE	410	84	80,50 %
VERSANT N-EST ROUB.TOURC.	50	10	60,00 %
DUNKERQUE	10	2	100,00 %
DOUAI	10	2	100,00 %
VALENCIENNES	10	2	0,00 %
FLANDRE LYS	0	0	-
Total	490	100	75,50 %

3.1.4.2.1 The employment needs for senior management positions in the "IT professions" in the Hauts-de-France region:

According to Pôle emploi's BMO, the recruitment projects in 2023 by department in the Hauts-de-France region for IT engineers, research and development managers, and IT project managers are concentrated in the Nord department (84%). In fact, 83% of the region's jobs are concentrated in the employment area of LILLE ROUBAIX TOURCOING, accounting for 98% of the needs in the Nord department.

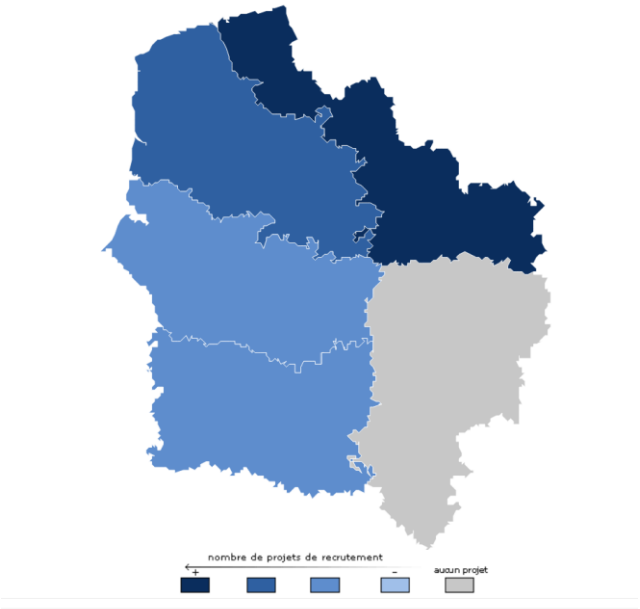

Figure 9 Number of recruitment projects for IT engineers, R&D managers and IT project Managers in Hauts de France Region

Department	Recruitment projects	%	Difficulties to recruit	Seasonal jobs
Nord 59	2 190	84	**76,30 %**	0,90 %
Pas-de-Calais 62	170	7	**35,30 %**	0,00 %
Somme 80	130	5	30,80 %	0,00 %

Oise 60	120	5	75,00 %	0,00 %
Total	2 610	100	70,90 %	0,80 %

Employment area	Recruitment projects	%	Difficulties to recruit
LILLE	410	84	80,50 %
VERSANT N-EST ROUB.TOURC.	50	10	60,00 %
DUNKERQUE	10	2	100,00 %
DOUAI	10	2	100,00 %
VALENCIENNES	10	2	0,00 %
FLANDRE LYS	0	0	-
Total	490	100	75,50 %

The number of recruitment projects in 2023, by department in the Hauts-de-France region, for IT engineers and administrative and maintenance managers, is concentrated in the Nord department, particularly in the employment area of LILLE ROUBAIX TOURCOING (90%).

Figure 10 Number of recruitment projects for IT engineers and administrative and maintenance managers in Hauts de France region

Department	Recruitment projects	%	Difficulties to recruit	Seasonal jobs
Nord 59	90	90	88,90 %	0,00 %
Pas-de-Calais 62	10	10	100,00 %	0,00 %
Somme 80	10	10	100,00 %	0,00 %
Total	100	100	100,00 %	0,00 %

Employment area	Recruitment projects	%	Difficulties to recruit

LILLE	80	88,89 %	100,00 %
VERSANT N-EST ROUB.TOURC.	10	11,11 %	100,00 %
Total	90	100,00 %	88,90 %

In conclusion, according to the data from Pôle emploi's BMO, whether it is for intermediate management or senior management positions, the workforce needs in the field of IT are primarily concentrated in the Nord department, particularly in the Lille region. This aligns with the training offerings provided by universities in the targeted fields of our study.

3.2 A training offer for intermediate and senior management, with diversified levels of specialization and expertise

While there are programs specifically focused on AI, cybersecurity, or IoT, the majority of the programs address these three domains with varying degrees of expertise. Therefore, we will present the level of expertise in each domain for each program offered by the universities using a table, and then illustrate it with a histogram graph.

The training offer is classified according to:

- The type of program: generalist, specialized, and career-oriented or focused on specific application areas
- The type of profile trained: intermediate or senior management

Nearly half, 48% of the training offerings in AI, cybersecurity, and/or IoT, are specialized programs, and more than a third (37%) are generalist programs.

Specialized programs in Cybersecurity, AI, and/or IoT	31
More generalist programs in Cybersecurity, AI, and IoT	24
Career-oriented specialized programs in AI for certain application areas	8
Programs on the environment of Cybersecurity, AI, and IoT	2

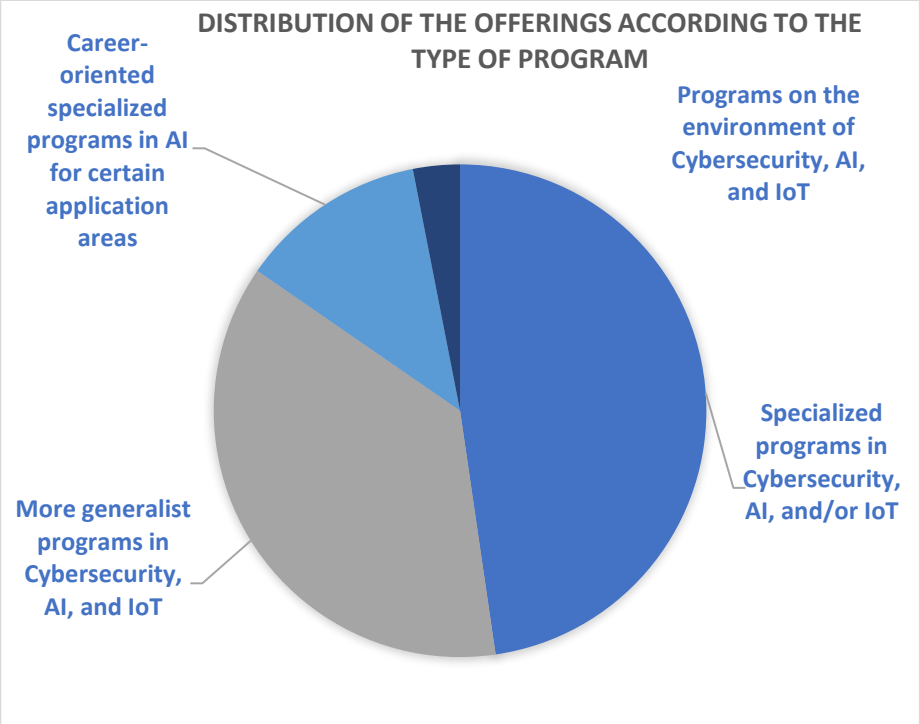

Figure 11 Distribution of the offerings according to the type of program

Training modalities:

- 13 programs available in both full-time and continuing education formats.
- 1 program available in both apprenticeship and continuing education formats.
- 4 programs available in apprenticeship format.
- 7 programs available in continuing education format
- 3 programs offered only in full-time education format.
- 7 programs available in both full-time education and apprenticeship formats.
- 26 programs available in full-time education, apprenticeship, and continuing education formats simultaneously

- 4 programs without information on the modalities.

3.2.1 Generalist programs in Cybersecurity, AI, and/or IoT

3.2.1.1 Intermediate management level programs

Programs	AI	Cybersecurity	IoT
DEUST « Infrastructures numériques », Université de Lille FST			
BUT informatique, parcours A : « Réalisations d'applications : conception, développement, validation ». UPHF IUT Maubeuge	2	2	2
BUT INFORMATIQUE, parcours « Réalisation d'applications : conception, développement, validation ». Université de Lille IUT	2	2	2
BUT GEII « Automatique et informatique industrielle ». Université de Lille IUT	1	2	1
LICENCE PROFESSIONNELLE : « MÉTIERS DES RÉSEAUX, INFORMATIQUE ET TÉLÉCOMMUNICATION - RÉSEAUX ET GÉNIE INFORMATIQUE ». Université de Picardie Jules Verne - UPJV IUT d'Amiens.	2	2	2
Licence professionnelle « Réseaux et Télécommunications ». UPHF INSA		1	1
Licence informatique. Université d'Artois, Faculté des sciences Jean Perrin	3		
Licence informatique. UPHF INSA	1	1	1
Licence informatique « MI (MATHS-INFO) ». Université de Lille, FST Département informatique.	1	1	1
Licence MIASHS. Université de Lille FST, Département mathématiques.	1	1	1
Licence informatique, parcours INFO. Université de Lille FST.	1	1	1
Licence informatique, parcours INFO renforcé recherche. Université de Lille FST.	2	1	1
Licence informatique Parcours MIAGE. Université de Lille FST.	1	1	1
Licence informatique-mathématiques. Université de Lille FST.	1	1	1

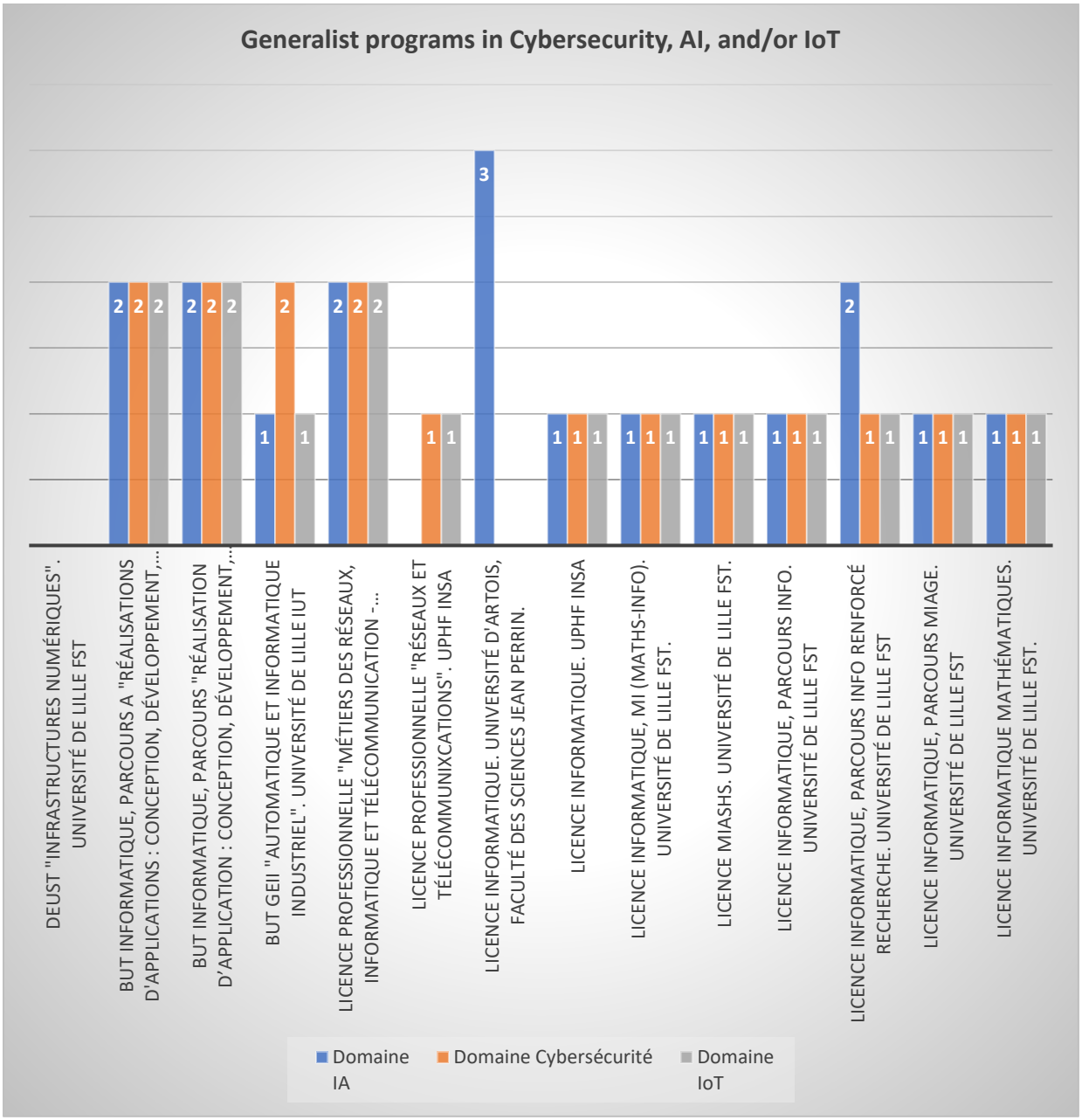

Figure 12 Generalist programs in Cybersecurity, AI, and/or IoT

A middle manager can be at best expertise level 2 (intermediate). In the proposed training offer, 2 BUT and 1 pro license train, depending on the options chosen by the learners, professionals with intermediate expertise in the 3 fields. 2 IT licenses, the INFO reinforced research course from the University of Lille FST and the IT license from the University of Artois, train professionals with level 2 expertise in AI. The other training courses are at level 1 of expertise in the 3 areas.

3.2.1.2 Senior management level programs

Programs	AI	Cybersecurity	IoT
Master « INFORMATIQUE », parcours « Génie logiciel : Conception, développement, agilité, DevOps, mobile, web, cloud, full stack, micro-services. Université de Lille FST.	2	2	1
Master « INFORMATIQUE », parcours 'E-services, conception, développement, UX, IHM, agilité, devops, mobile, web, centré utilisateur'. Université de Lille FST.	2	2	1
Master « INFORMATIQUE », parcours 'Réalité virtuelle Image, vision, IHM, 3D, informatique graphique'. Université de Lille FST.	2	1	1
Master MIAGE, parcours 'IPI-NT Méthodes informatiques appliquées à la gestion des entreprises, ingénierie de projets, nouvelles technologies'. Université de Lille FST.	2	1	1
Master Bio-informatique, parcours MISO 'S'orienter vers la bio-informatique et les biostatistiques'. Université de Lille FST.	2	1	1
Master 'Mathématiques et applications', parcours 'Scientific computing'. Université de Lille FST.	2	2	2
Master 'Informatique Ingénierie logicielle pour Internet, Intelligence artificielle et Ingénierie logicielle pour les Jeux'. Université d'Artois Faculté des sciences de Jean Perrin.	3		
Master "informatique Technologies nouvelles des systèmes d'information décisionnelle". UPHF INSA.	2	2	2
Master "Informatique Ingénierie des systèmes et réseaux informatiques". Université de Picardie Jules Verne - UPJV.		2	1
Ingénieur généraliste FISE - Domaine numérique. Université de Lille IMT	3	3	3

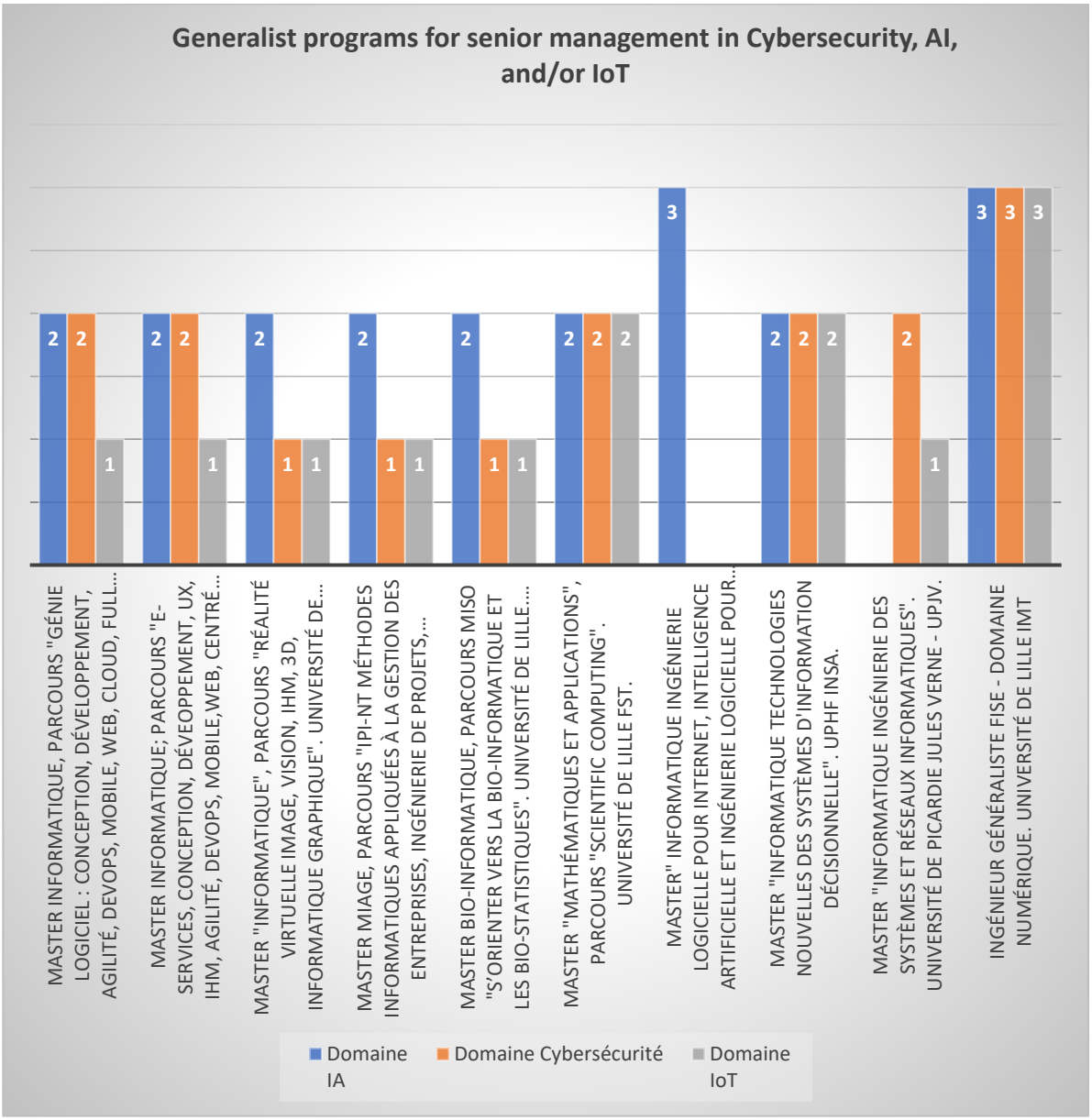

Figure 13 Generalist programs for senior management in Cybersecurity, AI, and/or IoT

8/10 training courses for senior executives from the general training offer in Cybersecurity, AI and/or IoT, training according to different degrees of expertise in the 3 areas. A master's degree only trains in cybersecurity and IoT, another only in AI.

Only one training course, “FISE Generalist Engineer - Digital Domain” from IMT Nord Europe, trains, depending on the engineering student's background, advanced level professionals in AI, cybersecurity or

IoT. A second training course trains advanced level experts in AI, this is the

Master’s degree in “Computer Science, Software Engineering for the Internet, Artificial Intelligence and Software Engineering for Games” from the University of Artois. All other training is at least intermediate level in 1, 2 or 3 areas.

3.2.2 **Specialized programs in Cybersecurity, AI, and/or IoT**

3.2.2.1 *Intermediate management level programs*

Programs	AI	Cybersecurity	IoT
BUT INFORMATIQUE, Parcours déploiement d'applications communicantes et sécurisées Université de Lille, IUT	1	2	1
BUT GEII « Électronique et Systèmes embarqués » Université de Lille IUT	1	1	2
BUT informatique, parcours B-Déploiement d'applications communicantes et sécurisées UPHF, IUT Maubeuge	1	3	2
BUT Réseaux et Télécommunications parcours Cybersécurité Université d'Artois, IUT Béthune		2	
Licence Sciences du Numérique Data, Maker, Gaming Université Catholique, ÉCOLE DU NUMÉRIQUE	2	2	2
Licence ROS pour développeur Université de Lille, ENSAM, Campus Lille	2	3	2
DU « Intelligence artificielle au service des entreprises » Université Catholique de Lille, FGES – ÉCOLE DU NUMÉRIQUE	1		

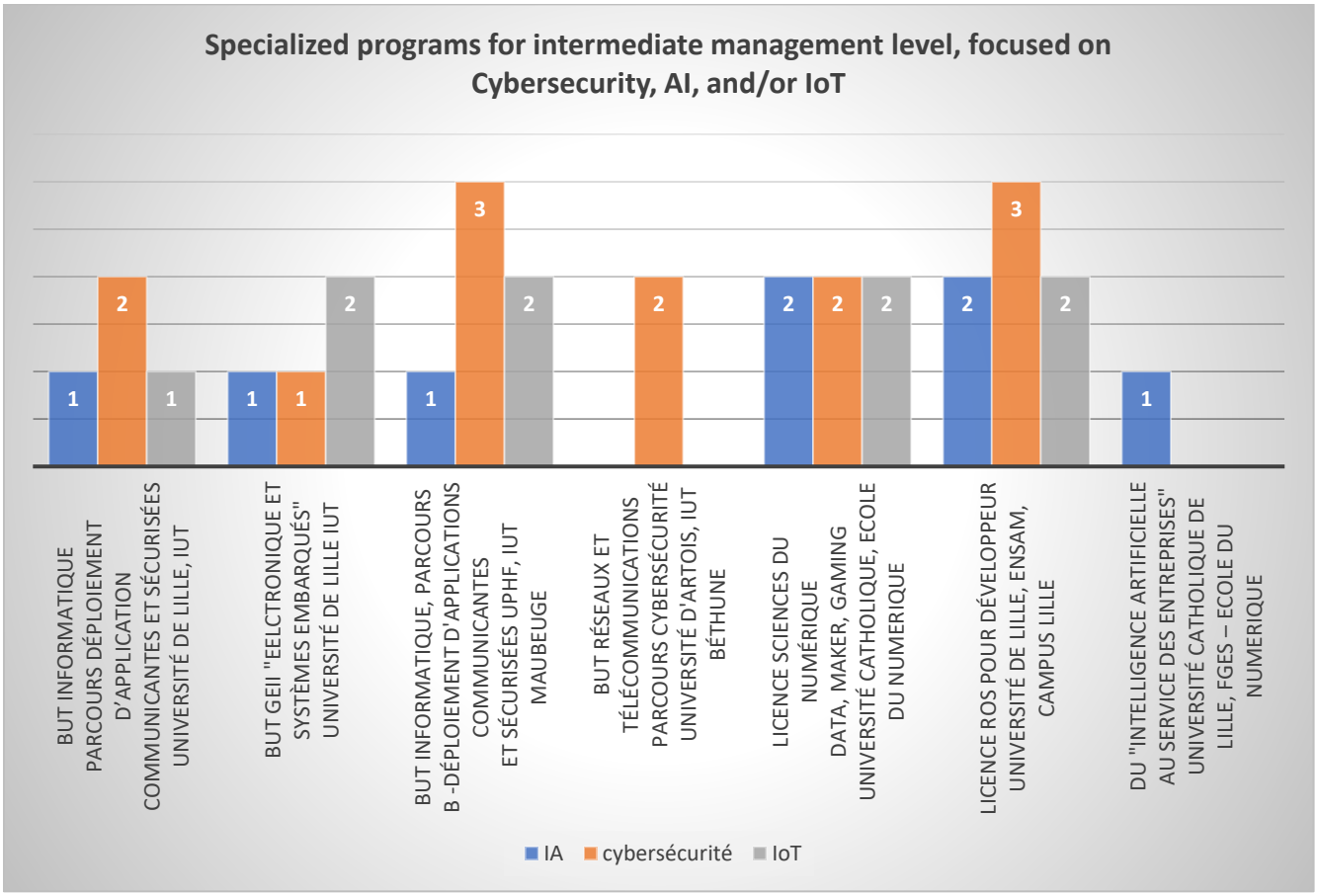

Figure 14 specialized programs for intermediate level in Cybersecurity, AI, and/or IoT

A middle manager can be at best expertise level 2 (intermediate). Depending on the options chosen by the learners, only the 2 licenses train middle managers on levels 2 of expertise in the 3 fields. 1 BUT trains level 2 middle managers in 2 areas, AI and IoT. The other 2 BUTs train level 2 middle managers in one of the fields, either in cybersecurity or in IoT. The DU trains level 1 professionals in AI.

3.2.2.2 Senior management level programs

Programs	AI	Cybersecurity	IoT
Master INFORMATIQUE Parcours « Cybersécurité et Cloud Computing » DevOps, sécurité, conception, déploiement, infrastructures Université de Lille, FST	2	3	2
Master INFORMATIQUE Parcours « Cybersécurité et Internet des Objets, Systèmes embarqués, réseaux de capteurs, web des objets, smart environnements, sécurité, systèmes temps réel » Université de Lille, FST	2	3	3
Master INFORMATIQUE, Parcours « machine Learning, apprentissage automatique pour la science des données, bases de données et algorithmique avancées » Université de Lille, FST	3	2	1

Master DATA SCIENCE, Parcours « DATA SCIENCE (international), Recherche en machine learning et intelligence artificielle, modèles mathématiques et algorithmes » Université de Lille, FST	3	1	1
Master management des systèmes d'information, parcours « systèmes d'information et aide à la décision » Université de Lille, FaSEST			
Master Cyber Université Catholique, ÉCOLE DU NUMÉRIQUE	1	3	
Master Data et IA Université catholique (FGES), ÉCOLE DU NUMÉRIQUE	3		
Master réseaux et télécommunications, Cybersécurité, défense des Systèmes d'information UPHF, INSA		3	
Master Informatique, Web et Science de données Université du Littoral - Côte d'Opale Ulco, SCIENCES & TECHNOLOGIES - SANTÉ/STAPS	3	1	2
Master Informatique, Web et Science de données Université du Littoral Côté d'Opale ULCO	3	3	2
Ingénieur informatique et statistique Université de Lille, POLYTECH	3	2	3
Ingénieur systèmes embarqués, Université de Lille, POLYTECH	3	2	3
Ingénieur ISEN domaine Cybersécurité Université Catholique, JUNIA ISEN		3	1
Ingénieur ISEN domaine Intelligence artificielle Université Catholique, JUNIA ISEN	2		
Master ROS pour développeur Université de Lille, ENSAM, Campus Lille	2	3	2
Ingénieur spécialisé informatique et cybersécurité UPHF INSA	2	3	2
Mastère spécialisé ingénierie de la cybersécurité Université de Lille, IMT	2	3	2
Mastère spécialisé, COLROBOT - Expert en robotique collaborative Université de Lille ENSAM, Campus Lille	3	1	3

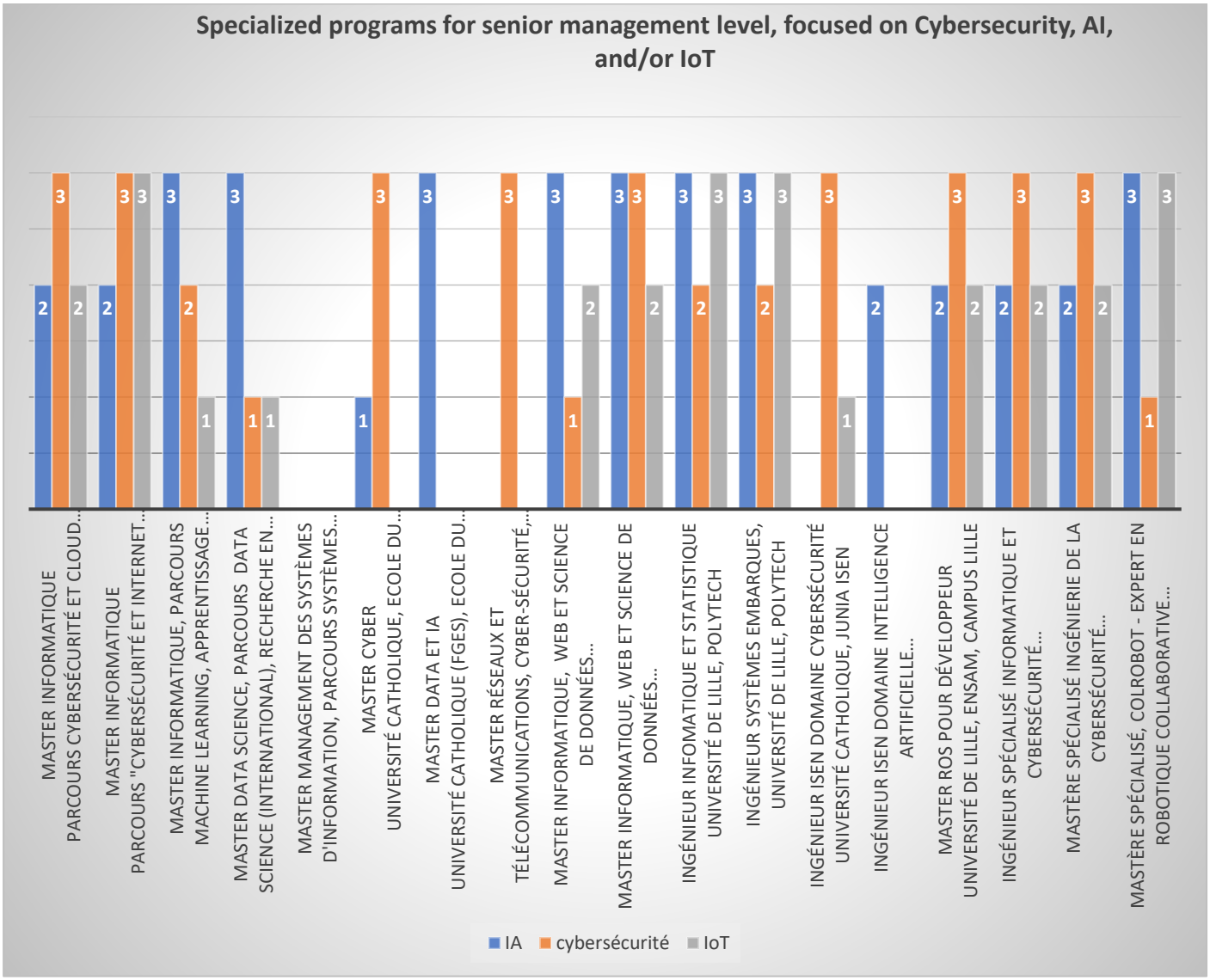

Figure 15 specialized programs for senior management level in Cybersecurity, AI, and/or IoT

None of these courses specialising in Cybersecurity, AI and/or IOT offer training for senior managers at advanced level in the 3 areas. On the other hand, depending on the options chosen by students, 4 of the 18 courses train experts to an advanced level in 2 of the 3 areas. Almost all of the courses train advanced-level experts in at least 1 of the 3 areas. There are more advanced training courses in cybersecurity (9 courses compared with 7 in AI), while there are far fewer advanced courses in IoT (4 courses). Does this correspond to the needs of companies? Is there a need to develop more advanced IoT training courses?

3.2.3 Specialized training in certain application areas

Specialized programs in AI for certain application areas	Number of programs	Course titles
Masters	5	**Master MARKETING VENTE, Université de Lille IAE :** • Parcours marketing et data science, ✓ Parcours Stratégie marketing et relation client. **Master Commerce et distribution, université de Lille IAE :** • Parcours commerce et distribution connectés. **Master INGÉNIERIE DE LA SANTÉ Université de Lille ILIS** (Faculté Ingénierie et Management de la Santé) : ✓ Parcours MIAS (co-accrédité Centrale Lille), ✓ Parcours data science en santé (DSS).
DU	1	**DU « INTELLIGENCE ARTIFICIELLE EN SANTÉ » Université de Lille, UFR3S**
Offre courte	1	**Introduction aux notions de cybersécurité, UTC université de Compiègne**
Ingénieur	1	**Ingénieur « GÉOMATIQUE ET GÉNIE URBAIN » Université de Lille, Polytech**

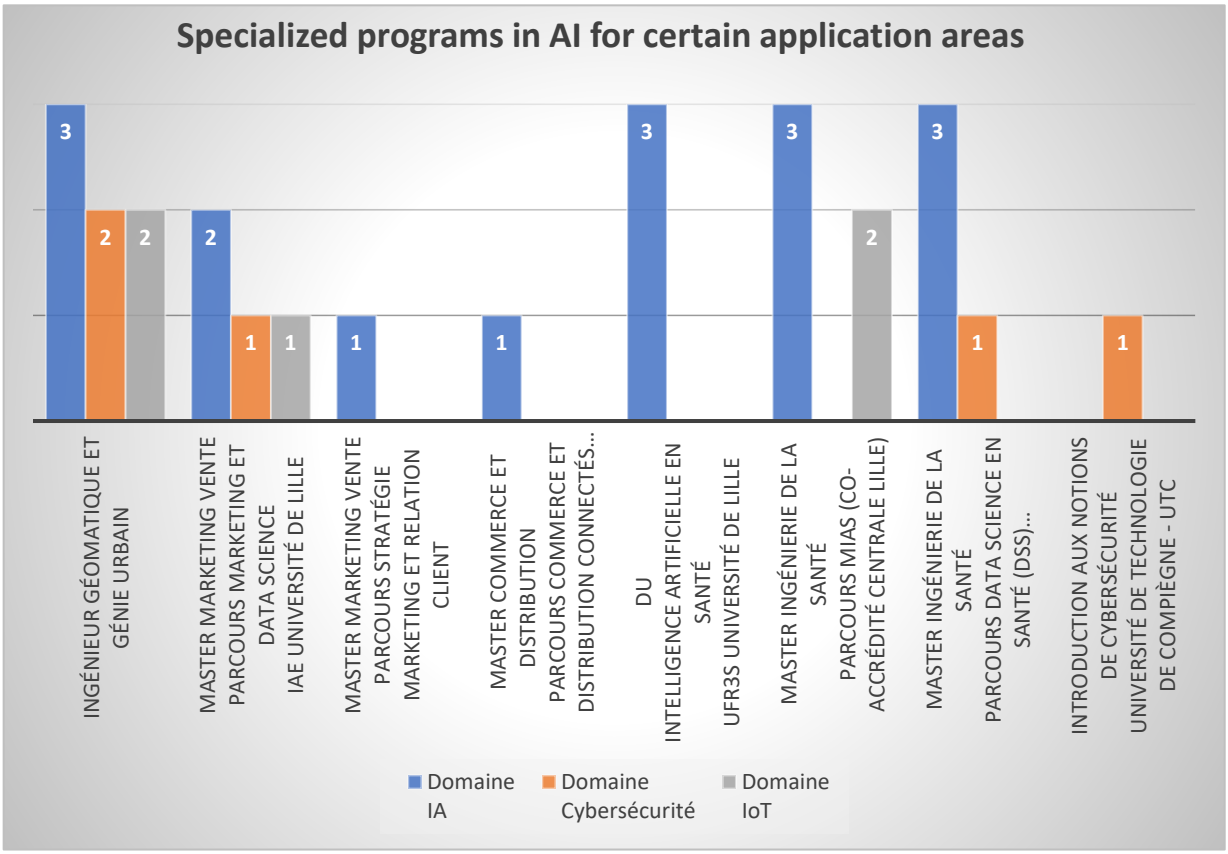

Figure 16 Specialized programs in AI for certain application areas

Only 1 of the specialized training courses for certain application areas is aimed at both middle and senior management: this is the course entitled "Introduction to cybersecurity concepts" at UTC Compiègne. The other 7 courses are aimed at senior managers.
-4 for advanced experts in AI, none in other fields.
-4 courses train intermediate-level cybersecurity professionals, 3 beginners.
-3 of these courses train IoT professionals, one at intermediate level, two at beginner level.

3.2.4 **Career-oriented programs in Cybersecurity, AI, and/or IoT**

3.2.4.1 Career-oriented programs in Cybersecurity, AI, and/or IoT

Programs	AI	Cybersecurity	IoT
CU « Concevoir et mettre en œuvre la sécurité informatique en entreprise » Université d'Artois	1	3	
CU « Data scientist » Université d'Artois	3		
CU « Technologie de l'information » Université d'Artois			
« Introduction aux notions de cybersécurité » Université de Technologie de Compiègne - UTC		1	
« Cybersécurité Risques et protection des systèmes d'information (RPSI) » Université de Technologie de Compiègne - UTC		1	
Certification professionnelle « Chef de Projet IA » Université de Lille IMT	1		

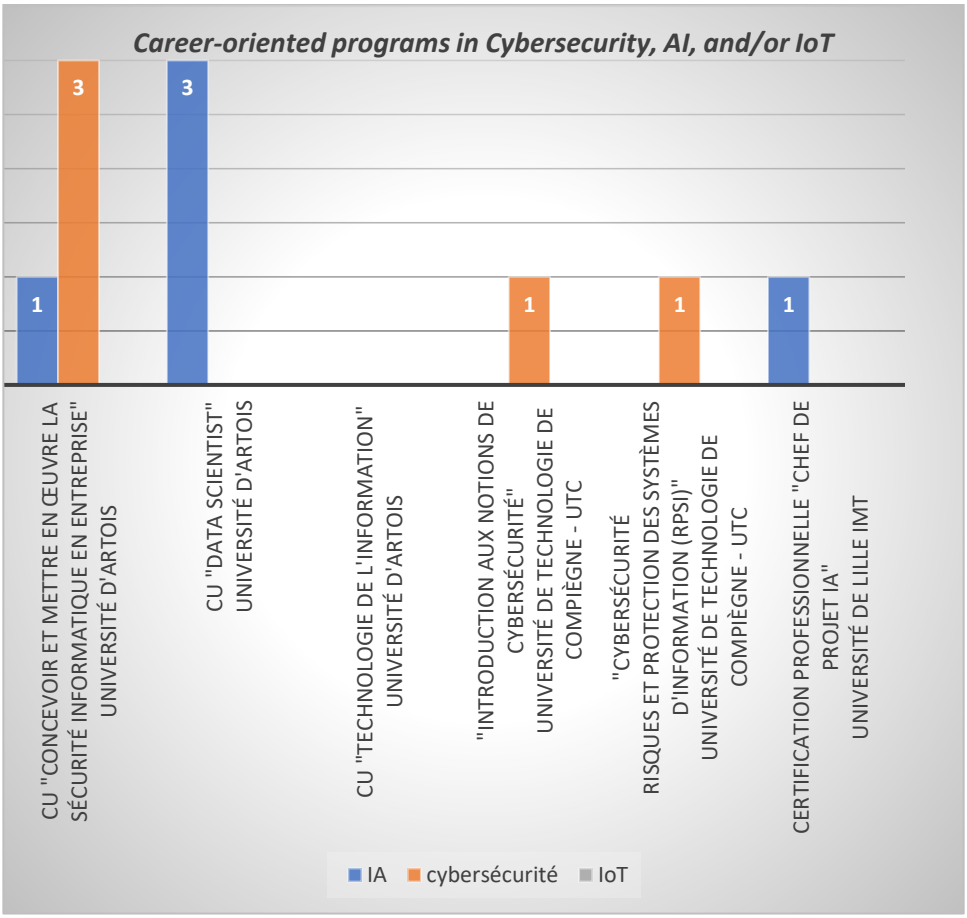

Figure 17 Career-oriented programs in Cybersecurity, AI, and/or IoT

2 programs train professionals with advanced expertise, one in cybersecurity, and the other in AI. The other training courses are for entry-level operators.

3.2.5 Programs on the environment of Cybersecurity, AI, and IoT

Programs	AI	Cybersecurity	IoT
Master DROIT NUMÉRIQUE, parcours droit du cyberespace : technologies et innovations numériques. Université **de Lille**	2	3	1
DU « INFORMATIQUE ET LIBERTÉS », parcours de l'informatique et des libertés. Université de Lille FSJPS (Faculté des sciences juridiques, politiques et sociales)		1	

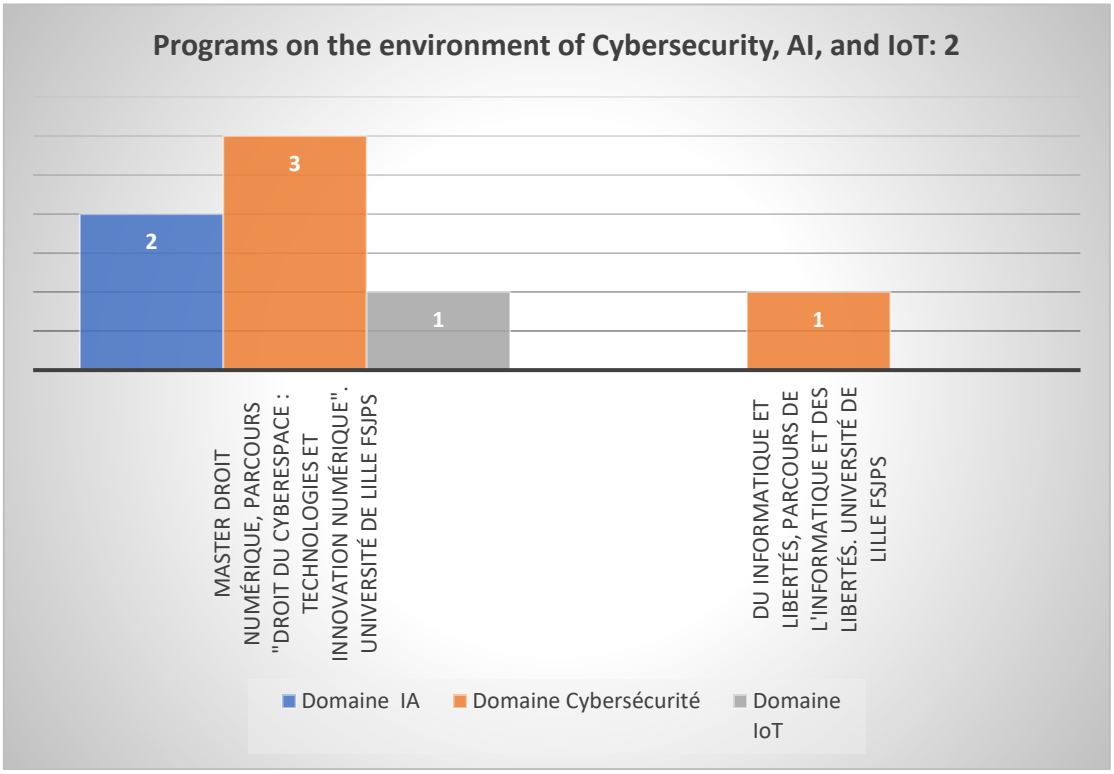

Figure 18 Programs on the environment of Cybersecurity, AI, and IoT

The master's degree in Digital Law, Cyberlaw: Digital Technologies and Innovations at the University of Lille, trains specialists in digital law, cybersecurity, AI and IoT. The 'DU' Informatics and liberties and the course informatics et liberties at the University of Lille FSJPS, focuses exclusively on cybersecurity law.

3.3 The current training offer provides the business world with university or specialized courses that allow customized training to adapt to the specific needs of companies

3.3.1 Characteristics of the programs offered by these universities: Diverse programs for all types of audiences

These universities are dedicated to providing education for:
• Full-time students,
• Apprentices,
• Employees pursuing continuing education.

Their programs cater to various audiences:
• Students,
• Apprentices,
• Employees,
• Job seekers and professionals seeking career change

3.3.2 University programs, specialized or customized, tailored to the needs

To address the needs of the business world, these universities can offer: • All or part of the accredited programs available in full-time education (Bachelor's, Master's, Doctorate), • Specialized programs (DEUST, University Technology Bachelor's, Professional Bachelor's, University Diplomas, and University Certificates, which are competency blocks of degrees, and professional certificates), • Customized training, certifying or non-certifying, co-created with a company or partners based on the competency blocks of multiple existing degrees, • Specially designed programs, co-created with partners to meet specific needs or to enhance the skills of employees or job seekers, • Short qualifying programs for rapid skills development.

The universities of Valenciennes and Catho Lille offer the "Licence Pluridisciplinaire Projet Personnel" (L3P), where students can choose their courses based on their personal projects, drawing from the subjects taught within these universities. Each student selects courses from the university catalogs according to their preferences. As a result, employees, job seekers, and individuals returning to studies can tailor a customized educational path in line with business needs and their professional projects. Employers can also create a tailored bachelor's program to meet the skill requirements for their intermediate management personnel.

3.3.3 Programs aligned with the business world, technological and scientific developments, often linked to research

To remain closely aligned with the business world, technological advancements, and scientific progress, these programs are:

- Linked to research,
- Led by academic researchers,
- Involving professionals who are experts in their respective fields.

Wherever possible, these programs take into account the constraints faced by employees.

3.3.4 **Prerequisites**

These programs often require prerequisites, such as a certain level of proficiency in mathematics and/or computer science or programming languages. Admission to academic programs typically demands specific diploma requirements. However, these proficiency requirements can be waived by engaging in a process of Validation of Prior Learning (VAE) or Validation of Acquired Professional Experience (VAPP).

3.4 **Conclusion on academic offerings**

The cartography provides an overview of the university training offerings in the fields of artificial intelligence, cybersecurity, and the Internet of Things in the Hauts de France region. The universities' training offerings in these domains are extensive and diverse. However, they are highly concentrated in the departments of Nord and Pas de Calais, particularly in the Lille metropolis. This geographical distribution of offerings appears relevant considering the location of employment needs.

The programs offered in the three domains, AI, cybersecurity, and IoT, cater to both intermediate and senior management positions. The offerings are more abundant for senior management roles. However, it seems that companies require more training for intermediate management positions. It would be worthwhile to investigate the intermediate management training offerings to determine if there is a need for further development.

Most of the programs offered do not solely specialize in AI, cybersecurity, or IoT. Instead, they approach these various domains with varying degrees of expertise depending on the curriculum.

We note that generalist training courses mainly train senior managers with intermediate or entry-level expertise (with the exception of the FISE - Digital Domain generalist engineering course at IMT Nord Europe, which, depending on the options chosen by the engineering students, trains senior managers with advanced levels in AI, cybersecurity and IoT, and the Master in Computer Science, Software Engineering for the Internet, Artificial Intelligence and Software Engineering for Games at the University of Artois, which trains senior managers with advanced levels in AI).

Middle managers are at best intermediate-level professionals. This is why the specialized training courses that train them are all at intermediate or beginner level in each of the fields.

As far as specialized courses for senior managers are concerned, none of them trains advanced-level professionals in any of the 3 fields. On the other hand, 4 of the 18 courses, depending on the options chosen by learners, train advanced-level experts in 2 of the 3 fields. Almost all courses train advanced experts in at least 1 of the 3 fields. These levels of training can meet skill requirements in all 3 areas.

The diversity and characteristics of academic, generalist and specialized training programs, as well as career-oriented training offered by universities in initial training, continuing education and work-study programmes are an initial response to the skills needs of the business world. The richness of this offer gives universities a great deal of flexibility in proposing tailor-made training courses, based on the skills blocks of existing diplomas, to offer training leading to certification, or with specific content, adapted to demand for training leading to qualifications.

4 Regional Private Trainings Mapping of Cybersecurity, AI and IoT Education

Important: This section does not list all the training programs exhaustively. It will be enriched gradually as the project progresses and partnerships are established.

4.1 Key institutions and organizations offering private trainings Cybersecurity, AI and IoT Education

We found it important to not only identify the offerings of the EDIH partners but also, more broadly, those of organizations present in the region. Several training programs and organizations have recently emerged to meet the specific needs of regional stakeholders.

4.1.1 EDIH partners

Several EDIH consortium partners offer training courses for awareness raising and personalised trainings:

CITC - IoT Cluster

The CITC gives training courses about the emerging technologies (embedded system, RFID, NFC, security, antennas design, connected objects conception, Internet of Things …)

Ref 1 https://iotcluster.fr/index.php/en/homepage/

INRIA – National Institute for Research in Digital Science and Technology

Inria aims to support the digital transformation of its ecosystems through education. Inria Academy now offers a training catalog consisting of four open-source software known for their international performance.

Ref 2 https://www.inria-academy.fr/

Chamber of Commerce Hauts-de-France Region

CCI proposes Tailor-made HR consulting and training for cybersecurity managers in SMEs.

Ref https://www.ccicampus.fr/bureautique-pao-informatique-web-cao/formation-referent-cyber-securite-en-tpepme

AMVALOR

AMVALOR offers awareness raising and tailor made trainings for experts and engineers: robotics, operational excellence, embedded AI.

Ref https://artsetmetiers.fr/fr

Likewise, IMT and UTC propose awareness raising and personalised trainings for SMEs.

4.1.2 Other organizations / Associations

Chambre de Métiers et de l'Artisanat Hauts de France

Established in 1925 and governed by artisanal business leaders, the CMA (Chambre de Métiers et de l'Artisanat) represents the general interests of the Crafts sector.

The CMA of Hauts-de-France carries out support missions, covering all stages of the artisanal business life. It also plays a crucial role in apprenticeship and continuous training.

From food and beauty trades to construction, healthcare, and more, with our comprehensive training catalog, you can update or develop new professional skills.

Ref 3 https://www.cma-hautsdefrance.fr/

CNAM Hauts de France

Cnam Hauts de France specializes in providing educational opportunities in Alternance (work-study programs) for young individuals under apprenticeship or professionalization contracts. Additionally, we excel in qualifying and retraining employees and job seekers throughout their professional lives.

Cnam Hauts-de-France operates 3 training centers in Amiens, Lille, and Valenciennes, along with around 30 other teaching locations spread across the Region.

We offer over 600 diploma or qualification programs ranging from high school level to bachelor's and master's degrees in various technical and tertiary specializations within the business domain. Furthermore, we cover areas related to social work and healthcare.

Ref 4 https://www.cnam-hauts-de-france.fr/presentation-du-cnam-hauts-de-france/

AFPI / CFAI

The AFPI, along with the CFAI, succeeded the ACM (Association de Formation Continue pour les Métiers) that has been in existence since 1949 and has emerged as a leading training organization for businesses, especially those in the metallurgical industry.

The AFPI, specialized in professional training, and the CFAI pool their resources to provide a comprehensive range of training programs, both for initial training and continuing education, tailored to the evolving needs of the company's professions.

The AFPI - Professional Training is present throughout the Nord-Pas de Calais region with 7 training centers: Lille Métropole (Marcq-en-Baroeul) ; Henin Beaumont ; Valenciennes ; Cambrai (Escaudoeuvres) ; Maubeuge (Feignies) ; Boulogne-sur-Mer (Saint-Martin-Boulogne) ; Saint-Omer ; Dunkerque. The head office of AFPI is located in Marcq-en-Baroeul.

Ref 5 https://www.afpi-acmformation.com/lafpi/

4.1.3 Companies , other training organizations

SkillS4All

Company, training organization with an e-learning catalog

Ref 6 https://www.skills4all.com/

Seela

Company, training organization with a speciality in Cybersecurity

Ref 7 https://seela.io/

Adaliance

Consulting company offering trainings in Cybersecurity

Ref 8 https://adaliance.com/training/la-cyber-securite/

IB Cegos

As an international leader in Learning & Development, the mission of the Cegos Group is to train individuals and support organizations in addressing their development challenges.

Ref 9 https://www.ib-formation.fr/qui-sommes-nous/raisons-de-choisir-ib

M2I Group

M2i Group has been a leading IT, Digital, and Management training provider in France for over 35 years.

Renowned for offering the most qualitative and comprehensive range of courses on the market, the group serves over 4,200 active clients, including major companies (Covéa, ATOS, Sopra Steria...), government agencies (Ministry of the Interior, DGFIP...), and numerous SMEs / ETIs.

Ref 10 https://www.m2iformation.fr/qui-sommes-nous/

FALCON ACADEMY

Company, training organization with an e-learning catalog

Ref 11 https://falconacademy.fr/

Pro Alterna / EPSI (Ecole Privée des sciences Informatiques Arras/Lille)

Pro Alterna / EPSI is a training organization and an Apprenticeship Training Center

Ref 12 https://www.proalterna-sarl.com/

CESI ASSO ARRAS / LILLE

CESI is a higher education and vocational training campus, comprising

Ref 13 https://www.cesi.fr/

e-Catalyst

Company, training organization in IT

Ref 14 https://e-catalyst.fr/

Institut Montaigne

The Montaigne Institute offers studies and debates on public policies for the common good. It is located at the confluence of reflection and action, ideas and decision-making.

Ref 15 https://www.institutmontaigne.org/initiatives/objectif-ia

SIMPLON.CO

School for digital professions

Ref 16 https://simplon.co/

Le Wagon Lille

Company, training organization in IT

Ref 17 https://www.lewagon.com/fr/about-us

ESGI formations

School with a program in computer science and a possible specialization in cybersecurity, IoT or IA

Ref 18 https://www.esgi.fr/ecole-informatique/programmes.html

SupInfo

School with a program in computer science and a possible specialization in cybersecurity, IoT or IA

Ref 19 https://www.supinfo.com/formations-metiers-informatique/master/

EPSI

School with a program in computer science and a possible specialization in cybersecurity, IoT or IA

Ref 20 https://www.epsi.fr/programmes/panorama-des-formations/

EPITECH

School with a program in computer science and a possible specialization in cybersecurity, IoT or IA

Ref 21 https://www.epitech.eu/fr/formations/epitech-en-5-ans/

4.2 Available Private Trainings Programs

60 trainings programs on AI; cybersecurity and IoT have been Identified

We cannot guarantee the completeness of this training catalog. We have compiled all of these training courses through iterative processes, starting with our first circle of partners and then expanding with the knowledge and contacts of the EDIH partners. However, we believe that this provides a first view of the private training ecosystem in the region.

The distribution of private training courses by theme is as follows. There are few specific courses tagged on IoT.

- 42 trainings programs in Cybersecurity
- 18 trainings programs in AI

- ✓ There are training programs for all levels, regardless of the prerequisites.
- ✓ Most of the trainings programs are eligible at CPF (Compte Personnel de Formation)
- ✓ Most of the programs are available in distance learning.
- ✓ The duration of the training varies, but they are primarily in-depth programs designed to prepare for a specific profession.

4.2.1 **Cybersecurity**

Organizations	**Number of Trainings**
CNAM Hauts de France	11
IB Cegos	9
CFAI	4
Chambre de Métiers et de l'Artisanat Hauts de France	2
e-Catalyst	2
INRIA	2
Adaliance	1
CESI	1
CITC	1
Falcon Academy	1
M2I	1
ProAlterna	1
Seela	1
SkillS4All	1
ESGI	1
SupInfo	1
EPSI	1
EPITECH	1

CNAM and IB CEGOS offer a large number of trainings in the region in Cybersecurity.
Among those trainings, few “first level” trainings to executive of non-IT employees.

Most of the programs are to acquire an intermediate level in cybersecurity, the focus is on the management of a security solutions and to be able to make technical choices and initiate a cybersecurity approach within the company. The offers are truly intended for candidates who already have a basic level in IT or network management.

Several high-level specialized training programs that train cybersecurity analysts capable of managing incidents and detecting vulnerabilities in the security system.

ESGI, SupInfo, EPSI and EPITECH are engineering schools in IT with a possible specialization in Cybersecurity

4.2.2 **Artificial Intelligence**

Organizations	**Number of Trainings**
Pro Alterna	6
SIMPLON.CO Hauts de France Roubaix	2

INRIA	2
Le Wagon Lille	1
Institut Montaigne	1
CNAM HAUTS DE France Lille/Valenciennes/Amiens	1
CITC	1
ESGI	1
SupInfo	1
EPSI	1
EPITECH	1

ProAlterna is a private school that offers several training programs in AI at various levels: Systems, Networks, and Database Administrator; AI and Data Science Developer; AI Developer. Depending on the type of training, it can be either initial training or continuous education. However, a prerequisite in computer science is required.

SIMPLON is also a private school that appears to offer a comprehensive curriculum on artificial intelligence (Machine Learning, Neural Networks) with a particular feature of providing a preparatory cycle to level up and lay the foundations for advanced AI courses.

ESGI, SupInfo, EPSI and EPITECH are engineering schools in IT with a possible specialization in AI

4.3 Conclusion

There is a private offering on cybersecurity and AI topics that is already extensive in the region. It can be challenging for an outsider to know which training to choose and how these courses are recognized in the job market. These programs most often prepare for specific professions and are less frequently focused on advanced or introductory training, such as awareness programs.

Several actors of the EDHI, including Inria and CITC, already have an initial offering of training, mainly short courses (few days of trainings). In this regard, their training stands out from the programs offered by other organizations and private schools.

5 Analysis of stakeholder's technological needs and requirements to build dedicated training programs not covered by the existing training programs offer

We have shared a questionnaire with public authorities and SMEs to better understand their training needs. About 44 local authorities and about 7 companies have replied to the questionnaire. Please find the questions and replies below.

5.1 Local authorities

5.1.1 What is your current level of knowledge of the following technologies?

- Data management
- Artificial Intelligence (AI)
- Internet of Things (IoT)
- Cybersecurity

BEGINNER [Red]: Little or no prior knowledge; Needs basic training to understand risks and good practice

INTERMEDIATE [Grey]: Basic knowledge acquired through courses or previous experience; Ability to implement simple measures/applications/projects

ADVANCED [Blue]: Solid knowledge acquired through in-depth study or professional experience; Ability to design and implement complex AI models / complex security strategies / complex and secure IoT systems

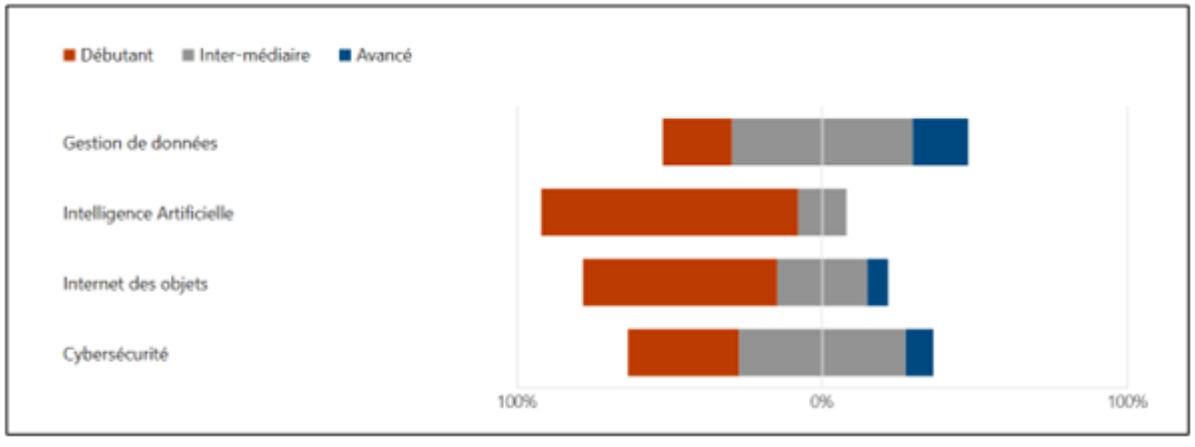

Figure 19 Level of knowledge of proposed technologies

2.1.2 **Which training have you already received? (Data management, Artificial Intelligence (AI), Internet of Things (IoT), Cybersecurity)**

About 50 percent have not been trained, 25 percent have been trained in data management, 20 percent on cyber security and about 1 percent have an academic background.

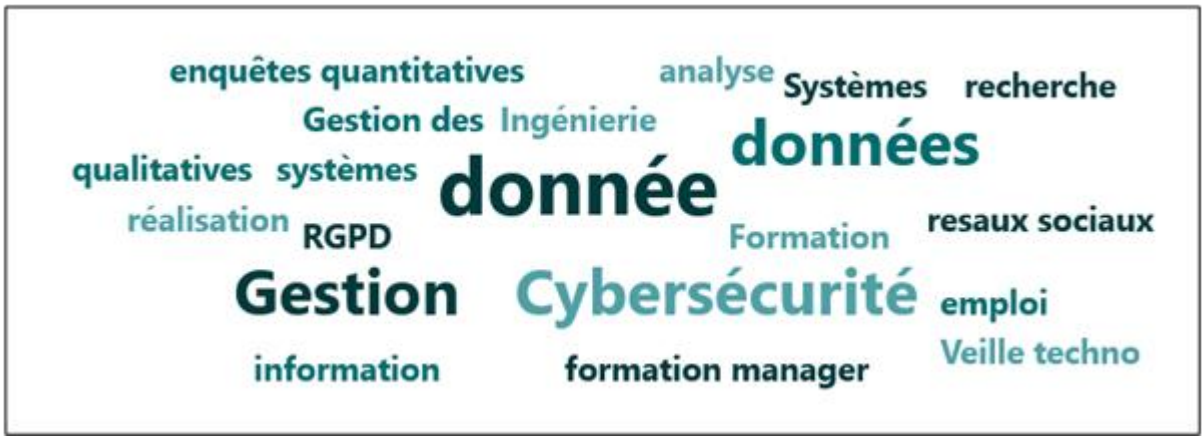

Figure 20 Level of knowledge of proposed technologies

5.1.2 **What training do you need?**

- Data management [blue]
- Artificial Intelligence (AI) [orange]
- Internet of Things (IoT) [green]
- Cybersecurity [red]
- Other [violet]

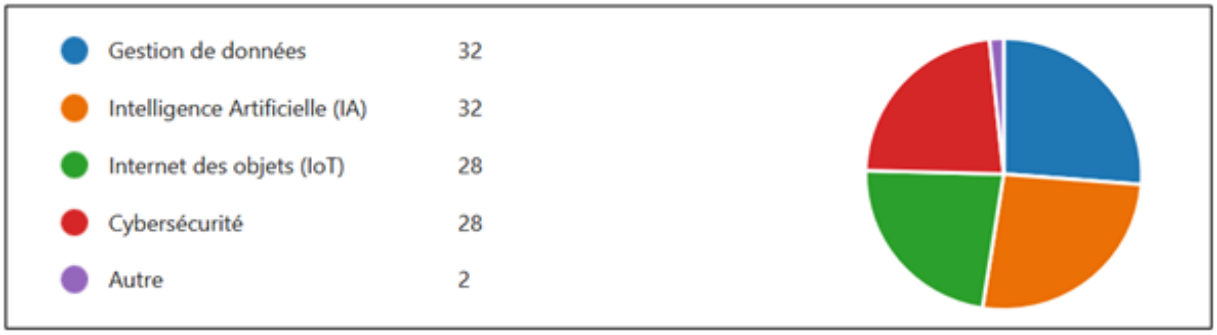

Figure 21 Training needs

Result for 'other [violet]*'*: Computer networks, Video surveillance

5.1.3 **Have you already identified specific training courses that meet your needs (in this area)?**

About 88 percent indicated they had not yet identified a specific training and about 12% were interested in a training course on

- CNFPT: Cybersecurity, cybersurveillance and data information systems security organisation" (code: SXSI5009)

- Windows Server and Active Directory

- Data governance, data quality, textual data processing, data enhancement, computer graphics

5.1.4 Ideally, what format should the training take to adapt to the work context?

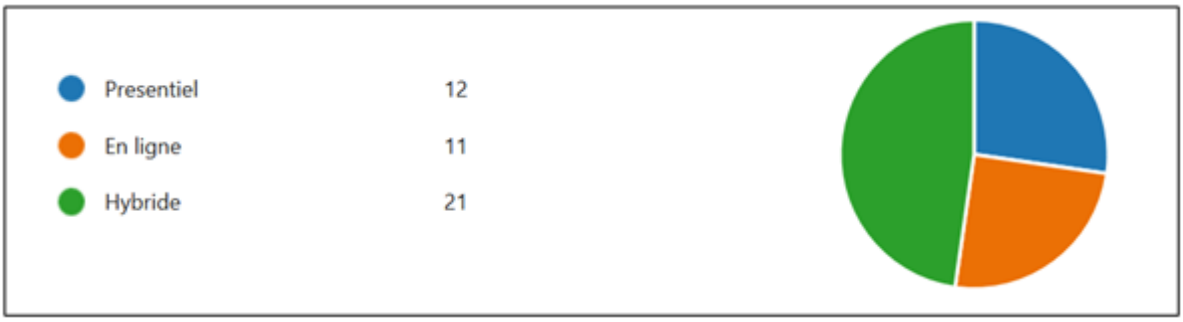

Figure 22 Training format

About 21 respondents prefer training in hybrid mode [green], 11 online [orange] and 12 in person [blue].

5.1.5 The availability of hours per months

- 1 - 3 hours: 6 participants
- 4 hours: 9 participants
- 8 hours: 6 participants
- 10 - 20 hours: 6 participants
- 21 - 35 hours and no limitation: 6 participants

5.2 SMEs

5.2.1 What is your current level of knowledge of the following technologies?

- Data management
- Artificial Intelligence (AI)
- Internet of Things (IoT)
- Cybersecurity

BEGINNER [Red]: Little or no prior knowledge; Needs basic training to understand risks and good practice

INTERMEDIATE [Grey]: Basic knowledge acquired through courses or previous experience; Ability to implement simple measures/applications/projects

ADVANCED [Blue]: Solid knowledge acquired through in-depth study or professional experience; Ability to design and implement complex AI models / complex security strategies / complex and secure IoT systems

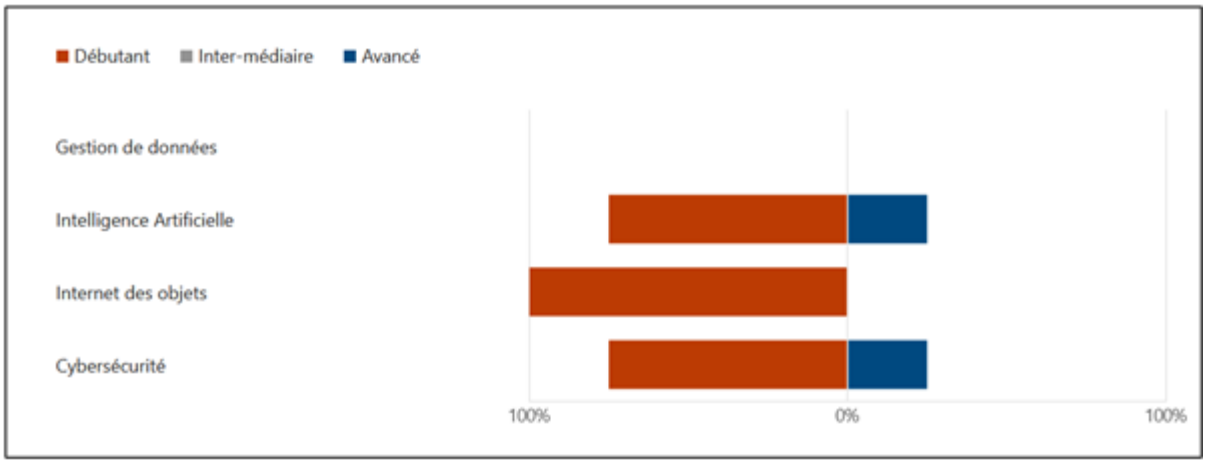

Figure 23 Level of knowledge of proposed technologies

5.2.2 Which training have you already received?

About 50 percent have not been trained, 25 percent have been trained in data management, 20 percent on cyber security and about 1 percent have an academic background.

5.2.3 What training do you need?

- Data management [blue]
- Artificial Intelligence (AI) [orange]
- Internet of Things (IoT) [green]

- Cybersecurity [red]
- Other [violet]

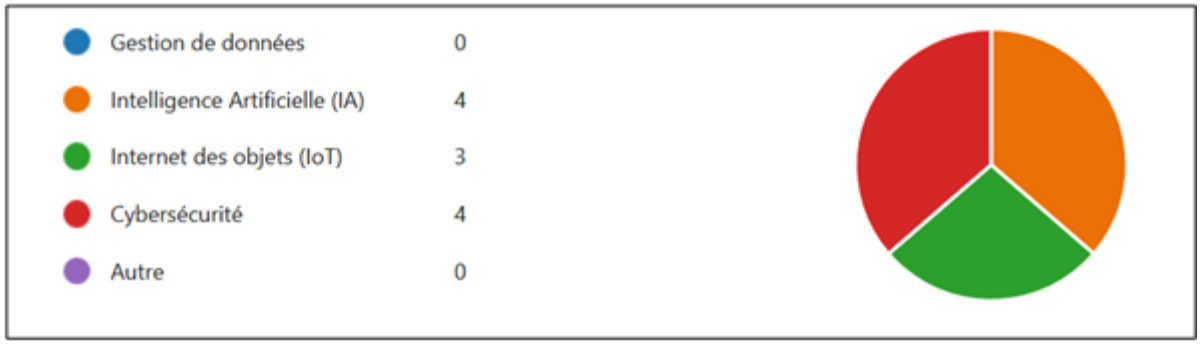

Figure 24 Training needs

5.2.4 Have you already identified specific training courses that meet your needs (in this area)?

About 100 percent indicated they had not yet identified a specific training course.

5.2.5 Ideally, what format should training take to adapt to the work context?

About 3 respondents prefer a training online [orange], 1 hybrid mode [green] and 0 in person [blue].

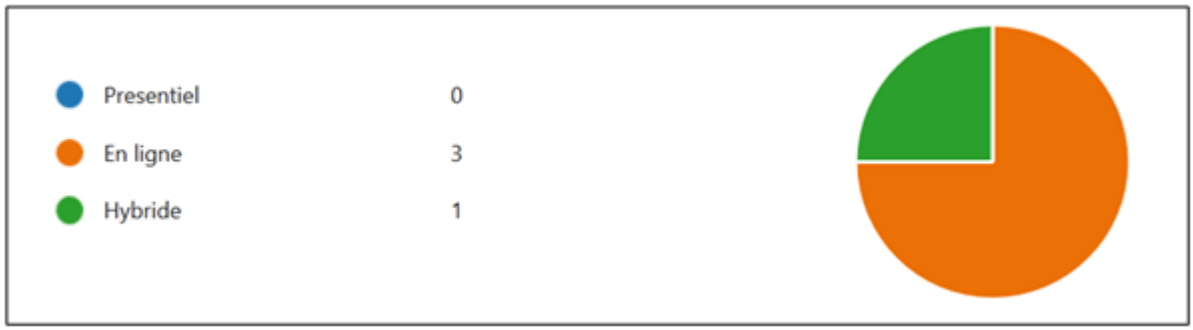

Figure 25 Training format

5.2.6 The availability of hours per months

- 4 - 16 hours: 3 participants
- 10 - 40 hours: 1 participant

5.3 Conclusion

Based on the analysis it can be concluded that the need for training on AI, IoT and Cyber Security is high for both target groups.

5.3.1 Local authorities

- As regards the current level of knowledge of technologies (Data, AI, IoT, Cyber) a large number have indicated beginner level, however, for data management and cyber security many respondents have indicated intermediate level and a small number of respondents have an advanced level (Data, IoT, Cyber).
- The interest in Data management, Artificial Intelligence (AI), Internet of Things (IoT) and Cybersecurity seems to be equally distributed, and respondents indicated several options.
- About 50 percent of respondents have not yet been trained and about 88 percent have not identified a training program.
- About 60 percent of respondents have a non-technical and about 35 percent have a technical professional background.

5.3.2 SMEs

- As regards the current level of knowledge of technologies (Data, AI, IoT, Cyber) the majority has indicated beginner level, and a minority of respondents have an advanced level (AI, Cyber).
- Likewise, the interest in Artificial Intelligence (AI), Internet of Things (IoT) and Cybersecurity seems to be equally distributed, and respondents indicated several options. Several respondents have indicated that they are interested in better understanding the link of their product/sector with AI and how to best secure their data.
- Many respondents have not yet received training; however, a minority has been trained in a specific technology (e.g., AI). About 100% have not yet identified a specific training program.

6 Conclusion

In conclusion, this report outlines a preliminary mapping of the training offerings proposed in the Hauts-de-France Region to enhance cybersecurity awareness and foster knowledge in the fields of data and artificial intelligence (AI), along with their implications. The target audience for these actions includes executives, local actors, and small and medium-sized enterprises (SMEs) within the region. The objective is to provide them with essential skills and knowledge to protect their organizations against cyber threats and harness the potential of data and AI.

The Hauts de France region has witnessed significant technological advancements, resulting in an increase in cyber threats and data-related challenges for businesses and organizations. To address this, a comprehensive training program is essential to empower executives and local actors with the expertise required to make informed decisions in the digital era. Additionally, offering specialized courses for SMEs can provide them with tailored solutions to navigate the complex landscape of cybersecurity and data utilization.

With the mapping, we were able to highlight that the universities and private offerings on cybersecurity and AI are already well-established in the region. They primarily target individuals with a background in computer science and provide specialized training for specific professions. The training capabilities already exist. It seems important that we can build upon the existing resources to address the needs of the region in collaboration with the stakeholders of the EDIH

The demand from local actors seems to be currently focused on requests for large-scale or introductory level training. Specialized courses appear to be less of a priority. This also reinforces the observation of a diverse training landscape that is rapidly expanding, with many new private players in the market, leaving inexperienced local actors uncertain amidst the maze of information about available training options.

Our action plan for the coming months is as follows:

- ✓ **Complete the needs assessment:** We will conduct exchanges and interviews with SMEs. to identify specific requirements and preferences of the target audience in the Hauts-de-France Region. This will help tailor the training programs to meet the demands of executives, local actors, and SMEs effectively.

- ✓ **Organization of a first AI training workshop on September 2023**. This event, held under the EDIH, is aimed at around fifteen SMEs and will allow us to test the format and refine the training program on this subject

- ✓ **Prepare a program of trainings under EDIH for 2024** : Plan training sessions (topics, targets, organizers…) The courses will be flexible in terms of duration and content, accommodating the time constraints and preferences of local authorities and SMEs. : The training sessions will be

conducted through a combination of in-person workshops, webinars, e-learning platforms, and practical exercises. To ensure accessibility, the materials will be available in various formats, and participants can choose the delivery mode that best suits their schedules.

- ✓ **Lead a collaborative approach and partnerships development**: Implementing these actions requires a collaborative approach involving public and private sector entities, academic institutions, and industry experts. Partnerships with actors as CNAM or CNFPT should be studied.

- ✓ **Evaluation and Continuous Improvement:** To measure the effectiveness of these training actions, regular evaluation and feedback mechanisms will be implemented. Post-training assessments will gauge participants' knowledge retention, and adjustments will be made to improve the courses continually.