WHITE PAPER

TECH TIME 2 SKILL

Co-funded by
the European Union

DISCLAIMER

The Tech Time 2 Skill project was launched in January 2023 by a consortium of three training organizations: Simplon.co in France, Becode in Belgium, and Factoría F5 in Spain, along with partner companies and professional associations (PIMEC, Agoria, Agence du Numérique as part of Digital Wallonia, and Microsoft).

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HaDEA). Neither the European Union nor HaDEA can be held responsible for them.

FOREWORD

The COVID-19 pandemic has acted as a powerful catalyst for Europe's digital transformation. According to McKinsey, COVID-19 accelerated the adoption of digital technologies in Europe by an estimated seven years. Between December 2019 and June 2020 alone, there was a 16% increase in the number of companies offering at least partially digitized products and services. By mid-2020, one in two companies had already embarked on their digital transformation journey.

An additional, game-changing shift came with the emergence of generative AI, notably the launch of ChatGPT in November 2022. This development was not anticipated when the project was first drafted, yet it rapidly reshaped market expectations and skills needs. As a result, our training content evolved to address practical, responsible use of generative AI in SMEs, ensuring the programme stayed relevant and actionable for learners and employers.

Against this backdrop of rapid change, Tech Time 2 Skill has, for nearly three years, been helping people and small and medium-sized enterprises (SMEs) make sense of AI and cybersecurity and turn that understanding into action.

The project is co-funded by the European Union under the Digital Europe Programme (DIGITAL) and implemented with the support of HaDEA, the European Health and Digital Executive Agency. DIGITAL strengthens Europe's critical digital capacities (spanning AI, cybersecurity, cloud computing, and microelectronics) and promotes their effective use across key sectors such as energy, climate and environment, manufacturing, agriculture, and health. Its ultimate goal: to accelerate recovery and drive Europe's ongoing digital transformation.

This white paper shares the Tech Time 2 Skill journey in a way practitioners can directly apply. It gathers practical lessons, human stories, and ready-to-use tools, distilling what we built, what changed, and how others can adapt the approach within their own contexts.

In short: Tech Time 2 Skill demystifies AI and cybersecurity for real workplaces and this white paper packages the methods and insights that worked.

PROJECT OVERVIEW

Across Europe, small and medium-sized enterprises (SMEs) face a common challenge: how to keep up with the accelerating pace of digital transformation while lacking the internal resources, time, or expertise available to larger companies[1]. Yet, SMEs are essential to Europe's economy and their ability to adopt technologies like Artificial Intelligence (AI) and Cybersecurity is now a decisive factor for competitiveness, resilience, and long-term growth.

Tech Time 2 Skill was created to help bridge this gap.

Launched by a consortium of training organisations and SME networks in France, Belgium and Spain, the project aims to make advanced digital skills accessible to those who need them most, SME leaders, employees, and job seekers seeking new opportunities. Its objective is simple: equip people with the practical skills required to understand, use, and integrate AI and Cybersecurity in real workplace situations, regardless of sector or prior technical background.

To achieve this, the partners developed a complete range of training opportunities, from short awareness sessions for decision-makers to intensive courses for employees and long-format bootcamps for those looking to enter the job market in digital professions. These programmes are available in several languages and are intentionally designed to be modular, concrete, and relevant to daily work, a direct response to what SMEs reported during interviews, surveys, and consultations carried out by the partners.

A key strength of Tech Time 2 Skill lies in its collaboration model. The consortium brings together:

- Specialised training providers (BeCode, Simplon.co, Factoría F5), known for their inclusive, hands-on approach and extensive experience in tech education.
- SME support organisations (PIMEC, Agoria, Agence du Numérique), which help identify needs, reach companies, and ensure the training responds to local economic realities.
- An industry expert, Microsoft, which contributes technical guidance and insights into the evolving landscape of AI and Cybersecurity.

Together, they have co-designed training programmes grounded in real business use cases rather than academic theory. The focus is always on what SMEs can do today, with the tools they already have, and how they can quickly benefit from new practices, whether improving internal processes, protecting sensitive data, or experimenting with emerging AI solutions.

[1] According to figures from the European Commission, 93% of European companies are micro-enterprises (fewer than 10 employees).

Over the course of the project, thousands of participants across Europe have attended workshops, complete intensive courses, or undertake career-changing bootcamps. These learners will join a growing community of professionals capable of driving responsible digital transformation within their organisations.

More broadly, Tech Time 2 Skill contributes to a wider ambition: strengthening Europe's digital autonomy by empowering its workforce with the skills needed to innovate securely and ethically. By investing in people, and not only technologies, the project supports a vision of digital transformation that is inclusive, sustainable, and beneficial to all.

TRAINING MODULES

AI FOR DECISION-MAKERS
1-DAY COURSE

Goals: Equip leaders with a solid understanding of AI's potential and business opportunities, enabling informed decisions on adoption and strategy.

Target Audience: Leaders, decision-makers, and managers in SMEs across all sectors seeking to understand AI's strategic implications.

Prerequisites: None required : this course is designed to be accessible to all business professionals regardless of technical background.

Learning objectives

- Introduction to AI & its strategic importance for SMEs
- Exploring AI generative models: use cases & limitations for SMEs
- Applications of predictive AI & computer vision across departments
- Strategies for effective AI integration & maximizing business impact
- Building a strategic vision for AI solutions in your SME

CYBERSECURITY FOR DECISION-MAKERS
1-DAY COURSE

Goals: Identify cybersecurity obligations and main threats for a company, understand how to respond to them, and learn the best practices and strategies in cybersecurity for SMEs.

Target Audience: Leaders, decision-makers, and managers of small and medium-sized companies in all sectors.

Prerequisites: None : designed for professionals at all levels of technical expertise.

Learning objectives

- Understanding key cybersecurity risks and obligations for SMEs
- Effective response strategies for identified cyber threats
- Best practices and strategies for robust cybersecurity
- Planning for business continuity in a cybersecurity context
- Integrating cybersecurity into overall corporate strategy

AI ESSENTIALS FOR SMES
5-DAY COURSE

Goals: Enable participants to understand the fundamentals of AI, explore practical applications, and design AI use-cases and strategic roadmaps for their organisation.

Target Audience: Up to 15 employees of small and medium-sized enterprises (SMEs) with no technical prerequisites.

Prerequisites: None : designed for professionals at all levels of technical expertise.

Learning objectives

- Introduction to AI fundamentals and SME applications
- Identifying high-value AI use-cases for your business
- Practical skills with LLMs, prompt design, and RAG customisation
- Generating multimedia content with Gen AI
- Automating workflows
- Designing your AI roadmap and next steps for adoption

CYBERSECURITY AMBASSADOR
5-DAY COURSE

Goals: Become a cybersecurity ambassador for your company, enabling you to implement best practices, spread a security culture throughout the organization, select the best security solutions, and effectively communicate with experts about your cybersecurity needs.

Target Audience: Any SME or start-up employee looking to champion security initiatives.

Prerequisites: At least 2 years of tertiary education and 2 years of professional experience.

Learning objectives

- Build your foundation in cybersecurity principles and threat landscapes
- Learn data classification, encryption, and information security best practices

- Master security for mobile devices and distributed work environments
- Understand network defense and email threat mitigation strategies
- Develop response plans and continuity strategies for your organization

Throughout the course, participants will be updating their SME's cybersecurity master plan and designing awareness activities for their co-workers, ensuring immediate practical application.

PROFESSIONAL BOOTCAMPS

Intensive training programmes for job seekers looking to specialise in either AI development or cybersecurity operations are available. SMEs and specialised professionals are also targeted by this programme, either by them being recruited directly or through their service providers. The comprehensive programmes combine rigorous training with practical applications.

AI DEVELOPER BOOTCAMP

Duration: 9 months

- Master the data cycle from collection to analysis
- Integrate existing AI models into end-user applications
- Learn project management for AI applications

CYBERSECURITY SOLUTIONS OPERATOR

Duration: 6 months

- Integrate & administer cybersecurity solutions.
- Secure network infrastructure components.
- Optimize infrastructure security levels

INDICATORS OF ACHIEVEMENT

TOTAL

98 TRAINING SESSIONS

1.471 PARTICIPANTS

47% WOMEN *(692)*

Over the course of the Tech Time 2 Skill initiative, the consortium successfully deployed an ambitious and diversified training offer targeting job seekers, SME employees, and business leaders across Europe. In total, 98 editions of the various programmes were delivered, enabling 1,471 participants to strengthen their skills in

Artificial Intelligence and Cybersecurity : two domains that are becoming essential for competitiveness and resilience.

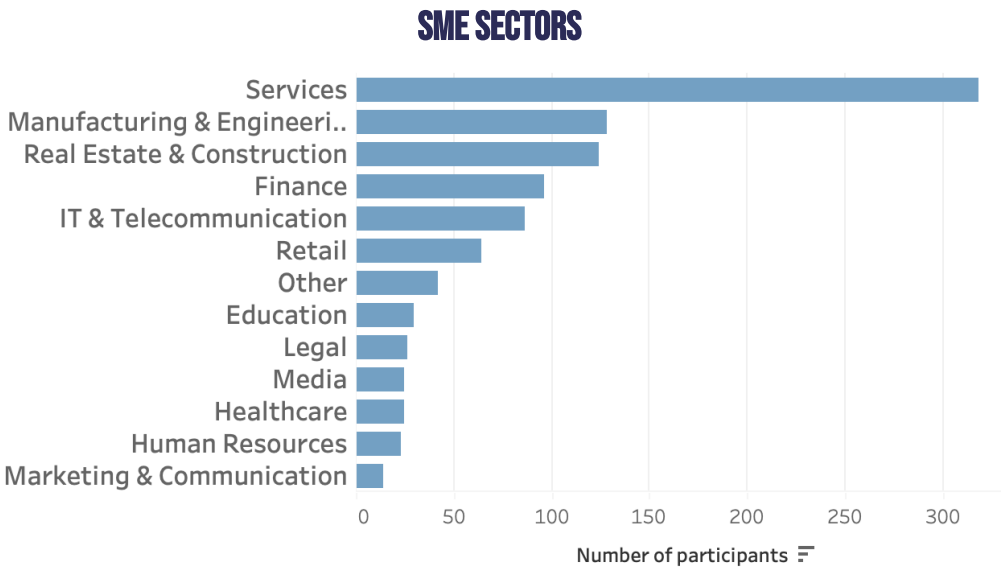
A key achievement of the project lies in its commitment to inclusiveness: 47% of all participants were women, demonstrating strong progress in gender balance in advanced digital skills training.

The bootcamps for job seekers, ranging from 400 to 1,250 hours, played a central role in accelerating access to high-demand digital careers. Across 9 editions, the programme trained 194 participants, including 43% women, equipping them with deep, job-ready expertise in AI and Cybersecurity.

For SME employees, the project delivered 32 editions of the 5-day intensive courses, with 473 professionals trained. Notably, these programmes achieved 51% female participation, a milestone that reflects the growing interest and engagement of women in technical upskilling pathways. These 35-hour courses enabled participants to quickly grasp practical applications, develop concrete use cases, and directly support their companies' digital transformation.

The initiative also reached a large audience of decision makers, a critical group for driving strategic adoption of digital technologies within SMEs. Through 57 one-day sessions, the project trained 804 leaders and managers, among whom 46% were women. These awareness sessions helped demystify AI and Cybersecurity, clarify business risks and opportunities, and empower leaders to build actionable roadmaps aligned with their organisational needs.

Taken together, these results illustrate the significant impact of Tech Time 2 Skill. Beyond the numbers, they highlight a growing appetite across Europe for practical, accessible, and business-oriented digital training,along with a strong momentum toward a more inclusive tech workforce.



TESTIMONIALS

Bouchaib: From Forensics to AI

Based in Nancy, France, Bouchaib successfully transitioned from forensic science to artificial intelligence through the TT2S program and a work-study placement at CHRU Nancy. Passionate about health and ethics, he contributes to projects such as automated robotics and a tailored OCR tool for the hospital. His journey shows how diverse backgrounds, coupled with the right training, can drive meaningful innovation in AI.

"It was quite difficult for me to find work after completing a traditional university education. So this practical experience with work-study makes my professional reorientation easier and more reassuring."

Noémie: Navigating AI with Responsibility

With a background in computer engineering and a career dedicated to digital responsibility and CSR, Noémie joined a five-day AI course to better understand the ethical and environmental challenges of emerging technologies. The experience gave her hands-on insights into AI's potential and limitations, particularly in generative content. Today, she integrates this knowledge into her coaching and training activities, promoting a reasoned, ethical, and practical use of AI.

"I was really concerned about the rapid development of AI. This democratization seemed too fast and not sufficiently regulated to me. So I preferred to address these issues as early as possible in order to better understand the challenges and get on top of them."

Myriam: leading upskilling for European SMEs

Myriam is an experienced trainer specialising in Artificial Intelligence and Cybersecurity, with a strong track record in designing and delivering training for SMEs, entrepreneurs, and corporate teams. She has facilitated a wide range of formats, from half-day awareness sessions to two-day intensive programs, offering highly adaptable learning experiences tailored to the needs and maturity levels of diverse audiences.
She advocates strongly for in-person training, especially for complex or rapidly evolving topics. For her, face-to-face sessions enable spontaneous questions, deeper interaction, and real-time adjustment of the content, elements that are harder to achieve in e-learning and significantly enhance the impact of the learning experience for both trainers and participants.

"I favor hands-on workshops and real-life scenarios. Participants work on concrete cases, whether they involve cyberattack scenarios or experiments with AI tools. This makes the training dynamic and allows everyone to get involved, regardless of their level."

CHALLENGES ENCOUNTERED

One of the most significant challenges encountered throughout Tech Time 2 Skill was the strong imbalance in interest between Artificial Intelligence (AI) and Cybersecurity. With the rapid rise of generative AI from late 2022 onward, AI dominated public attention and was widely perceived as a source of innovation and future opportunity. Cybersecurity, on the other hand, struggled to gain traction. Many SMEs still viewed it as a highly technical field reserved for specialists, and a reactive rather than preventive mindset often prevailed. As a result, participation in AI-related activities was consistently higher, while everyday security practices remained under-adopted.

To address this gap, the project adopted a strategy that interwove both topics within the same training experiences. By leveraging the natural enthusiasm for AI, it became possible to sustain engagement and gradually introduce cybersecurity concepts in a more accessible way. Over time, partners observed a tangible shift: as participants progressed through the sessions, their awareness of Cybersecurity's importance increased, showing that interest can be cultivated when exposure is consistent and the learning experience is concrete and relatable.

Another core challenge stemmed from the diversity of SME contexts and participant profiles. The people attending training sessions came from vastly different sectors, roles, and levels of digital maturity : from leaders to HR managers, marketing teams, finance officers, project managers, and more technical staff. Their needs were not the same, and examples that resonated in manufacturing settings did not necessarily apply to healthcare, retail, or services. Even within the same company, digital practices varied widely. This diversity made it difficult to design a single training approach that could suit everyone, especially for practical activities such as AI prototyping. The project therefore structured its content so that foundational concepts remained accessible to all, while sector-specific scenarios and role-relevant applications helped anchor learning in everyday reality.

Time constraints also played a major role : SME employees often cannot free themselves for several consecutive full days, making intensive formats challenging to attend. Participation frequently depended on employees finding small windows in their schedules, often at the last minute. This reality pushed the project toward shorter, more flexible formats, sometimes delivered online in 2- to 3-hour segments, while still preserving space for hands-on discovery. Balancing the need for brevity with the importance of practical experimentation was a constant design challenge, but essential to transforming awareness into real capability.

Technological evolution presented yet another difficulty. AI tools, models, interfaces, and best practices evolve at extraordinary speed, making some examples outdated only a few months after they were introduced. Cybersecurity risks and attack techniques also shifted rapidly. Partners responded by regularly refreshing content and focusing on

principles and transferable methods rather than tool-specific skills, helping learners retain approaches that would remain relevant despite technological change.

In addition, basic technical conditions were not always met. Some SMEs lacked reliable connectivity, suitable equipment, or even the foundational digital skills required to follow online sessions. In these cases, simply joining a videoconference or using collaborative tools could become an obstacle, illustrating disparities in digital readiness across regions and sectors.

Despite these barriers, the project saw steady growth in participants' understanding of Cybersecurity's relevance. Across sessions, it became evident that exposure and clear, practical communication can shift mindsets from reactive to proactive. This matters greatly: Cybersecurity is not just a technical issue, but a shared responsibility across the entire organisation. SMEs, often without dedicated IT teams or advanced security infrastructures, are particularly vulnerable. A single human error, such as clicking on a phishing link or using a weak password, can lead to breaches, operational disruptions, or financial losses that are difficult to absorb. Cultivating everyday security practices therefore requires a cultural shift, one in which employees at all levels understand their role as the first line of defence.

This broader perspective also applies to AI. While enthusiasm for AI is strong, responsible adoption is essential. AI offers SMEs concrete benefits, from automating tasks to improving operations and reducing costs, but it also carries environmental, ethical, and social implications. Behind AI tools lie energy-intensive infrastructures and global labour conditions that often remain invisible. The use of AI can introduce risks such as bias, data privacy issues, or overreliance on opaque systems, and SMEs may lack the internal structures to manage these challenges. For this reason, the project emphasised not only how to use AI tools, but also why and at what cost, encouraging a more informed and thoughtful approach.

Together, these challenges shaped the evolution of Tech Time 2 Skill. They underscored the need for training that is flexible, inclusive, realistic, regularly updated, and grounded in responsible digital practice. They also highlighted an essential truth: meaningful digital transformation requires not only skills and tools, but awareness, culture, and collective responsibility.

RECOMMENDATIONS

The experience gained throughout Tech Time 2 Skill highlights a set of actionable recommendations for strengthening Europe's digital readiness. While SMEs face common challenges, the solutions must be tailored to different actors: employees, SME leaders, public authorities, and training providers. The following recommendations

synthesise the insights gathered during the project and outline concrete steps to support responsible, sustainable digital transformation.

FOR SME EMPLOYEES

1. Facilitate access to training through flexible, realistic formats
Employees in SMEs often struggle to free themselves for long sessions. Training should therefore be available in highly adaptable formats emphasizing peer-to-peer exchange:

- short modules (1–3 hours)
- online or hybrid delivery
- intensive days or programmes spread over several weeks
- modules grouped by practical challenges rather than technical themes

2. Encourage participation through incentives
Mechanisms that motivate employees to upskill can help remove barriers to participation like microcredentials, diplomas or attendance certificates.

3. Provide concrete, immediately applicable tools
Employees benefit most from sessions that include:

- real-life SME use cases
- step-by-step guided exercises
- templates, checklists, and quick-start guides they can directly apply in their organisation

4. Integrate Cybersecurity as a transversal skill
Cybersecurity should not be treated as a separate specialty for experts. Employees should systematically be introduced to:

- secure digital practices
- everyday risk detection
- data protection habits
- and the role they play as a first line of defence

FOR SME LEADERS AND MANAGERS

1. Adopt training programs that mix AI and Cybersecurity
AI attracts attention and can serve as an entry point for building awareness of Cybersecurity. Combined sessions help managers understand both opportunities and risks in an accessible and strategic way.

2. Build actionable transformation plans
Programs should support leaders in:

- identifying relevant use cases for their organisation

- evaluating risks
- prioritising actions
- and designing realistic roadmaps adapted to their constraints

3. Engage teams through hands-on opportunities
Decision-makers should encourage internal pilot projects and team-based experimentation, ensuring that skills acquired in training translate into real implementations.

4. Treat Cybersecurity as a strategic responsibility
Leaders must ensure that Cybersecurity is not confined to IT teams but embedded across the organisation as a shared responsibility, influencing governance, culture, and daily routines.

FOR PUBLIC AUTHORITIES AND EUROPEAN INSTITUTIONS

1. Invest in large-scale Cybersecurity awareness campaigns
Regional, national, or Europe-wide initiatives are essential to raise baseline knowledge, counter complacency, and reach SMEs who are not connected to training networks.

2. Create financial and regulatory incentives for SME training
Authorities can play a decisive role by:

- offering fiscal benefits for companies investing in digital upskilling
- simplifying access to grants and subsidies
- prioritising SMEs in training vouchers and national funds

3. Support flexible, modular, skill-based learning frameworks
Funding schemes should explicitly encourage:

- modular course designs
- short-cycle upskilling
- and hybrid learning infrastructures tailored to SME constraints

4. Promote responsible and European-aligned infrastructures
Public policies should encourage the adoption of European AI and cybersecurity tools that reinforce sovereignty, privacy protection, and compliance with EU regulations.

FOR TRAINING PROVIDERS AND LEARNING ORGANISATIONS

1. Develop highly modular training pathways
Training formats should be designed as adaptable building blocks that can be combined, reordered, or customised to fit diverse SME profiles, sectors, and local constraints.

Modularity ensures that content remains relevant despite heterogeneous learner backgrounds and differing organisational needs.

2. Maintain constant content iteration

Given the rapid evolution of AI and Cybersecurity, training materials must be updated every 3–6 months with expert input.

Importantly, this rapid pace of change makes e-learning formats significantly harder to maintain, as updating digital modules, videos or interactive content requires time, technical resources, and frequent redevelopment cycles to stay relevant.

For this reason, in-person training formats should be favoured and strengthened, as they allow trainers to:

- adjust examples and tools in real time
- incorporate the latest developments immediately
- and ensure the content remains aligned with the fast-moving technological landscape.

3. Offer both inter-company and in-company formats

A dual approach maximises impact:

- Inter-company sessions create cross-sector exchanges and enable SMEs to learn from peers facing similar challenges.
- In-company sessions enable deeper tailoring to organisational culture, sector-specific use cases, and strategic priorities.

4. Strengthen partnerships with SME networks

Training providers should work closely with chambers of commerce, SME associations, federations, and clusters. These networks are essential for reaching companies efficiently, understanding local needs, and ensuring that training interventions respond to real market conditions.

5. Embed Cybersecurity across all digital training

Cybersecurity should not be siloed as a specialist subject. Secure practices must be embedded across AI, data, cloud, and digital workplace modules so that every learner, regardless of role or expertise, adopts Cybersecurity as part of everyday digital behaviour.

6. Provide implementation-ready materials

To maximise impact, providers should supply SMEs with:

- practical templates
- checklists
- scenario-based exercises
- and simple frameworks to immediately apply lessons learned

7. Strengthen European cooperation for quality and impact

Digital transformation is a shared European challenge, and training providers gain immensely from collaboration across borders. This includes:

- exchanging best practices, methodologies, and emerging pedagogical insights;
- co-developing or adapting training content to ensure alignment with European standards and technological priorities;
- participating in European training networks to pool expertise and reduce duplication of efforts;
- sharing updates on regulatory evolutions (e.g., AI Act, NIS2) and aligning training accordingly;
- forming cross-country communities of trainers to sustain collaboration and accelerate innovation.

Such cooperation enhances training quality, promotes consistency across Europe, and strengthens the continent's capacity to build a skilled, resilient digital workforce.

PARTNER CONTACTS

LOUIS DE VIRON

Head of Tech & Pedagogy
louis.deviron@becode.org

OLGA CORRALES

B2B relationship & Project Manager
olga.corrales@factoriaf5.org

TIMOTHÉE LEENHARDT

International development & pedagogical innovation manager
tleendardt@simplon.co

Co-funded by
the European Union