

National Course Plan

France – Anemo



Co-funded by
the European Union

Contents

1. Summary	3
2. Target group description	3
3. Training setting.....	3
4. Learner Journey(s).....	6
Beginner & Intermediate (Turtle & Mouse) learner journey	7
Advanced (Hare) learning journey	7
5. Conclusion.....	8

MECyS is 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 Education and Culture Executive Agency (EACEA).

Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under [CC BY-SA 4.0](https://creativecommons.org/licenses/by-sa/4.0/)



1. Summary

The training plan for the MECyS project offers adaptive learning journeys tailored to Micro and Small Enterprise (MSE) professionals' proficiency levels. It begins with level tests to assess learners' cybersecurity knowledge, followed by problem-solving conferences fostering collaborative learning. Asynchronous course content delivery includes interactive modules, videos, quizzes, and games. These steps ensure a dynamic learning experience, empowering MSE professionals to navigate cybersecurity challenges effectively and foster a safer digital environment for MSEs in Europe.

2. Target group description

In France, the primary target group for the MECyS project include young adults who are employed in MSEs as well as their managers across diverse industries. This group is heterogeneous, with varying levels of education, previous experience in cybersecurity, and knowledge based on their work positions. Additionally, vocational students within MSEs may be considered as a secondary target audience. The working conditions of this target group vary significantly, reflecting the heterogeneity of roles and responsibilities within MSEs. Given the varying levels of digitalization in MSEs across different fields, there exists a tangible need for digital skills and increased awareness of cybersecurity. The competencies within the target group regarding digital skills, cybersecurity, and data protection are expected to be diverse. Consequently, the MECyS course is designed to cater to an intermediate level, ensuring inclusivity for participants with varying skill sets. Recognizing the time constraints and potential future budget limitations, the course aims to offer flexibility to accommodate the needs of the French target group.

3. Training setting

Course delivery

The MECyS training program, tailored for participants in small enterprises and startups in France, is designed to meet the unique needs and challenges faced by these businesses. Recognizing the distinct characteristics and often limited resources of small enterprises, the course delivery prioritizes accessibility and flexibility.

Course duration

The duration of the courses is divided into six modules, each lasting approximately 90 minutes. This modular approach allows participants to engage with the content in manageable segments, promoting focused learning and minimizing potential information overload.

Learning format

The online, asynchronous format allows individuals from small enterprises and startups to engage with cybersecurity training at their own pace, accommodating the dynamic and often demanding nature of their work environments. Emphasizing a self-regulated learning approach further enables participants to customize their learning experience, ensuring that the training aligns with the specific cybersecurity requirements and digitalization needs of their businesses.

Content strategy

The content includes informative videos offering real-world insights into cybersecurity practices, theory courses that delve into fundamental concepts, and interactive challenges that simulate practical scenarios. To reinforce understanding and retention, quizzes are strategically integrated to assess knowledge and provide instant feedback. Recognizing the diverse learning preferences within the target audience, gamified elements are embedded in the training, enhancing participant engagement and making the learning process enjoyable. The incorporation of interactive boards fosters collaborative learning, allowing participants to share experiences and insights. This comprehensive approach ensures that the MECyS training content not only imparts theoretical knowledge but also cultivates practical skills through hands-on challenges, fostering a well-rounded understanding of cybersecurity tailored to the unique needs of MSEs in France. Here are some contents considered relevant for our target:

Basic Cybersecurity Concepts: Covering fundamental principles such as the importance of strong passwords, secure online behavior, and protection against common threats like phishing and malware.

Practical Application: Real-world scenarios and case studies relevant to small enterprises and startups, showcasing how cybersecurity measures can be implemented in everyday business operations.

Data Protection and Privacy: Understanding the significance of data protection laws, secure data handling, and safeguarding sensitive information in compliance with regulations.

On the other hand, here some learning materials that may fit our target the most:

Informative Videos: Short and engaging videos providing insights into cybersecurity concepts, industry trends, and practical tips.

Theory Courses: Comprehensive written content and presentations covering essential theoretical aspects of cybersecurity, delivered in a digestible format. ,

Interactive Challenges: Simulated exercises and challenges allowing participants to apply theoretical knowledge in practical scenarios, enhancing hands-on skills.

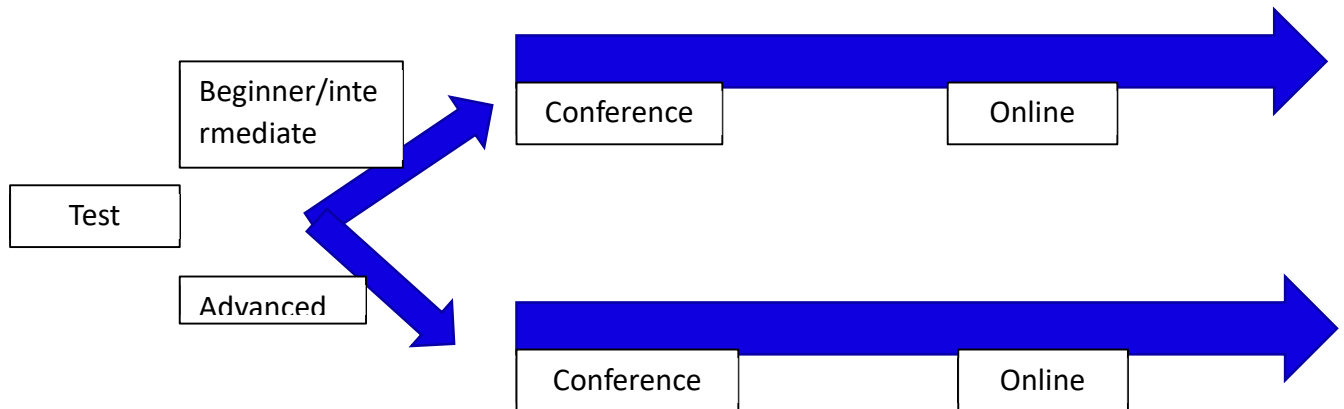
Outreach strategy

The outreach strategy emphasizes communication and strategic collaboration. Leveraging digital channels, including social media platforms, targeted email campaigns, and industry-specific forums, the outreach aims to raise awareness about the MECyS training program's relevance and benefits. By highlighting the program's practical approach to enhancing cybersecurity resilience in the context of small enterprises and startups, the outreach strategy aims to resonate with the specific challenges faced by these businesses.

Collaboration with business associations, chambers of commerce, and startup networks will play a pivotal role in reaching the target audience. The outreach materials will underscore the program's flexibility, acknowledging the time constraints of busy professionals, and emphasize the potential positive impact on organizational cybersecurity practices.

4. Learner Journey(s)

Outlining the learning journey steps, content structure, and the adaptive approach taken a first draft may resemble to:



1. Level Test:

The MECyS course begins with a thorough level test to assess the existing knowledge and competencies of participants. This test covers foundational aspects of cybersecurity and data protection. By understanding the diverse levels of expertise within the target group, the course can be tailored to meet the specific needs of each participant. The results of the level test serve as a roadmap for crafting individualized learning journeys.

2. Conference:

A virtual conference is organized to bring participants together for an interactive discussion on cybersecurity challenges and potential solutions. Facilitated by experts in the field, this conference encourages participants to share their experiences and insights. The collaborative atmosphere fosters a sense of community and allows for the exchange of best practices. Identified challenges become focal points for addressing real-world issues throughout the course, ensuring practical relevance.

3. Asynchronous Course Content:

The core of the MECyS course is an asynchronous online learning experience that accommodates the diverse schedules and preferences of participants. This content-rich course covers a spectrum of topics, ranging from fundamental cybersecurity principles to advanced techniques. The inclusion of theoretical modules ensures a comprehensive understanding, while interactive games and quizzes provide engaging and practical learning

opportunities. Participants progress through the material at their own pace, promoting flexibility and personalized skill development.

BEGINNER & INTERMEDIATE (TURTLE & MOUSE) LEARNER JOURNEY

What?

Basic Cybersecurity Fundamentals: Covering the foundational principles of cybersecurity, including the importance of strong passwords, secure online behaviour, and an introduction to common threats.

Introduction to Data Protection: Providing an overview of data protection laws and the significance of responsibly handling and securing sensitive information.

Understanding Phishing and Malware: Exploring common types of phishing attacks, malware, and practical tips for recognizing and avoiding them.

Network Security Basics: Introduction to securing networks, including Wi-Fi security and protecting against unauthorized access.

How?

Utilize interactive presentations, real-world examples, and practical exercises to introduce key cybersecurity concepts.

Incorporate case studies, legal frameworks, and interactive discussions to emphasize the significance of data protection.

Why?

The beginner level content focuses on establishing a solid foundation in cybersecurity for individuals with limited prior knowledge. These fundamental concepts are essential for building a baseline understanding of cybersecurity risks and best practices. By covering basic principles, cyber hygiene, and introductory topics, the course ensures that participants develop a strong understanding of essential cybersecurity concepts before moving to more advanced content.

ADVANCED (HARE) LEARNING JOURNEY

What?

Cloud Security: Exploring the challenges and best practices for securing data and operations in cloud environments, considering the specific needs of small enterprises and startups.

Advanced Threats and Cyber Attacks: In-depth examination of sophisticated cyber threats, understanding the tactics of hackers, and strategies for defending against advanced attacks.

How?

Combine theoretical lectures with hands-on labs, case studies, and discussions on real-world network security scenarios.

Engage in hands-on labs, live demonstrations, and collaborative discussions on advanced threat scenarios.

Why?

The expert level content is designed for participants with a strong foundation in cybersecurity and professional experience in the field. This content provides a deeper dive into advanced topics, focusing on strategic cybersecurity management, incident response, and specialized areas like cloud security. By addressing the complex challenges faced by small enterprises and startups, the course equips participants with the expertise needed to implement comprehensive cybersecurity measures within their organizations.

5. Conclusion

Addressing the target group's heterogeneity, the national plan focuses on MSEs. Recognizing varying levels of education, experience, and digital literacy, the course employs a segmented learning approach, offering Beginner, Intermediate, and Advanced levels.

One potential challenge lies in the diverse educational backgrounds and prior experiences of the target group. To tackle this, the course employs a comprehensive level test at the outset, enabling personalized learning journeys that cater to the varying proficiency levels of participants.

The finalized English version of the French National Course Plan was to basically align the Course Plans of the MECyS partners. Further developments will be done in the French version.



MECyS

Micro - Enterprise Cybersecurity

mecys.eu



Co-funded by
the European Union