Micro - Entreprise Cybersecurity

MECyS

Report Learning Tools

1st Part of Training Plan

Co-funded by
the European Union

Point of Contact	Bernd Remmele
Institution	Pädagogische Hochschule Freiburg (PHFR)
E-mail	Bernd.remmele@ph-freiburg.de
Phone	+49 761 682 625

Project Acronym	MECyS
Project Title	Microenterprise Cybersecurity
Funding	Erasmus+/Movetia
Project start date	31/12/2022
Dissemination level	Public
Date of submission	30/08/2023
Lead partner	ANEMO
Contributing partners	FHNW, PHF, STHEV, AB IED, CESUR
Main Authors	Antoine Akiki, Gyna Montoya, Juan Marcos

Contents

1 Introduction

1.1 Purpose of this report

The purpose of this report is to provide a comprehensive analysis of the learning tools discussed during the workshop. It aims to evaluate the effectiveness, usability, and suitability of these tools in enhancing the learning experience. By examining their features, benefits, and limitations, this report aims to guide partners in making informed decisions regarding the adoption and integration of learning tools in their educational practices. The insights gathered from this report will contribute to the continuous improvement of teaching and learning methodologies, ultimately enhancing the overall learning outcomes for learners.

1.2 Workshop objectives and overview

The workshop was designed with the primary goal of fostering a collaborative environment for participants to explore and discuss various aspects of cybersecurity education. It aimed at enhancing participant's knowledge and understanding of key concepts, emerging trends, and best practices in the field of cybersecurity. Through interactive sessions, presentations, and group activities, the workshop facilitated knowledge sharing, networking, and the exchange of ideas among participants from diverse backgrounds and expertise. The report will provide a detailed account of the workshop objectives, the topics covered, and the overall structure of the workshop.

First the participants were divided into three groups based on their level of knowledge in cybersecurity. The objective was to create a tailored learner journey for each category, considering their specific needs and skill gaps. Through collaborative discussions and brainstorming sessions, the groups worked together to identify the key learning objectives and milestones for each stage of the journey. The workshop provided a platform for participants to share their insights, experiences, and best practices. This exercise aimed to ensure that the workshop outcomes were aligned with the diverse learning needs of the participants, ultimately enhancing the effectiveness and relevance of the learning tools and materials discussed throughout the session

Second, following the categorization of participants based on their cybersecurity knowledge, each partner had the opportunity to present learning tools from their respective countries. The objective was to identify and determine the most suitable tools for each category of learners. Each partner showcased their recommended learning tools, highlighting their unique features, functionalities, and effectiveness in addressing specific learning objectives and skill levels. The presentations sparked insightful discussions among the participants, enabling them to compare and evaluate the various learning tools in terms of their appropriateness for each learner category. This collaborative process aimed to facilitate informed decision-making and the selection of the most relevant and effective learning tools for each group of participants. By leveraging the diverse expertise and experiences of the partners, this exercise contributed to the identification of tailored learning solutions that would meet the specific needs and requirements of each learner category.

2 Learning tools

The description of tools below provides an overview of selected and presented tools by the partners in the context of the workshop. The partners have selected these tools according to their qualification as a tool in the MECyS training prototypes. In the appendix, a larger collection of tools assembled by the partners can be found (Report Training Tools – Tool List). This extensive list provides an overview on a larger number of tools according to the requirements made by MECyS.

2.1 France

Rootmee is a learning tool introduced during the workshop from France. It is designed to enhance cybersecurity education and provide an immersive learning experience for participants. Rootmee offers a comprehensive range of interactive modules and exercises that cover various aspects of cybersecurity, including threat detection, risk assessment, and secure coding practices. The platform utilizes gamification elements to engage learners and make the learning process more enjoyable. One of the key features of Rootmee is its adaptive learning approach. The tool assesses the learner's knowledge and progress and adjusts the difficulty level accordingly, ensuring personalized learning paths for everyone. It provides real-time feedback and performance analytics to track the learner's improvement and areas for further development. Rootmee also emphasizes practical application through hands-on exercises and simulations. Participants can engage in simulated cyber-attack scenarios and practice their skills in a safe and controlled environment. The tool encourages active participation and critical thinking, fostering the development of problem-solving and decision-making abilities. Furthermore, Rootmee promotes collaboration and knowledge sharing among participants. It includes discussion forums and collaborative projects where learners can exchange ideas, ask questions, and learn from their peers. This collaborative aspect enhances the social learning experience and allows participants to benefit from diverse perspectives and experiences. Overall, Rootmee offers a comprehensive and interactive learning platform for cybersecurity education in France. It combines theoretical knowledge, practical application, and collaborative learning to ensure an effective and engaging learning experience for participants.

Hackademics is another learning tool introduced during the workshop, originating from an online platform. It aims to provide a comprehensive and accessible learning experience in the field of cybersecurity. Hackademics offers a diverse range of courses and resources tailored to different skill levels and areas of interest within cybersecurity. One notable feature of Hackademics is its extensive course catalog. It covers a wide range of topics, including network security, ethical hacking, cryptography, and secure coding. Each course is designed with clear learning objectives and structured modules, allowing participants to progress at their own pace. The platform provides a combination of text-based lessons, video tutorials, practical exercises, and quizzes to ensure a well-rounded learning experience. Hackademics also emphasizes hands-on learning through virtual labs and practical assignments. Participants can apply their knowledge in simulated environments, engage in real-world scenarios, and practice their skills in a controlled setting. This practical approach helps reinforce understanding and develop practical cybersecurity skills. Furthermore, Hackademics fosters a supportive learning community. Participants can engage with instructors and fellow learners through discussion boards, forums, and chat features. This encourages collaboration, knowledge sharing, and the opportunity to seek guidance and support from experts and peers. The platform also incorporates gamification elements to enhance engagement and motivation. Participants can earn badges, points, and achievements as they progress through the courses, providing a sense of accomplishment and encouraging continued learning. In summary, Hackademics offers a diverse range of cybersecurity courses and resources through its online platform. It provides a flexible and self-paced learning experience, combining theoretical knowledge, practical exercises, and a supportive learning community. Participants can enhance their cybersecurity skills and knowledge through interactive lessons, hands-on labs, and collaborative learning opportunities.

Dokeos is a highly regarded learning management system (LMS) used widely in France and beyond. It is designed to support efficient and effective online learning experiences. Dokeos offers a range of features and functionalities that cater to diverse educational needs, making it a versatile learning tool. With Dokeos, educators can create and manage courses, track learner progress, and deliver engaging multimedia content. The platform provides a user-friendly interface, allowing instructors to easily upload and organize course materials, facilitate discussions, and assess student performance. Additionally, Dokeos offers collaborative tools, such as group workspaces and communication channels, fostering interaction and knowledge sharing among learners. One of the notable strengths of Dokeos is its adaptability and scalability. The platform can accommodate both small-scale and large-scale educational institutions, making it suitable for various learning environments. Moreover, Dokeos prioritizes data security and compliance, ensuring the protection of sensitive student information and maintaining privacy standards. Overall, Dokeos empowers educators to create engaging and interactive online learning experiences, enabling learners to access educational materials, participate in activities, and track their progress. Its comprehensive features and user-friendly interface make it a valuable learning tool for enhancing the educational journey in France and beyond.

2.2 Cyprus

Introduction to Cybersecurity is a comprehensive learning tool in Cyprus that aims to provide individuals with a foundational understanding of cybersecurity concepts and practices. This tool is designed to cater to learners who are new to the field of cybersecurity and seek to develop essential knowledge and skills.The learning tool covers various fundamental aspects of cybersecurity, including the basics of computer systems, network security, data protection, and threat mitigation strategies. It introduces learners to common cybersecurity threats and vulnerabilities, emphasizing the importance of proactive security measures and best practices.Through a combination of theoretical explanations, practical examples, and interactive exercises, "Introduction to Cybersecurity" offers an engaging learning experience. Participants will gain insights into key cybersecurity principles and learn how to apply them in real-world scenarios. The tool also provides opportunities for hands-on practice and simulations to enhance comprehension and reinforce learning outcomes.Moreover, "Introduction to Cybersecurity" fosters a collaborative learning environment, encouraging participants to engage in discussions, ask questions, and share their experiences. It promotes critical thinking and problem-solving skills by presenting authentic cybersecurity challenges and guiding learners towards effective solutions.

Cyber Security Tutorial is a comprehensive learning resource that provides individuals with valuable insights into the field of cybersecurity. Designed to cater to a wide range of learners, this tutorial serves as an introductory guide to understanding the fundamental principles and practices of cybersecurity.Covering various essential topics, the tutorial offers a systematic approach to learning about cybersecurity. Participants will delve into key concepts such as threat analysis, risk management, network security, cryptography, and incident response. The tutorial presents these topics in a structured and accessible manner, making it suitable for beginners who have limited prior knowledge of cybersecurity.Through a combination of informative text, visual aids, and practical examples, the tutorial engages learners and facilitates their understanding of complex cybersecurity concepts. Participants will gain insights into different types of cyber threats, the methods used to exploit vulnerabilities, and the preventive measures to safeguard digital assets.One of the key strengths of the "Cyber Security Tutorial" is its interactive nature. It encourages participants to actively engage with the content, ask questions, and seek clarification. Additionally, the tutorial incorporates hands-on exercises and scenarios that allow learners to apply their knowledge in simulated real-world situations. This practical approach enhances comprehension and enables participants to develop practical skills in cybersecurity.By utilizing the "Cyber Security Tutorial," individuals can acquire a solid foundation in cybersecurity, empowering them to make informed decisions and take appropriate actions to protect themselves and their organizations from cyber threats. Whether for personal use or professional development, this tutorial serves as a valuable resource for anyone looking to enhance their understanding of cybersecurity.

Cyber Security Tutorial: A Step-by-Step Guide on **simplelearn.com** is a comprehensive online resource that offers individuals a systematic approach to learning about cybersecurity. Designed to cater to various learning styles and skill levels, this tutorial serves as a valuable tool for those looking to develop a strong foundation in cybersecurity. The tutorial begins with an introduction to the fundamental concepts of cybersecurity, providing participants with a clear understanding of its importance and relevance in today's digital landscape. From there, the tutorial takes learners on a step-by-step journey, covering key topics such as threat detection, risk assessment, network security, data protection, and incident response. What sets this tutorial apart is its user-friendly format and interactive nature. Each module is presented in a structured manner, guiding learners through the content in a logical progression. Participants can navigate through the tutorial at their own pace, making it suitable for both beginners and individuals with prior knowledge of cybersecurity. The tutorial incorporates a variety of learning resources to enhance comprehension and engagement. Participants have access to informative text-based lessons, visual aids, diagrams, and practical examples that illustrate real-world scenarios. Furthermore, interactive quizzes and exercises are included to reinforce understanding and assess progress. Through the "Cyber Security Tutorial: A Step-by-Step Guide," participants will gain practical knowledge and skills in cybersecurity. By following the step-by-step instructions and applying the principles learned, individuals can develop a solid understanding of cybersecurity best practices and effectively mitigate risks in their personal and professional lives. With its comprehensive coverage of cybersecurity topics, user-friendly interface, and interactive learning resources, the "Cyber Security Tutorial: A Step-by-Step Guide" on simplelearn.com is an invaluable tool for anyone looking to enhance their knowledge and skills in cybersecurity. Whether you are a beginner or seeking to deepen your understanding, this tutorial provides a structured and accessible pathway to becoming well-versed in the field of cybersecurity.

2.3 Spain

Rol Game offers a unique approach to cybersecurity education, employing elements of role-playing to engage learners in a dynamic and captivating learning experience. The tool provides participants with the opportunity to assume different roles and engage in simulated cybersecurity scenarios. Through this gamified approach, learners can actively apply their knowledge and skills to solve challenges, make decisions, and navigate complex cybersecurity situations. The platform fosters critical thinking, problem-solving, and collaboration, allowing participants to develop a deeper understanding of cybersecurity concepts and practices. One of the key strengths of "Rol Game" is its ability to create a realistic environment where participants can explore the consequences of their actions and witness the impact of different cybersecurity strategies. This hands-on approach enables learners to develop practical skills and gain insights into the complexities of real-world cybersecurity incidents. The platform offers a variety of engaging scenarios that cover a wide range of cybersecurity topics, including threat detection, incident response, network security, and ethical hacking. These scenarios challenge participants to apply their knowledge in dynamic and evolving situations, promoting active learning and skill development. The analysis of the "Rol Game" learning tool revealed its effectiveness in capturing learners' interest, promoting engagement, and fostering a deeper understanding of cybersecurity concepts. By immersing participants in realistic scenarios, "Rol Game" enables them to acquire practical skills, enhance decision-making abilities, and develop a proactive mindset towards cybersecurity.In summary, the "Rol Game" learning tool from Spain offers a unique and engaging approach to cybersecurity education. By leveraging elements of role-playing, the platform provides learners with immersive scenarios and opportunities to apply their knowledge and skills. The analysis conducted during the workshop highlighted the value of "Rol Game" in enhancing the learning experience and fostering practical cybersecurity expertise among participants.

The **board game** offered by **INCIBE** (**National Cybersecurity Institute of Spain**) provides an engaging and interactive learning experience for participants. Designed to educate individuals about cybersecurity, this game offers a hands-on approach to understanding and applying essential cybersecurity concepts. The board game incorporates elements of strategy, problem-solving, and teamwork, making it an enjoyable and educational activity for players of all ages. By navigating through different scenarios and challenges, participants are exposed to various cybersecurity situations and learn how to make informed decisions to protect digital assets. Through gameplay, participants develop critical thinking skills, enhance their understanding of cybersecurity risks, and learn effective strategies to mitigate those risks. The game covers a wide range of cybersecurity topics, including data protection, online privacy, secure communication, and safe internet practices. The analysis of the board game revealed its effectiveness in promoting active learning, fostering collaboration, and enhancing cybersecurity awareness. By engaging in the game, participants gain practical knowledge, improve their problem-solving abilities, and develop a proactive mindset towards cybersecurity. The board game serves as an innovative and engaging learning tool, enabling individuals to explore and learn about cybersecurity in a dynamic and interactive way. It offers a valuable educational resource for individuals, families, and even educational institutions seeking to enhance cybersecurity awareness and promote responsible online behaviors summary, the board game provided by INCIBE offers an engaging and educational approach to cybersecurity learning. Through interactive gameplay, participants develop essential cybersecurity skills, enhance their understanding of online risks, and learn effective strategies to protect themselves and their digital assets. The analysis conducted during the workshop highlighted the game's effectiveness in promoting active learning and fostering cybersecurity awareness among participants.

The **cybersecurity podcast "Ciber Afterwork"** from Capital Radio provides a valuable resource for individuals seeking to expand their knowledge and stay updated on the latest trends in cybersecurity. Hosted by industry experts, this podcast offers insightful discussions, interviews, and analysis on a wide range of cybersecurity topics. "Ciber Afterwork" offers a convenient and accessible platform for individuals to engage with cybersecurity content. Listeners can tune in to the podcast at their own convenience, whether during their commute, while exercising, or during their leisure time. The podcast format allows for in-depth discussions and expert insights, making it an engaging and informative resource for cybersecurity enthusiasts. Each episode of "Ciber Afterwork" covers a specific aspect of cybersecurity, such as emerging threats, data breaches, cybersecurity strategies, and industry developments. The podcast features interviews with cybersecurity professionals, thought leaders, and industry experts, providing valuable perspectives and firsthand experiences. The analysis of "Ciber Afterwork" revealed its effectiveness in delivering up-to-date and relevant cybersecurity information to listeners. The podcast's engaging format, combined with expert insights, ensures that participants stay informed about the latest trends, best practices, and emerging challenges in the cybersecurity landscape. By regularly listening to "Ciber Afterwork," individuals can expand their knowledge, deepen their understanding of cybersecurity issues, and stay informed about the ever-evolving cybersecurity field. The podcast serves as a valuable resource for professionals, students, and anyone interested in staying updated on cybersecurity trends and developments. In summary, the "Ciber Afterwork" podcast from Capital Radio offers an informative and engaging platform for individuals to expand their cybersecurity knowledge. Through interviews, discussions, and expert insights, listeners gain valuable insights into the dynamic and rapidly evolving field of cybersecurity. The analysis conducted during the workshop highlighted the podcast's effectiveness in delivering timely and relevant cybersecurity information to a wide audience.

2.4 Greece

SecureSME, a cybersecurity tool used in Greece, plays a significant role in enhancing cybersecurity practices for small and medium-sized enterprises (SMEs). The tool provides a comprehensive and user-friendly platform designed to address the unique cybersecurity challenges faced by SMEs in Greece.SecureSME offers a range of features and functionalities tailored to the specific needs of SMEs. It provides tools for risk assessment, vulnerability scanning, threat intelligence, and incident response, empowering SMEs to strengthen their cybersecurity defence. The tool emphasizes proactive measures to identify and mitigate potential vulnerabilities and threats, thereby reducing the risk of cyber incidents.One key aspect of SecureSME is its user-friendly interface and intuitive navigation, ensuring that SMEs can easily navigate the platform and leverage its capabilities effectively. The tool offers step-by-step guidance and best practices to help SMEs implement robust cybersecurity measures and adhere to industry standards. The analysis of SecureSME highlighted its effectiveness in addressing the cybersecurity needs of SMEs in Greece. The tool enables SMEs to assess their cybersecurity posture, identify weaknesses, and take appropriate measures to enhance their resilience against cyber threats. By using SecureSME, SMEs can protect their sensitive data, maintain business continuity, and build trust with their customers and partners. SecureSME serves as a valuable resource for SMEs in Greece, enabling them to enhance their cybersecurity practices and navigate the evolving threat landscape. It plays a crucial role in fostering a cybersecurity culture among SMEs and raising awareness about the importance of protecting digital assets.

The online tool for the security of personal data processing offered by **ENISA** (European Union Agency for Cybersecurity) provides a valuable resource to individuals and organizations involved in processing personal data. This tool aims to assist users in assessing the risks associated with personal data processing activities and implementing appropriate security measures. By accessing the ENISA online tool, users can gain insights into the potential risks and vulnerabilities related to the processing of personal data. The tool offers a structured framework that guides users through a series of questions and assessments, allowing them to evaluate their data processing practices and identify areas of improvement. The tool considers various aspects of personal data processing, including data collection, storage, sharing, and disposal. It considers factors such as data sensitivity, potential threats, and the effectiveness of existing security measures. Based on the assessment results, users receive recommendations and best practices to enhance the security of their personal data processing activities. The analysis of the ENISA online tool revealed its effectiveness in promoting awareness and guiding users towards better security practices for personal data processing. By using this tool, individuals and organizations can assess their level of compliance with relevant data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union. The ENISA online tool offers a user-friendly interface, ensuring that users can easily navigate through the assessment process and understand the results. It serves as a valuable resource for individuals and organizations seeking to improve their data processing security and comply with data protection regulations. In summary, the online tool for the security of personal data processing provided by ENISA offers a comprehensive and accessible resource for individuals and organizations. Through its structured assessment process, the tool enables users to evaluate their data processing practices, identify potential risks, and receive recommendations to enhance security. The analysis conducted during the workshop highlighted the effectiveness of the ENISA tool in promoting better security practices for personal data processing activities.

The Cybersecurity Maturity Assessment for Small and Medium Enterprises (SME) provided by **ENISA** (European Union Agency for Cybersecurity) is a valuable resource for SMEs seeking to evaluate and enhance their cybersecurity practices. This online assessment tool aims to help SMEs assess their current cybersecurity maturity level and identify areas for improvement. By accessing the ENISA Cybersecurity Maturity Assessment tool, SMEs can navigate through a series of questions and assessments that cover various cybersecurity domains. These domains include governance, risk management, human resources, technical security measures, and incident management. The tool evaluates SMEs' cybersecurity practices against best practices and industry standards. Through the assessment process, SMEs gain insights into their cybersecurity strengths and weaknesses. The tool provides a visual representation of their cybersecurity maturity level and highlights areas where improvements are needed. Based on the assessment results, SMEs receive recommendations and guidance to enhance their cybersecurity posture. The analysis of the ENISA Cybersecurity Maturity Assessment tool revealed its effectiveness in helping SMEs identify gaps in their cybersecurity practices and develop a roadmap for improvement. By using this tool, SMEs can enhance their resilience against cyber threats, protect their sensitive data, and maintain the trust of their customers and business partners. The ENISA Cybersecurity Maturity Assessment tool offers a user-friendly interface, making it accessible to SMEs with varying levels of cybersecurity knowledge and expertise. It serves as a valuable resource for SMEs looking to enhance their cybersecurity capabilities and establish a robust security framework.

2.5 Germany

The phishing quiz offered by **BAKGAME** in Germany is a valuable tool designed to educate individuals about phishing attacks and enhance their awareness of cybersecurity risks. This interactive quiz allows users to test their knowledge and skills in identifying and avoiding phishing attempts. By accessing the BAKGAME phishing quiz, users can navigate through a series of scenarios and questions related to phishing. The quiz presents realistic phishing scenarios, simulating common tactics used by cybercriminals to deceive individuals into sharing sensitive information or clicking on malicious links. Users are challenged to identify the telltale signs of phishing and make informed decisions to protect themselves. Through the quiz, users gain insights into the various techniques employed by cybercriminals in phishing attacks. They learn about common red flags such as suspicious email addresses, grammatical errors, urgent requests, and unfamiliar URLs. The quiz provides immediate feedback, explaining the correct answers and offering tips to enhance users' phishing detection skills. The analysis of the BAKGAME phishing quiz revealed its effectiveness in educating individuals about phishing risks and equipping them with the knowledge to identify and avoid such attacks. By engaging in this interactive quiz, users develop a heightened sense of cybersecurity awareness and become more resilient against phishing attempts. The BAKGAME phishing quiz offers a user-friendly and engaging interface, making it accessible to individuals with varying levels of cybersecurity knowledge. It serves as a valuable resource for individuals, employees, and organizations looking to enhance their phishing awareness and strengthen their cybersecurity defenses. In summary, the phishing quiz provided by BAKGAME in Germany is an effective tool for raising awareness about phishing attacks and improving users' ability to recognize and respond to such threats. By engaging in this interactive quiz, users can enhance their cybersecurity knowledge and develop the skills needed to protect themselves and their sensitive information from phishing attempts. The analysis conducted during the workshop highlighted the significance of the BAKGAME phishing quiz in promoting phishing awareness and empowering individuals to safeguard against these types of cyber threats.

The website "**Have I Been Pwned**" is a valuable online tool that helps individuals assess their exposure to data breaches and compromised accounts. By visiting haveibeenpwned.com, users can check if their email addresses or usernames have been involved in known data breaches. Through this tool, users can enter their email address or username, and the website cross-references this information with a comprehensive database of breached accounts. If a match is found, users receive a notification indicating which data breaches their accounts have been compromised in. This information allows users to take appropriate actions, such as changing passwords, enabling two-factor authentication, and monitoring their accounts for suspicious activity. The analysis of the "Have I Been Pwned" website revealed its effectiveness in raising awareness about the prevalence of data breaches and the importance of maintaining strong security practices. By providing users with information about compromised accounts, the website empowers individuals to take proactive measures to protect their personal information and prevent unauthorized access to their accounts. The "Have I Been Pwned" website offers a user-friendly interface and operates with a strong focus on privacy and security. It does not store or collect sensitive information during the account checking process, ensuring user confidentiality. This commitment to privacy and security contributes to the trustworthiness and reliability of the tool. In summary, "Have I Been Pwned" is a valuable online tool that allows individuals to assess their exposure to data breaches and compromised accounts. By providing notifications about breached accounts, the tool enables users to take necessary steps to secure their accounts and protect their personal information. The analysis conducted during the workshop highlighted the significance of "Have I Been Pwned" in promoting cybersecurity awareness and empowering individuals to take control of their online security.

3 Key findings and insights

3.1 Tools selected

Among the tools selected, we have identified some notable choices. From France, the learning tool called "Rootmee" demonstrated its effectiveness in providing hands-on practical exercises and simulations to develop cybersecurity skills. It offers a comprehensive learning experience that covers various aspects of cybersecurity, such as network security, encryption, and threat detection.

Another noteworthy tool is "Hackademics," which was presented from Germany. This platform stands out for its interactive and gamified approach to cybersecurity learning. It engages users through challenges, puzzles, and simulated hacking scenarios, fostering an immersive and engaging learning environment.

From Spain, the board game offered by "Incibe" showcased its ability to create a collaborative and educational experience. This interactive game allows players to navigate real-life cybersecurity scenarios, make informed decisions, and learn from the consequences of their actions.

In Greece, "SecureSME" emerged as a valuable tool for small and medium enterprises (SMEs) to enhance their cybersecurity practices. It provides tailored resources and guidance specifically designed to address the unique challenges faced by SMEs in securing their digital assets and protecting against cyber threats.

Lastly, the online tool called "Cybersecurity Maturity Assessment for SMEs" offered by ENISA (European Union Agency for Cybersecurity) stands out for its comprehensive evaluation framework. It enables SMEs to assess their cybersecurity maturity level, identify gaps, and develop a roadmap for improving their cybersecurity practices.

These selected tools have been recognized for their ability to enhance cybersecurity knowledge, skills, and awareness. They offer diverse learning approaches and cater to different learning preferences. The insights gained from these tools contribute to a well-rounded and comprehensive learning experience in cybersecurity.

3.2 Workshop results review and analysis

The workshop on learning tools in cybersecurity yielded significant results and provided valuable insights into the effectiveness and applicability of various resources. Through interactive discussions and practical demonstrations, participants engaged in a thorough analysis of the presented tools, leading to several key observations. More details can be found in the Training Report (see appendix: Training Report September 2023)

Firstly, the workshop highlighted the importance of tailoring learning experiences based on participants' existing knowledge and skill levels. By categorizing participants into three groups based on their cybersecurity expertise, a learner journey was created to ensure that each individual received appropriate guidance and relevant content.

Furthermore, the workshop emphasized the significance of international collaboration and exchange of best practices. Each partner shared their country-specific learning tools, fostering a collaborative environment where participants could explore different perspectives and identify suitable resources for their respective learner categories.

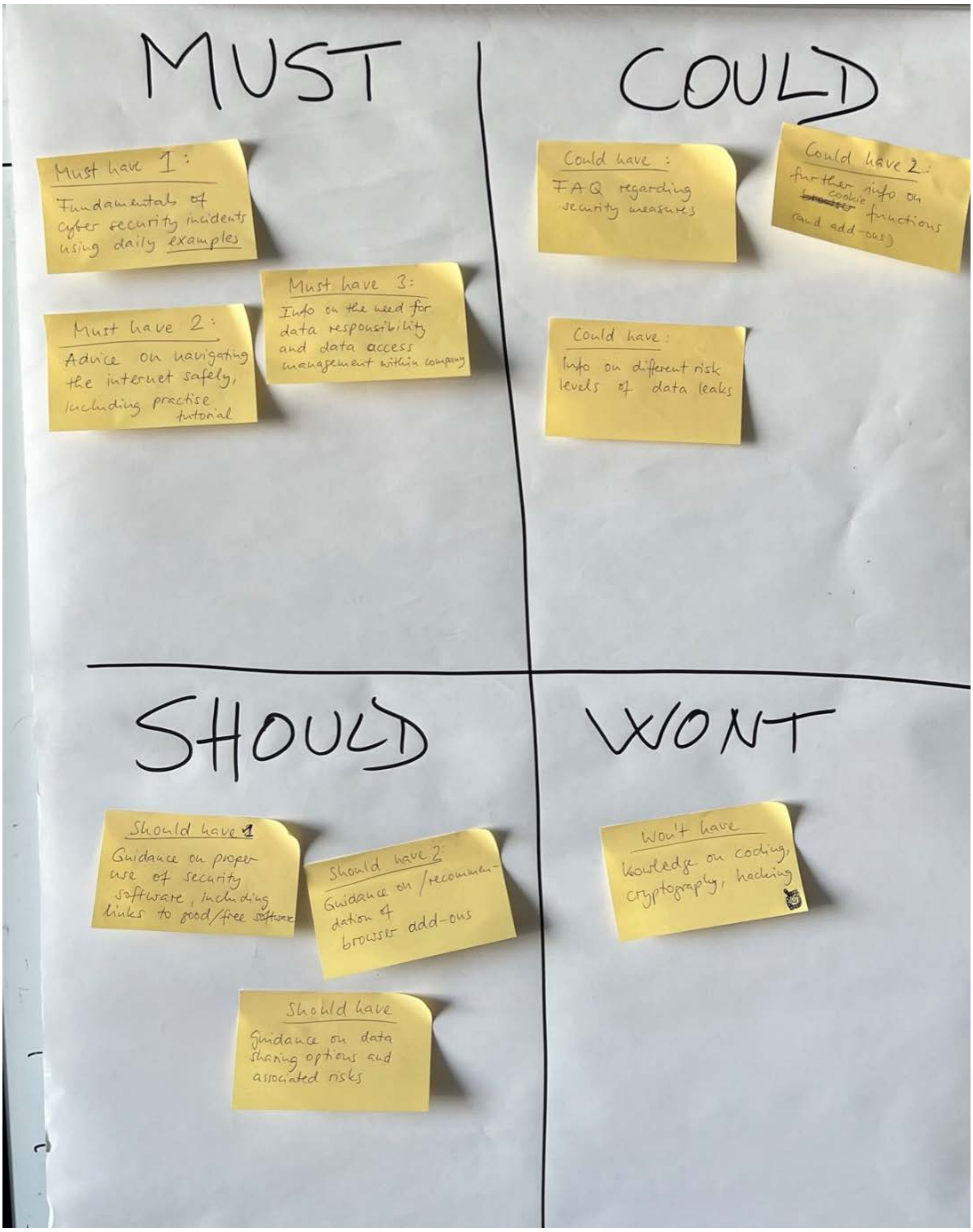
The analysis of learning tools showcased a diverse range of options, catering to various learning preferences and objectives. Tools such as "Rootmee" from France, "Hackademics," and the "Introduction to Cybersecurity" course from Cyprus exhibited unique features and strengths, addressing different aspects of cybersecurity education. These tools offered engaging and interactive learning experiences, covering theoretical foundations, practical application, and gamified learning approaches.

The workshop's findings highlighted the need for continuous evaluation and improvement of learning tools to ensure their effectiveness in enhancing the learning experience. Through thorough analysis, it was evident that a combination of theoretical knowledge, practical exercises, and gamified elements contributed to a comprehensive and engaging learning environment.

The workshop results and analysis underscored the significance of learning tools in cybersecurity education. The evaluation of various resources and the collaborative exchange of ideas fostered a dynamic and informed approach to selecting appropriate tools. The insights gained from this workshop will contribute to the ongoing enhancement of learning methodologies, ensuring that participants receive high-quality education and develop the necessary skills to thrive in the cybersecurity domain.

4 Integration of Learning Tools into Learner Journeys

In a first step, the workshop participants discussed the rough concept of each level in three groups. To achieve a first understanding, each group decided what must/could/should/won't be part of the training on their according level (see figure 1-3). These aspects included mostly learning contents and methods that are in line with these contents (e.g. basic safety advice on browsing the internet and presentation of incidents examples for level 1 learners).



MUST

Must have 1:
Fundamentals of cyber security incidents using daily examples

Must have 2:
Advice on navigating the internet safely, including practise tutorial

Must have 3:
Info on the need for data responsibility and data access management within company

COULD

Could have:
FAQ regarding security measures

Could have 2:
further info on ~~browser~~ cookie functions (and add-ons)

Could have:
Info on different risk levels of data leaks

SHOULD

Should have 1
Guidance on proper use of security software, including links to good/free software

Should have 2:
Guidance on /recommendation of browser add-ons

Should have
Guidance on data sharing options and associated risks

WONT

Won't have
Kowledge on coding, cryptography, hacking

Figure 1: Level 1 aspects according to method

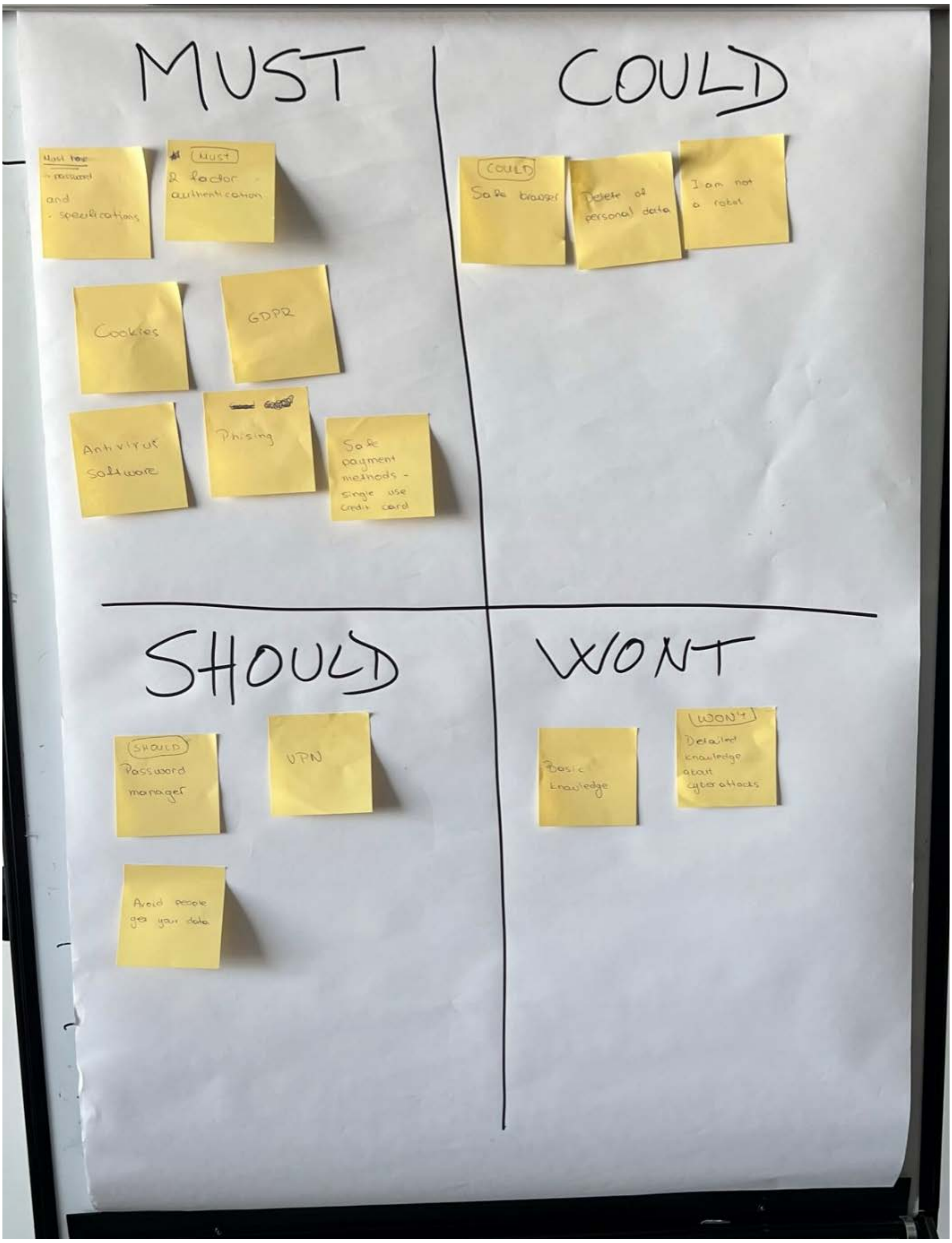


Figure 2: Level 2 aspects according to method

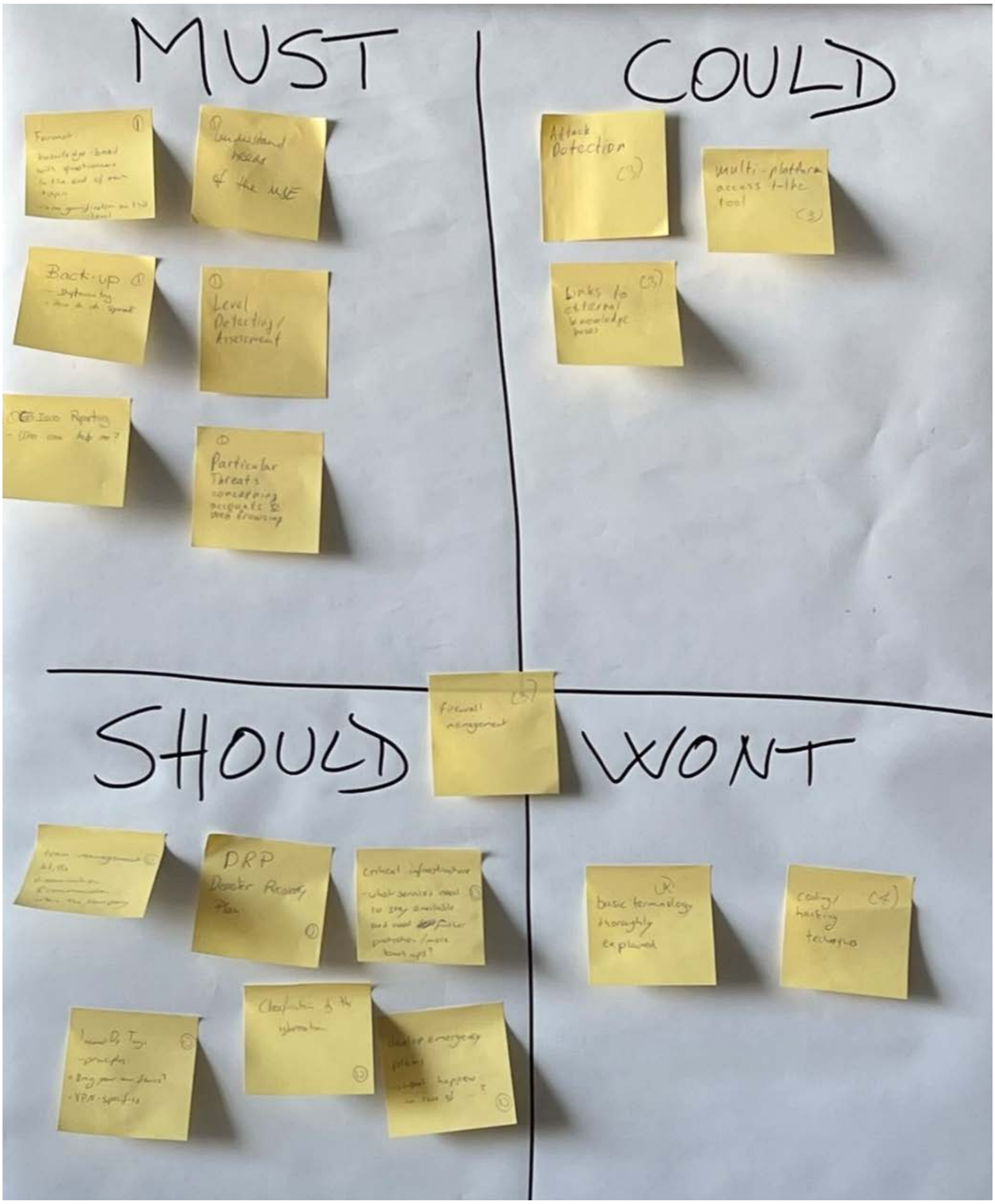

MUST
COULD
SHOULD
WONT
Back-up
Level Detecting / Assessment
Particular Threats concerning accounts & web browsing
Attack Detection (3)
multi-platform access to the tool (3)
Links to external knowledge bases (3)
firewall management (3)
DRP Disaster Recovery Plan
Critical infrastructure
basic terminology thoroughly explained
coding / hashing techniques (4)

Figure 3: Level 3 aspects according to method

The results were presented and discussed in plenary session. As a next step, the groups continued working on the learner journeys for each level. The participants considered the ideas created in the first step as a basis for aligning relevant learning tools among a learner journey tailored to the specific target group on the respective level. In this way, contents were organized in chronological order together with relevant learning tools. The drafts created in the workshop will serve as a basis for creating the detailed learner journey prototypes.

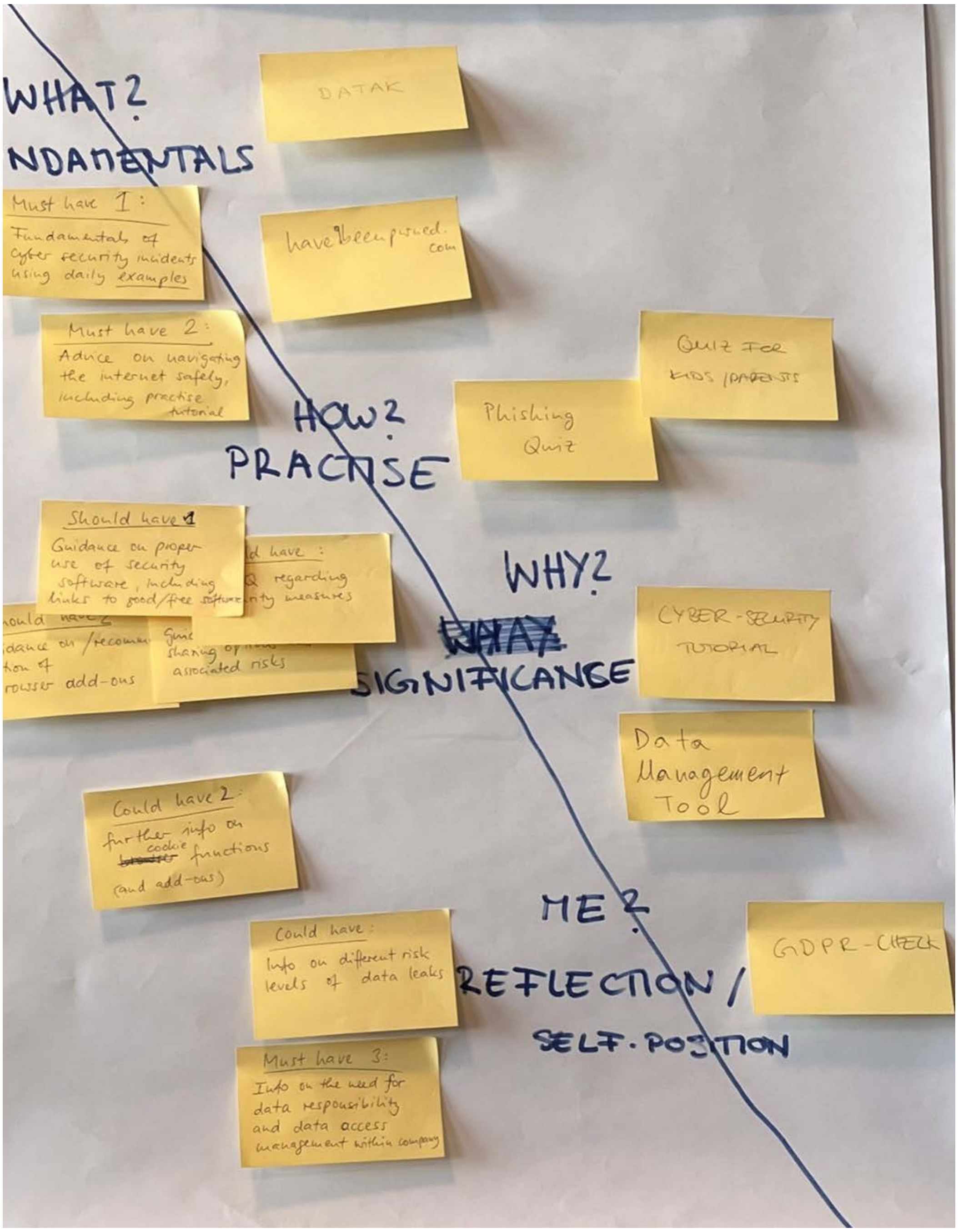

WHAT?
NDAMENTALS
DATAK
Must have 1: Fundamentals of cyber security incidents using daily examples
havebeenpwned.com
Must have 2: Advice on navigating the internet safely, including practise tutorial
HOW?
PRACTISE
Phishing Quiz
Quiz for kids/parents
Should have 1 Guidance on proper use of security software, including links to good/free software
d have: Q regarding rity measures
ould have 2 dance on/recommen tion of rowser add-ons
sharing op associated risks
WHY?
~~WHAT~~
SIGNIFICANCE
CYBER-SECURITY TUTORIAL
Data Management Tool
Could have 2: further info on cookie functions (and add-ons)
ME?
REFLECTION / SELF-POSITION
Could have: Info on different risk levels of data leaks
GDPR-CHECK
Must have 3: Info on the need for data responsibility and data access management within company

Figure 4: Level 1 Learner Journey Draft

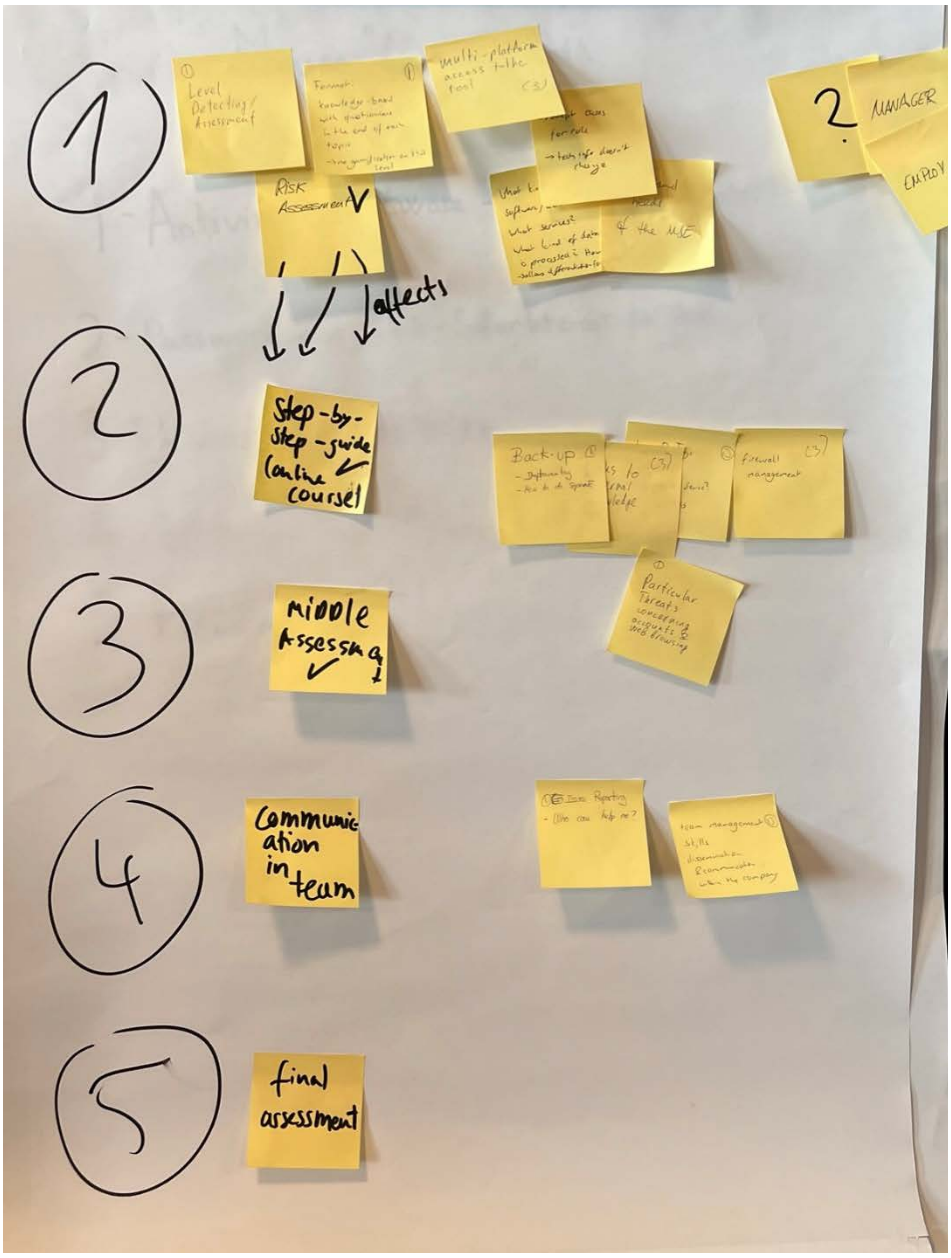

1
Level Detecting/ Assessment
Format: knowledge-based with questionnaire in the end of each topic
multi-platform access to the tool
for role
Risk Assessment
of the MSE
What services?
affects
2
MANAGER
EMPLOY
2
Step-by-step-guide (online course)
Back-up
firewall management
3
Middle Assessment
Particular Threats concerning accounts & web browsing
4
Communication in team
Issue Reporting
- Who can help me?
team management
skills
5
final assessment

Figure 5: Level 3 Learner Journey Draft

5 Conclusion

In conclusion, the workshop provided a platform for sharing insights, exploring innovative resources, and fostering collaboration in the field. The knowledge and information obtained during the workshop will shape the future direction of cybersecurity education, ultimately leading to a more informed and prepared workforce capable of addressing emerging cybersecurity challenges.

Through collaborative discussions and presentations, participants explored different learning platforms, games, tutorials, online resources and gained valuable insights and information regarding various tools and resources available in the field. The workshop revealed the importance of incorporating diverse learning approaches and tools to enhance cybersecurity education and awareness.

Overall, the workshop underscored the need for continuous learning and adaptation in the rapidly evolving field of cybersecurity. It demonstrated the importance of collaboration between educators, industry stakeholders, and participants to identify and address gaps in cybersecurity training and awareness.

The insights gained from the workshop will serve as a foundation for future improvements in cybersecurity education and the development of effective learning strategies. The analysis of the tools and resources presented will guide educators, organizations, and stakeholders in selecting appropriate learning tools and integrating them into their educational practices.

By leveraging the knowledge and experiences shared during the workshop, participants can work towards strengthening cybersecurity awareness, enhancing training programs, and fostering a cybersecurity culture. This collective effort will contribute to building a more resilient and secure digital environment.