CYBARVERSE

DIGITAL LITERATE IN VET BY CYBERSECURITY TRAINING WITH IMMERSIVE TECHNOLOGIES

BEST PRACTICE GUIDE

Co-funded by
the European Union

INTRODUCTION

1.1 The project and its goals

The CybARverse project, launched under the Erasmus+ program, is designed to enhance the standards of digital literacy and cybersecurity skills through the use of immersive technologies within vocational education and training (VET). Led by Asociacija "Langas į ateitį" in Lithuania and in partnership with S.C.P. Serv Limited and the Cyprus Computer Society in Cyprus, Tech.mt in Malta, and Fundatia EOS - Educating for an Open Society in Romania, the project aims to address the existing digital skill gaps by incorporating state-of-the-art Augmented Reality (AR) and Virtual Reality (VR) technologies into VET curricula. This approach not only enriches the learning experience but also equips educators and trainers with the necessary tools to impart essential cybersecurity skills, thereby enhancing the resilience of educational environments against cyber threats.

CYBARVERSE

Co-funded by the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission nor National Agency cannot be held responsible for any use which may be made of the information contained therein.

https://www.cybarverse.eu/

TABLE OF CONTENTS

INTRODUCTION

The CybARverse project is structured around four primary objectives, each aimed at fostering a comprehensive and sustainable impact within the realm of cybersecurity education:

Enhancing Professional, Personal, and Digital Competencies:

- Professional Development: Equip educators and trainers with cutting-edge cybersecurity knowledge and practices to address and mitigate evolving cyber threats efficiently.
- Personal Growth: Foster essential skills such as critical thinking, problem-solving, and decision-making through interactive and scenario-based learning experiences.
- Digital Fluency: Advance the digital capabilities of VET professionals, with a particular focus on the proficient use of AR and VR technologies to simulate and respond to cybersecurity challenges.

Integration of Modern and Immersive Technologies:

- Implement AR and VR to craft dynamic, engaging training environments that simulate real-world cybersecurity scenarios, offering practical, hands-on learning experiences surpassing traditional educational methods.

Structured Professional Qualification:

- Develop a comprehensive, tiered training program that systematically enhances cybersecurity awareness and expertise, from foundational knowledge to advanced operational skills.

Sustainability of Educational Impact:

- Establish a sustainable educational model that includes ongoing professional development and updates to the training materials, ensuring the curriculum remains current with the fast-paced evolution of cybersecurity threats and technologies. Additionally, promote a community of practice that supports ongoing learning and the sharing of best practices among cybersecurity educators.

By adhering to these detailed goals, the CybARverse project endeavours to create a robust educational framework that not only meets current needs but also adapts to future demands in the field of cybersecurity training.

INTRODUCTION

1.2 Pedagogical Guidelines - Understanding the role of Pedagogical Guidelines within the CybARverse Project

As part of the comprehensive approach to enhancing cybersecurity education within the vocational education and training (VET) framework, the CybARverse project has developed an essential document titled “Pedagogical Guidelines.” This document serves as a key role in guiding VET educators on effective ways to integrate advanced digital and immersive technologies into their teaching practices.

1.3 Purpose and Impact of the Pedagogical Guidelines

The Pedagogical Guidelines are designed to provide educators and trainers with a detailed understanding of how to employ augmented reality (AR) and virtual reality (VR) technologies in a pedagogically sound manner. These guidelines are essential for achieving the primary objectives of the CybARverse project:

- Enhancement of Digital Skills: By detailing the application of AR and VR in educational settings, the guidelines equip educators with the skills to effectively incorporate these technologies into their curricula, thus enhancing the digital competencies of learners.
- Structured Learning Paths: The guidelines outline structured approaches to using immersive technologies, ensuring that the training delivered is both systematic and comprehensive. This helps in building a well-qualified cadre of VET educators who are adept in cybersecurity and digital literacy.
- Promotion of Engaging Educational Practices: Through innovative teaching methods suggested in the guidelines, educators can create more engaging and interactive learning experiences. This not only improves the quality of education but also makes learning more appealing and effective for students.
- Sustainability of Educational Practices: The guidelines advocate for ongoing updates and adaptations in teaching strategies to keep pace with technological advancements. This approach ensures that the educational content remains relevant and that the benefits of the project are sustained over time.

While the Pedagogical Guidelines stand as an independent deliverable within the CybARverse project, they complement the broader goals outlined in the “Best Practice Guide” by providing practical applications of the theoretical frameworks discussed. Educators who use the Best Practice Guide will find the Pedagogical Guidelines to be an invaluable resource for implementing the recommended practices effectively.

INTRODUCTION

The “Pedagogical Guidelines” are not just a set of instructions; they are a transformative tool that empowers educators to utilize the potential of modern technologies for cybersecurity education. By detailing the effective use of AR and VR, these guidelines help bridge the gap between traditional teaching methods and the demands of the digital age.

The reference to these guidelines in the Best Practice Guide underscores the CybARverse project’s commitment to a holistic educational strategy that is both forward-thinking and grounded in practical application. This discussion highlights the interconnection between the two documents and their collective impact on enhancing educational practices.

The pedagogical guidelines document can be consulted here.

1.4 Overview of training levels

The CybARverse project offers three progressive training levels, each designed to cater to the varying degrees of familiarity and expertise with digital technologies and cybersecurity among participants:

- **Beginner Level:** This initial stage introduces fundamental concepts of digital literacy and cybersecurity, targeting educators and trainers who are novices in the digital realm. It lays the groundwork for more complex learning.
- **Intermediate Level:** This level expands on the foundational knowledge, exploring more intricate cybersecurity protocols and digital practices. Participants engage with interactive AR and VR scenarios that simulate real-world cyber threats, which enhances their analytical and problem-solving skills.
- **Advanced Level:** The most advanced stage is tailored for participants who have a robust understanding of digital tools and cybersecurity. It focuses on specialized areas such as threat analysis, advanced coding techniques, and the strategic implementation of cybersecurity measures in educational settings.

https://www.cybarverse.eu/

INTRODUCTION

1.5 Brief description of course content and structure

The training framework of the CybARverse project is meticulously structured to offer a thorough educational experience that is both engaging and informative. The course content is strategically developed to build proficiency in both digital literacy and practical cybersecurity applications, augmented by innovative AR and VR technologies.

- **Course Content:** The curriculum encompasses a blend of theoretical knowledge and practical cybersecurity skills, along with a deep dive into AR and VR technologies and their application in educational settings. Each module is crafted to build on the previous one, enhancing the depth of knowledge and skill level with each progression.
- **Course Structure:** The course is modular, allowing for a focused approach to each aspect of cybersecurity and digital literacy. It integrates interactive elements like VR and AR simulations, workshops, and live webinars led by field experts. Comprehensive assessments follow each module to ensure participants' understanding and readiness for subsequent levels.
- **Interactive Components:** Utilising AR and VR technologies, the course creates realistic scenarios where participants can apply their cybersecurity skills in a virtual yet lifelike environment. This method not only solidifies their learning but also prepares them to effectively handle similar challenges in real-world contexts.

In addition to the core curriculum, the CybARverse project includes continuous professional development components, enabling educators and trainers to keep up with the latest cybersecurity trends and technological advancements. This ongoing learning process ensures that the teaching methodologies remain current and effective, further strengthening the overall cybersecurity posture of their respective educational environments.

By integrating these advanced technological tools with expertly designed educational content, the CybARverse Best Practice Guide aims to equip VET educators and trainers with the necessary skills to effectively teach cybersecurity, thereby contributing to the creation of a safer digital future. Through fostering an ecosystem of continuous learning and adaptation, CybARverse ensures that its beneficiaries are well-prepared to lead and innovate in the ever-evolving digital landscape, ultimately enhancing their educational impact and effectiveness.

LEARNING MANAGEMENT SYSTEM (LMS)

The course content is available on the LearnPress Learning Management System (LMP). It is one of the most widely used LMS for online courses, providing opportunities to create a course curriculum with lessons and quizzes, and which contains easy-to-use interface for learners and users.

2.1 Course design and structure

Course design and structure is designed to be the modular course, allowing for a focused approach to each aspect of cybersecurity and digital literacy. It integrates interactive elements like VR and AR simulations, workshops, and live webinars led by field experts. Comprehensive assessments follow each module to ensure participants' understanding and readiness for subsequent levels.

The course covers 17 learning modules that are divided into three different levels, so learners can choose the ones that are most relevant to them.

Beginners level covers six essential cybersecurity topics for beginners with the learning volume of 6 hours:

- introduction to malware,
- social engineering,
- grooming,
- social media threats,
- phishing,
- and Internet of Things (IoT) attacks.

Intermediate level delves into six advanced cybersecurity threats with the learning volume of 8 hours:

- ransomware,
- rootkits,
- pharming,
- cryptojacking,
- cross-site scripting,
- and SQL injection.

Advanced level focuses on 5 complex cybersecurity threats with the learning volume of 10 hours:

- man-in-the-middle attacks,
- Internet of Things (IoT) vulnerabilities,
- zero-day exploits,
- DoS attacks,
- and DDoS attacks.

Each module contains the same structure:

1. Theoretical readings that cover the description of the threat itself, the features allowing to recognize the threat and the means of risk mitigation and/or prevention. The theoretical materials are provided in a structured, yet comprehensive, way for the learner to get a deeper understanding of the threat.
2. Several case studies to better understand the relevance of the described threat in today's online world.
3. Interactive Components - videos, AR/VR/WebVR technologies, which allow to create realistic scenarios where learners can apply their cybersecurity skills in a virtual yet lifelike environment.
4. Each module includes lesson plans to simulate and understand these threats, also to provide the knowledge further to learners.
5. Each course level concludes with an exam designed for VET trainers to evaluate their knowledge gained and expertise. Passing the exam is necessary to receive the course certificate.

2.2. Effective online learning strategies

The course developed by the project can be used for self-paced individual learning, or the VET institution can organise online or blended courses for the whole group. Learners could receive support from the instructor on both the subject and the use of the LMS and resources.

2.2.1 For Instructors and Educators

The following points should be considered when organising training using the material in this online course.

- **Course Design and Structure**
  - **Clear Objectives**: Define clear learning objectives and outcomes for each module. This helps students understand what they are expected to learn and achieve.
  - **Modular Content:** the course content is broken into manageable modules or units. Each module should cover a specific topic or skill in cybersecurity.
  - **Interactive Elements**: every module incorporates interactive elements such as quizzes, demonstrations, simulations, case studies and VR/AR hands-on labs. These activities help reinforce learning and keep students engaged.
  - **Multimedia Resources**: use multimedia resources, including available in the course or online videos, to cater to different learning styles.

LEARNING MANAGEMENT SYSTEM

- **Engagement and Interaction**
  - **Discussion Forums**: create discussion forums (e.g. on social network) where students can ask questions, share insights, and collaborate. Encourage active participation by posing thought-stimulation questions.
  - **Live Sessions**: schedule regular live sessions (webinars or virtual classrooms) to provide real-time interaction and feedback. Use these sessions for Q&A, discussions, and guest lectures from industry experts.
  - **Feedback Mechanisms**: monitor learners' progress and provide timely and constructive feedback.

- **Assessment and Evaluation**
  - **Formative and Summative Assessments**: every course has final quiz as summative assessment, but the instructor can use own short assignments to gauge student understanding throughout the course. This allows for timely intervention if needed.

- **Technical Support and Resources**
  - **Technical Guidance**: Provide clear instructions and support for using the online learning platform and tools. Offer tutorials and FAQs to help students navigate the technology.
  - **Resource Accessibility**: Ensure that all course materials are accessible to students with disabilities. Use accessible formats and provide alternative resources when necessary.

- **Integration of Online and Offline Activities**
  - **Seamless Transition**: Ensure a seamless transition between online and offline activities. Align online modules with in-person sessions to reinforce learning.
  - **Hybrid Assignments**: Design assignments that require both online research and offline application. This helps students integrate knowledge from various sources.

2.2.2 For Participants

1. **Time Management**
   - **Set a Schedule**: Create a study schedule that includes dedicated time for attending live sessions, completing assignments, and reviewing course materials. Stick to this schedule to stay on track.
   - **Prioritise Tasks**: Prioritise tasks based on deadlines and importance. Use tools like to-do lists and calendars to manage your workload effectively.
2. **Active Participation**
   - **Engage in Discussions**: Actively participate in discussion forums and live sessions. Share your insights, ask questions, and collaborate with peers.
   - **Seek Feedback**: Don't hesitate to seek feedback from instructors and peers. Use this feedback to improve your understanding and performance.
3. **Self-Motivation and Discipline**
   - **Set Goals**: Set specific, achievable goals for each study session. This helps maintain focus and motivation.
   - **Stay Disciplined**: Maintain discipline by minimizing distractions during study time. Create a conducive learning environment that is free from interruptions.
4. **Utilize Resources**
   - **Leverage Multimedia**: Take advantage of the multimedia resources provided in the course. Watch videos and visual resources to reinforce your learning.
   - **Practice Hands-On Skills**: Engage in VR/AR simulations to apply theoretical knowledge to practical scenarios. This is especially important in cybersecurity training.

2.3. Accessibility and inclusivity considerations for diverse learners

Creating accessible and inclusive learning materials and websites is essential to ensure that all learners, regardless of their abilities or backgrounds, can fully participate and benefit from the educational experience. While the project offers ready-made learning materials, these will need to be updated, can be localised in other countries, and will be used by different educators to deliver e.g. blended learning courses.

2.3.1 Accessibility - Key Consideration

Here are some key considerations for course development and application:

1. Universal Design for Learning (UDL)

Universal Design for Learning (UDL) is an educational framework that aims to create a learning environment that accommodates all learners. The principles of UDL include:

- **Multiple Means of Representation**: Provide information in various formats such as text, videos, audio recordings, and interactive elements to cater to different learning preferences.
- **Multiple Means of Expression**: Allow learners to demonstrate their knowledge in various ways, such as written assignments, presentations, or projects.
- **Multiple Means of Engagement**: Encourage motivation and engagement by offering diverse activities and tasks that align with learners' interests and needs.

2. Accessibility

Ensuring accessibility means making learning materials available to everyone, including individuals with disabilities. Key aspects include:

- **Alternative Text for Visual and Audio Content**: Provide text descriptions for images and captions for videos to ensure that all content is accessible.
- **Appropriate Colour Contrast**: Use colour combinations that are easy to read and understand, especially for individuals with visual impairments.
- **Screen Reader Compatibility**: Ensure that websites and documents are compatible with screen readers to assist visually impaired learners.
- **Keyboard Navigation**: Make sure that the website can be easily navigated using only a keyboard, which is crucial for individuals with motor impairments.

In practice, the design of the website and educational material is based on the main WCAG 2.0 guidelines, of which the following are important and can be simply implemented:

- Ensure that the text is easy to read by using sufficient contrast between the text and the background. Background should be avoided if it is not necessary.
- Use larger fonts and allow users to change the font size as required. Use a clear and simple font such as Arial or Verdana. Avoid italics and underlining, which can make reading difficult.
- Heading styles define the structure of the text and so should be used consistently from top level to the lower one; they are not decorative elements to highlight the text.
- Never use any texts (such as titles, menus, adds) as images. Such information can ‘t be readable by screen readers and cannot be resizable in many cases.
- Attached documents: Make sure the attached documents are compatible with the screen readers. PDF documents can be adjusted with the online tool https://pave-pdf.org/index.html?lang=en
- Visual material: add alt text to all images (except decorative items) to allow screen readers to describe the image. Use clear and understandable illustrations and diagrams.
- Video and audio material: add subtitles to all videos. Provide transcripts for audio tracks.
- Navigation and structure: ensure that the website is easy to navigate using the keyboard. Use a clear and logical site structure with consistent menus and links.
- Open materials online accessibility can be checked using online tool https://www.accessibilitychecker.org/

3. Language and Imagery

Using inclusive language and imagery helps all learners feel valued and included:

- **Easy to understand**: use short sentences and paragraphs. Put the most important information at the beginning. Use lists and bullet points to make the information easier to understand.
- **Inclusive Language**: Avoid gender bias and stereotypes. Use neutral and inclusive language that respects all individuals.
- **Diverse Imagery**: Use images that reflect different cultures, abilities, and backgrounds to represent the diversity of the learning community.

4. Technology Accessibility

Ensure that all learners have access to the necessary technology:

- **Technology Access**: Provide learners with access to the required tools and reliable internet connections. As learners rarely have personal access to VR and AR equipment, they need to be offered an agreed time when they can use it at the VET institution and get the technical support they need.
- **International Restrictions**: Consider international specifics on technology use and ensure that materials are accessible to all learners, regardless of their location.

5. Time Accessibility

Consider learners' time constraints:

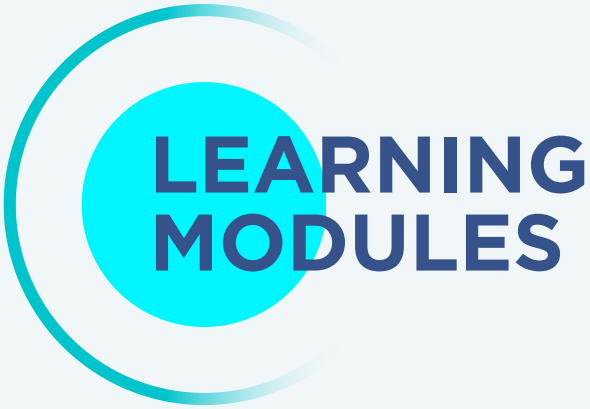
- **Flexible Timing**: Offer flexible deadlines and opportunities to review materials at any time to accommodate different schedules.

2.3.2 Recommendations

Augmented and virtual reality (AR and VR) can be especially useful in training, but it is important to ensure that these technologies are safe for people with disabilities. Here are some recommendations:

1. **Physical safety:**
   - Ensure that users have sufficient space to move around and are protected from obstacles.
   - Provide instructions on how to use the equipment safely and supervise users to avoid possible injuries.
2. **Emotional safety:**
   - Use simple and less stimulating VR environments to avoid excessive sensory overload that can cause stress or anxiety.
   - Avoid bright lights and fast-moving images.
   - Continuously monitor students' physical and emotional well-being using VR technology. Long-term use of VR can lead to short-term cognitive impairments such as attention disorders, memory problems and difficulty orienting in real-world environments.
   - Allow students to withdraw from a session at any time if they feel uncomfortable or experience discomfort.

By following these recommendations, an accessible and inclusive learning environment can be developed where all learners can thrive and reach their full potential.



3.1 Incorporating case studies

For VET trainers, the integration of case studies into the CybARverse learning modules offers a powerful tool to enhance the teaching of cybersecurity concepts. Case studies serve as practical, real-world examples that allow trainers to move beyond theoretical instruction and engage their learners in solving real-life cybersecurity problems. These carefully crafted scenarios provide a first hand approach to understanding how cyber threats unfold and the steps needed to mitigate them, making them an essential part of the curriculum for trainers aiming to equip their students with actionable skills.

The CybARverse online Learning Management System (LMS) includes a wide range of detailed lesson plans, each built around specific case studies that cover various types of cybersecurity incidents. These 45-minute lesson plans are designed to be flexible and can be adapted to different teaching styles and levels of expertise. Trainers can access these resources through the LMS, allowing them to easily integrate case studies into their existing curricula. Each lesson plan outlines the objectives, learning outcomes, and step-by-step guidance for delivering the case study, ensuring that trainers can effectively lead discussions, facilitate problem-solving activities, and assess learner understanding.

The case studies are organised to address a variety of cybersecurity topics, such as malware, phishing attacks, ransomware incidents, and social engineering tactics. For each scenario, the lesson plans include background information and key cybersecurity examples, to guide learners through the analysis of the case. This structure helps trainers emphasise critical thinking and decision-making, as learners explore how and why security breaches occur and what can be done to prevent them. Moreover, the lesson plans include sessions for group discussions and collective problem-solving, where trainers can help their learners develop both technical expertise and the soft skills necessary for success in cybersecurity roles.

The LMS also provides trainers with the ability to track learner progress through assessments tied to each case study. These assessments, which range from quizzes to practical exercises, help trainers evaluate their learners' grasp of the material and identify areas for further development. The platform's analytics tools offer insights into how learners are performing, allowing trainers to tailor their instruction to better meet the needs of their students.

For VET trainers, the incorporation of case studies is not just about teaching cybersecurity concepts—it's about giving learners the opportunity to apply these concepts in realistic scenarios. By leveraging the lesson plans and resources available through the CybARverse LMS, trainers can offer an engaging and impactful learning experience that prepares their students for the challenges of the modern cybersecurity landscape.

The flexibility and accessibility of the case study resources ensure that trainers can easily integrate them into their teaching, while the LMS platform provides all the tools necessary to monitor learner progress, facilitate discussions, and deliver effective instruction. It should be highlighted that the LMS is available in 5 languages (English, Greek, Lithuanian, Maltese and Romanian).

3.2 Real-world scenarios for applied learning

For VET trainers, incorporating real-world scenarios into cybersecurity training is crucial for providing learners with practical, hands-on experience. The CybARverse learning modules are designed to present real-world cyber incidents, allowing learners to apply theoretical knowledge in realistic, controlled environments. This method of applied learning bridges the gap between classroom instruction and the dynamic challenges faced by cybersecurity professionals, making it an essential component of the training process.

The online Learning Management System (LMS) of the CybARverse project offers examples of real-world scenarios that trainers can easily integrate into their lessons. Each scenario is carefully crafted to reflect current cybersecurity threats, such as social engineering, pharming, SQL injection incidents, and Zero-day attacks. These scenarios are accompanied by detailed lesson plans that outline the objectives, step-by-step instructions, and expected outcomes, allowing trainers to smoothly incorporate them into their teaching.

Each real-world scenario is designed to be adaptable for different skill levels, making it suitable for VET trainers working with learners at varying stages of their cybersecurity education. For beginners, the scenarios might involve straightforward tasks such as identifying common phishing attempts or basic malware detection. For more advanced learners, scenarios can become increasingly complex, requiring them to manage sophisticated attack vectors, such as advanced persistent threats (APTs) or multi-vector attacks, where rapid decision-making and the application of advanced cybersecurity protocols are critical.

Trainers can use these real-world scenarios to foster active participation and engagement. Learners are encouraged to collaborate with peers to resolve the simulated cyber incidents, mimicking the teamwork required in professional cybersecurity settings. These collaborative exercises enhance communication skills and promote a deeper understanding of how cybersecurity professionals must work together to mitigate and prevent cyber threats in real-time.

Integrating real-world scenarios into the CybARverse learning modules offers VET trainers an effective way to provide applied learning experiences. The structured, scenario-based approach available through the LMS ensures that learners are not only exposed to theoretical cybersecurity concepts but also to the practical realities of defending against cyber threats. By using these tools, trainers can foster a deeper, more interactive learning experience that equips their learners with the skills needed to navigate the ever-evolving landscape of cybersecurity.

3.3 Leveraging videos for engaging learning experiences

The use of video content is a powerful method to create engaging and immersive learning experiences in the CybARverse project's cybersecurity curriculum. Videos serve as an effective medium for illustrating complex cybersecurity concepts, demonstrating real-world applications, and keeping learners actively engaged throughout the training process. By incorporating short videos into their lessons, trainers can enhance the depth and quality of their instruction, providing learners with visual and auditory examples that are easier to understand and retain.

The CybARverse Learning Management System (LMS) offers nine short videos for some scenarios that trainers can seamlessly integrate into their courses. These videos available on the CybARverse YouTube Channel cover the following topics: Social Engineering, Malware, Phishing, Social Media Threads and Grooming from the Beginner Level and Ransomware, Pharming and Cross-Site Scripting (XSS) from the Intermediate Level, ensuring that VET trainers have access to high-quality materials suitable for learners at different skill levels. The videos are designed to complement theoretical lessons and applied learning activities, making them a versatile tool for enhancing both comprehension and engagement.

This visual learning approach helps demystify complex concepts, making them more accessible to learners, particularly those who may struggle with purely text-based materials. Trainers can use these videos as discussion starters, encouraging learners to analyse the decisions made and propose alternative solutions.

Videos also serve as a valuable tool for diversifying the learning experience, catering to different learning styles. Visual learners benefit from seeing concepts demonstrated in action, while auditory learners can absorb information through expert voiceovers and explanations. Trainers can use this flexibility to create a more inclusive learning environment, ensuring that their instruction resonates with a wider range of learners. The LMS also offers accessibility features, such as subtitles and transcripts, making the video content accessible to learners with hearing impairments or those who prefer reading along while watching.

3.4 Integration of immersive technologies (VR/AR)

The integration of immersive technologies, particularly Virtual Reality (VR) and Augmented Reality (AR), into the CybARverse learning modules represents a transformative approach to cybersecurity education for VET trainers and their learners. These technologies create highly interactive and engaging learning environments that allow learners to experience complex cybersecurity scenarios firsthand. By leveraging VR and AR, trainers can enhance the practical application of cybersecurity concepts, making the training experience both more impactful and memorable.

One of the primary benefits of VR and AR technologies is their ability to immerse learners in realistic scenarios. For example, a VR module might simulate a corporate environment where learners must identify and respond to a phishing attack or a ransomware incident. By actively participating in these simulations, learners can apply their theoretical knowledge to practical situations, enhancing their problem-solving skills and decision-making abilities. This immersive experience allows learners to understand the urgency and complexity of cybersecurity challenges, fostering a sense of preparedness and confidence in their abilities.

The VR app is available on the project website and it includes the following eight training modules: Malware, IoT attacks, Rootkit and Ransomware from the Beginners Level, SQL injections and Cross-site Scripting (XSS) from the Intermediate Level and Dos/DDos Attacks from the Advanced Level.

The integration of immersive technologies like VR and AR into the CybARverse learning modules offers VET trainers a dynamic way to enhance cybersecurity education. By providing learners with hands-on, interactive experiences that simulate real-world challenges, trainers can foster deeper understanding, critical thinking, and confidence in their cybersecurity skills. The resources available through the LMS make it easy for trainers to incorporate these technologies into their lessons, ensuring that learners are well-prepared to navigate the complexities of the cybersecurity landscape. More information is available in the next section.

VR/AR TECHNOLOGY SETUP & IMPLEMENTATION

4.1 Supported Headsets

Meta Quest 2 and Meta Quest 3 are supported VR headsets.

4.2 Creating a Meta Account

To use a Meta Quest headset, you need a Meta (formerly Facebook) account. Depending on your needs, you can create either a personal Facebook account or a generic account (for business/organisation purposes).

4.3 Steps to Create a Personal Facebook Account

- Visit Facebook: Go to the Facebook website or download the Facebook app.
- Sign Up: Click on "Create New Account."
- Enter Personal Details: Provide your name, mobile number or email, password, date of birth, and gender.
- Verification: Facebook will send a verification code to your email or phone. Enter the code to confirm.
- Set Up Profile: Add a profile picture and cover photo and complete your profile with additional information.
- Start Connecting: Add friends, join groups, and follow pages.

4.4 Setting Up the Meta Quest App on Your Phone

The Meta Quest app is essential for managing your VR experience. Here's how to set it up:

- Download and open the Meta Quest app on your phone.
- Log in with your Meta account (personal or business).
- Pair your Meta Quest headset by following the on-screen prompts.
- Use the app to configure settings, download content, and manage your device.

4.5 Requirements

- Mobile Device: Ensure you have a smartphone ready for the Meta Quest app and setup process.
- PC: A computer that can be used to interact with the headset and upload the APK.
- Oculus Quest Headset: The Oculus device you want to install the app on.
- USB Data Cable (USB-A to USB-C): This will connect the Oculus headset to your PC for transferring the APK.

4.5.1 Software

- Meta Quest App: You need to install the Meta Quest app on your mobile device to manage the Oculus headset. This app will assist with the initial setup and managing developer permissions.
- Meta Quest App Download and Setup: https://www.meta.com/quest/setup/
- SideQuest: Download and install SideQuest on your PC. SideQuest allows you to sideload APKs (Android apps) onto your Oculus Quest device.
- SideQuest Setup Guide: https://sidequestvr.com/setup-howto
- APK File: Ensure the APK file of the app you want to upload is downloaded and unzipped on your PC.

4.5.2 Permissions

- **Meta Developer Organization:** You need to create a Meta developer organization by signing up at Meta's Developer Dashboard to enable developer mode on your headset. Make sure your organization is confirmed.
- **Meta Developer Dashboard:**
- **Oculus Headset Admin Rights:** You must be the admin of the Oculus headset to manage its permissions. Learn more about this in Meta's Developer Mode guide.
- **Meta Quest Developer Mode Setup:**
- **Admin Member of Developer Organization:** The admin of the Oculus headset must be a member of the Meta developer organization created earlier. Ensure you add the admin as a member in the Developer Dashboard using the link provided above.
- **Oculus Headset PIN Code:** Set up the PIN code for your Oculus headset by following instructions on Meta's support page.
- **Meta Oculus Headset PIN Setup:**
- **Mobile Device Access Code:** Ensure your mobile device has an active passcode or biometric setup.

4.6 Setting Up the Meta Quest Headset

To set up your Meta Quest headset:

- **Charge** the headset before first use.
- **Adjust** the head strap to fit comfortably.
- **Power on** the device with the power button.
- **Follow the Setup Instructions**: Wear the headset and follow the on-screen guide.
- **Connect to Wi-Fi**: Select your network and enter the password when prompted.
- **Set Up Guardian Boundary**: Define a safe play area to prevent accidents while using the headset.

4.7 Using Hand Tracking and Gestures in Meta Quest

Meta Quest supports hand tracking, allowing you to interact with the VR environment without controllers. To use this feature:

- **Enable Hand Tracking** in the headset's settings.
- **Learn and Practise Gestures**: Start with basic gestures like pinching, grabbing, and pointing to interact with VR applications.
- **Test in Apps**: Use apps designed for hand tracking to become comfortable with controller-free interaction.
- Hand Gestures guide

https://www.cybarverse.eu/

PILOT TESTING

The CybARverse course underwent pilot testing in four countries - Lithuania, Cyprus, Malta, and Romania- where IT and non-IT educators, including teachers, tutors, and lecturers, participated. These educators provided valuable feedback through an extensive evaluation process that assessed the course's effectiveness.

Three separate surveys were conducted: one for the course participants, another for experts reviewing individual lessons, and a third for experts evaluating various course elements such as navigation, clarity, design, engagement, and the use of immersive technology. Each survey included a comment and suggestion box to gather qualitative insights, further enriching the feedback.

A total of 70 participants contributed to the evaluation, offering diverse opinions on the course's strengths and areas for improvement. Experts provided detailed evaluations for each of the 17 cyber-attack scenario lessons, yielding 71 responses. This feedback is critical for refining the course to better meet the needs of future learners.

In addition, 14 experts from the participating countries offered their perspectives through another survey that focused on various course aspects. Their detailed feedback, including qualitative insights from the comment sections, will guide the ongoing development of the CybARverse course, ensuring it becomes more effective and responsive to the needs of future participants.

PILOT TESTING

5.1 Findings from initial pilot testing

1. Course Structure and Understandability
The structure of the online cybersecurity course received overwhelmingly positive feedback, with 79% of experts rating its understandability as excellent. This indicates that the course content is presented in a clear and accessible manner, effectively simplifying complex cybersecurity concepts for learners. The high rating reflects the strength of the instructional design, which ensures that explanations are concise and supported by high-quality materials, contributing to a strong overall learning experience.

2. Grammar and Syntax
The course's grammar and syntax were highly praised, with 80% of participants rating it as excellent. This positive feedback underscores the importance of clear and professional language in maintaining the integrity and effectiveness of educational content. Proper grammar and syntax not only prevent distractions but also enhance the learners' focus on the material, thus supporting better comprehension.

3. Content Relevance
The relevance of the course content to current cybersecurity challenges was another strong point, with 70% of respondents rating it as excellent and an additional 27% rating it as very good. This indicates that the course material is well-aligned with the real-world demands of the cybersecurity field, providing learners with pertinent and applicable knowledge.

4. Adaptability to Learning Styles and Expertise Levels
Feedback on the adaptability of course elements to diverse learning styles and expertise levels was mixed. While a significant portion of experts appreciated the course's inclusive and versatile approach, some felt it did not adequately address their specific needs. This indicates a need for further refinement to better cater to the full spectrum of learners.

5. Effectiveness of Quizzes
The online quizzes received mixed feedback, with most experts recognizing their effectiveness but also highlighting areas for improvement. While the majority were satisfied with the time allocation for quizzes, some felt the time allotment was too long and the quiz content could be more comprehensive and varied to better assess the diverse expertise levels of participants.

6. Overall Challenge Level

The overall challenge level of the course was rated as excellent by 9% of experts, suggesting that while the course was well-suited to some, it may not have been challenging enough for others. This mixed perception indicates a need to balance the difficulty level more effectively.

7. Enhancing the VR/AR Experience

Feedback highlighted the need for more interaction and engagement within the VR/AR elements of the course. Participants also pointed out the challenges faced during the installation of the app on Oculus devices, emphasising the importance of clear, step-by-step instructions.

The pilot testing results highlight the strengths of the course, particularly in its structure, content relevance, and clarity. However, addressing the feedback related to adaptability, quiz effectiveness, and VR/AR interactions will be crucial in further refining the course. By implementing these best practices, the course will be better positioned to meet the diverse needs of learners, enhancing their educational experience and success in the field of cybersecurity.

5.2 Improvements/enhancements implemented after Pilot Testing

5.2.1 Learning Management System (LMS) Enhancements

To optimise user experience and course delivery, several key improvements were made to the LMS:

- **Content accessible and user-friendly:** The website's course content is now highly accessible and user-friendly, featuring comprehensive accessibility tools like dyslexia support, text magnification, dark contrast, readable fonts, highlighted titles and links, and more, allowing users to personalise the interface to their needs. Additionally, an AI-based application continuously optimises accessibility, adjusting the site's HTML for screen readers and keyboard functions to support users with visual and motor impairments.
- **Better Mobile Menu Display**: The mobile menu was re-designed to ensure seamless navigation across devices, enhancing accessibility for users who prefer learning on mobile platforms.
- **Case Studies Linked to PDFs**: To ensure reliable access to resources, case studies are now linked to downloadable PDFs rather than external websites, providing a more consistent learning environment and reducing the risk of broken links.

- **Registration Verification**: Enhanced verification processes have been implemented to streamline user registration and ensure that only authorised participants gain access to the course.
- **Tailored Level Descriptions**: Each course level now features distinct descriptions, providing learners with a clearer understanding of the content and objectives at each stage of their journey.
- **User Profile Adjustments**: User profiles have been refined by removing unnecessary features, such as wish lists and orders, to simplify the interface and focus on essential course-related information.

5.2.2 Quizzes and Content Optimization

To better assess learner understanding and engagement, several adjustments were made to the quizzes/assessment:

- **Time Allocation Adjustment**: The time limit for quizzes was standardised at 20 minutes, providing sufficient time for learners to thoughtfully engage with the questions while maintaining a sense of urgency.
- **Varied Question Types**: Quiz questions were diversified to include a range of formats, such as multiple-choice and true/false to more accurately gauge different aspects of learner knowledge and understanding.
- **Passing Score Maintained at 60%**: The passing threshold for quizzes was kept at 60%, balancing the need for rigour with the goal of ensuring learner success and confidence.

5.2.3 VR/AR App Enhancements

To create a more immersive and interactive learning environment, several updates were made to the VR/AR application:

- **Enhanced Interactive Lady Figure**: Additional animations were integrated into the interactive lady figure, making the learning experience more dynamic and engaging.
- **Voiceover Text Added**: Voiceover narration was introduced to complement the visual elements, catering to auditory learners and enhancing overall comprehension.
- **Module Completion Indicators**: Visual indicators were added to track module completion, providing learners with a clear sense of progress and achievement.
- **Scenario Background Updates**: Backgrounds in selected scenarios were updated to provide a more immersive and contextually accurate environment for learners.

- **Music Customization**: A variety of background music options were added, along with muting capabilities, allowing learners to personalise their learning environment.
- **Introductory Video**: A tutorial was added on the VR app to guide users through the app's features and set the stage for their learning experience.
- **Logos and Disclaimers**: Logos and disclaimers were added to the "About Us" section, enhancing transparency and providing essential information about the course and its creators.
- **App Controls Reviewed and Amended**: User controls were thoroughly reviewed and adjusted to ensure intuitive interaction with the VR/AR environment, improving overall usability.
- **WebVR Scenarios**: Web-based VR scenarios were Zero-day exploits, Man-in-the-Middle attacks, and Cryptojacking, making the immersive experience accessible across multiple platforms.

These enhancements were strategically implemented to ensure that the cybersecurity online course is not only engaging and interactive but also effective in equipping learners with the practical skills needed to excel in the field. By leveraging immersive technologies and refining both the LMS and content delivery, the course aims to provide a comprehensive and impactful learning experience. Furthermore, these adjustments will not only improve user satisfaction but also ensure the course effectively meets the educational needs of all participants.

5.3 Insights gained

After conducting a pilot training of a cybersecurity course using immersive technology, several key insights were gained that highlight the effectiveness and participant engagement with this innovative approach. Here are the primary insights:

1. Enhanced Engagement and Retention

- **High Levels of Engagement:** Participants were significantly more engaged compared to traditional training methods. The immersive technology, such as virtual reality (VR) or augmented reality (AR) together with the videos provided a hands-on experience that made complex cybersecurity concepts more accessible and relatable.
- **Improved Retention:** The interactive nature of the course led to better retention of information. Participants were able to actively apply what they learned in real-time simulations, which reinforced their understanding and memory of key cybersecurity principles.

2. Positive Feedback on Interactivity

- **Interactivity Praised:** The interactive elements of the course were particularly well-received. Participants appreciated the ability to interact with virtual environments that closely mimicked real-world scenarios. This interactivity not only made the course more engaging but also allowed for practical, experiential learning, which participants found invaluable.
- **Real-world Applications:** Participants reported that the videos and case studies helped bridge the gap between theoretical knowledge and practical application. They felt more prepared to manage real cybersecurity threats after engaging with the interactive simulations.

3. Increased Confidence in Skills

- **Confidence Boost:** Immersive technology helped participants build confidence in their cybersecurity skills. The opportunity to practise in a controlled, risk-free environment allowed them to make mistakes, learn from them, and improve their skills without fear of real-world consequences.

4. User Experience and Accessibility

- **Ease of Use:** While most participants found the immersive technology intuitive and easy to use, there were some initial learning curves for those less familiar with VR or AR. However, after a brief acclimatisation period, most participants reported a smooth and enjoyable experience.
- **Access and Equipment:** Some participants noted that access to the necessary equipment (e.g., VR headsets) was a potential barrier. However, when provided, the equipment significantly enhanced the learning experience.
- **Accessibility features:** accessibility barrier was removed with enhanced features that support dark contrast, reading guide, readable fonts and line spacing, and highlighted titles and links, ensuring an inclusive experience for all users including persons with dyslexia.

5. Areas for Improvement

- **Technical Issues:** A few participants experienced minor technical issues, such as glitches or difficulty navigating the virtual environment. These issues, though not widespread, highlight the need for robust technical support and thorough testing before broader deployment.
- **Varied Learning Curves:** While most participants adapted well to the immersive technology, some required additional support. Tailoring the training to accommodate various levels of technological proficiency could enhance the overall effectiveness.

6. Overall Satisfaction

- **High Satisfaction Levels:** Overall, participants were highly satisfied with the immersive cybersecurity training as well as with the videos. They appreciated the innovative approach and the engaging, interactive environment.
- **Recommendation for Wider Use:** Many participants expressed a desire to see more training programs adopt immersive technology, citing the enhanced learning experience and the potential for such methods to revolutionise training in cybersecurity and beyond.

https://www.cybarverse.eu/

CONLUSION

6.1 Summary of Best Practices for Cybersecurity Course Delivery

The effective delivery of the cybersecurity course within the CybARverse platform, which leverages immersive technology, hinges on several key best practices:

1. Interactive Learning Environments: Utilise immersive VR/AR simulations to create realistic, hands-on scenarios where learners can practise cybersecurity skills in a controlled, engaging environment.
2. Adaptive Content Delivery: Tailor the course content to accommodate varying levels of learner expertise. Provide foundational materials for beginners, intermediate and advanced challenges for experienced participants, ensuring that all users benefit from the training.
3. Assessment: Assessments/quizzes at the end of each level embedded within the course track progress and reinforce learning outcomes.
4. Accessible Technology: Ensure that the necessary immersive technology is easily accessible and user-friendly. At the beginning of the course, offer support for learners who may be less familiar with VR/AR tools to minimise barriers to participation.
5. Security and Privacy Considerations: Ensure that the immersive technology platform adheres to the highest security standards to protect user data and maintain the integrity of the training environment.

CONLUSION

6.2 The Purpose and Impact of the Guide

The purpose of this guide is to provide educators, trainers, and instructional designers with a comprehensive framework for delivering effective and engaging cybersecurity courses using the CybARverse platform. By adhering to the best practices outlined in this guide, instructors can create immersive learning experiences that not only enhance the understanding of complex cybersecurity concepts but also significantly improve learners' practical skills.

The impact of this guide extends beyond individual training sessions. By adopting these practices, organisations can ensure that their cybersecurity teams are better prepared to tackle real-world threats, leading to a more secure digital environment. Additionally, the guide helps standardise the delivery of immersive technology-based training, fostering consistency and quality across different learning environments.

6.3 Final Thoughts and Next Steps for Continuous Improvement

As we continue to evolve in a rapidly changing technological landscape, it is essential to view this guide as a living document. The field of cybersecurity is dynamic, with new threats and technologies emerging regularly. Therefore, continuous improvement and adaptation are key.

Next Steps:

1. Regular Updates: Periodically review and update the guide to reflect the latest developments in cybersecurity and immersive learning technologies. Incorporate feedback from instructors and learners to refine best practices.
2. Community Collaboration: Encourage collaboration among educators, cybersecurity professionals, and technologists to share insights, experiences, and innovations. Building a community around immersive cybersecurity training can lead to the development of new methods and tools.
3. Scalability and Customization: Explore ways to scale the immersive training approach across different organisations and customise it to specific industry needs. This will help make the CybARverse platform more versatile and widely applicable.

In conclusion, by embracing these best practices and committing to continuous improvement, we can ensure that cybersecurity training within the CybARverse not only remains effective but also leads the way in innovative, immersive learning experiences. This approach will empower cybersecurity professionals with the knowledge and skills they need to protect our digital world in an increasingly complex threat landscape.

ABOUT THE PROJECT

CybARverse is an Erasmus+ co-funded project which supports IT as well as non-IT teachers and trainers' digital skills development, through the use of immersive technologies. The focus of this project is to train the target group on how to recognise and react correctly to cyberattacks. It promotes cyber security awareness, the implementation of the Digital Education Action Plan (Actions 5 and 7) as well as national agendas, and contributes to a more digital, greener and more inclusive teaching and learning.

Project no: 2022-1-LT01-KA220-VET-000089116
Project duration: November 2022 – October 2024

Objectives:

- To promote professional, personal, and digital skills among VET teachers and trainers in the field of cybersecurity.
- To incorporate modern and immersive technologies into VET cybersecurity training.
- Structured qualification of teachers and trainers to become cybersecurity aware and literate.
- To ensure the sustainability of the project results.

Project Consortium

LANGAS | ATEITI
https://www.langasiateiti.lt

Tech.mt
MALTA - LEADING THROUGH INNOVATION
https://tech.mt/

SCP School of Certified Professionals
https://scp.ac.cy/

CYPRUS COMPUTER SOCIETY
https://ccs.org.cy

eos FUNDAȚIA EOS ROMÂNIA
http://www.eos.ro/

CONTACT US

academy@cybarverse.eu

https://www.cybarverse.eu/

YouTube: @CybARverseproject