IO6: Game testing, evaluation and feedback analysis.

Co-funded by the Erasmus+ Programme of the European Union

Table of content

List of Figures

Co-funded by the Erasmus+ Programme of the European Union

1 Executive summary

This report focuses on the testing of an online cyber security game in schools. The game was designed to educate students on safe internet practices and increase their awareness of potential cyber threats. The study aimed to evaluate the effectiveness of the game and gather feedback from students on its usability, relevance, and educational value.

To achieve these goals, the study utilized the eye-tracking methodology. Eye-tracking technology has been widely used in research to measure visual attention, gaze patterns, and other aspects of human behaviour. In this study, the eye-tracking technology was used to track the students' eye movements and interactions with the cyber security game. By analysing the data collected from the eye-tracking software, the researchers could gain insights into how students interacted with the game, what parts of the game attracted their attention, and how effective the game was in communicating key cyber security concepts.

In addition to the eye-tracking methodology, an online survey was conducted to collect feedback from students in Poland and Estonia on the game's usability, relevance, and educational value. The survey included questions about the students' experience playing the game, their perceived level of learning, and their attitudes towards cyber security. The survey data was analysed using statistical software, which allowed the researchers to identify patterns in the students' responses and gain a deeper understanding of their attitudes and perceptions towards the game.

Furthermore, the study also included IT testing, which was carried out in Germany, to ensure that the game met technical standards and requirements. This involved testing the game's performance on various devices and platforms, as well as assessing its compliance with relevant laws and regulations.

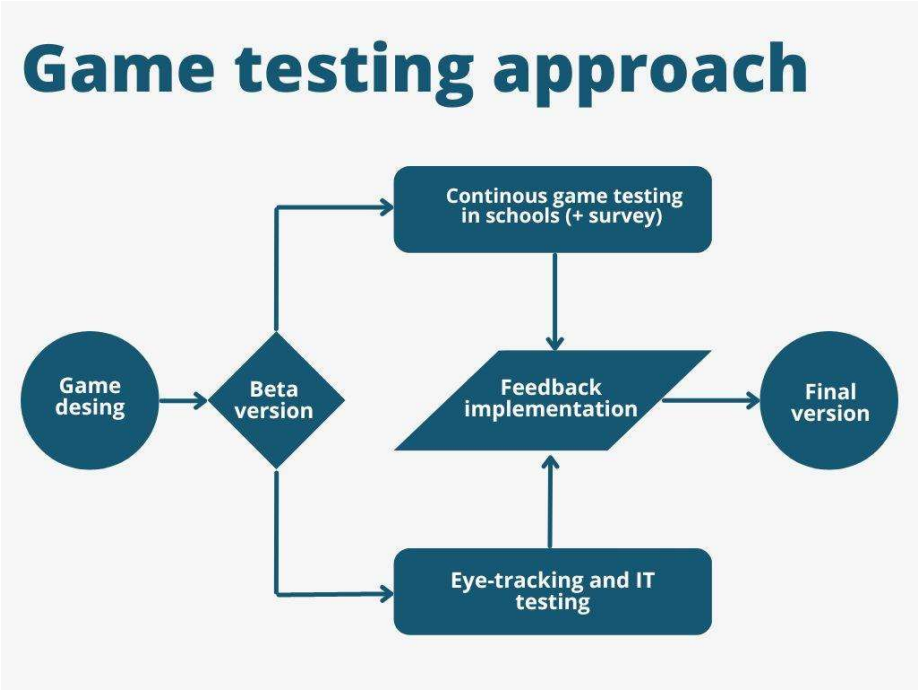
Overall, this report aims to provide a comprehensive overview of the testing process, the results of the study, and the implications for the use of online games as an educational tool for cyber security in schools.

Co-funded by the Erasmus+ Programme of the European Union

2 Methodology behind the testing

Testing an online game can be a complex and multifaceted process that requires a thorough methodology. In this case, the approach involves live testing during lessons in schools in Poland and Germany, using an eye-tracking system to validate UX/UI, testing the game in a software environment, and gathering feedback from students via a CAWI online survey (see Figure 1). This methodology is designed to provide developers with valuable information about the game's playability, quality, and the effectiveness of in-game scenarios related to cybersecurity.

Figure 1 - Cyber 4 Schools game testing approach



The first part of the methodology involves live testing of the game during lessons in schools in Poland and Germany. This involves observing students as they play the game in a real-world setting and noting any issues they encounter, such as difficulty understanding game mechanics or frustration with the game's interface. By testing the game in a classroom environment, developers can gather feedback from a diverse group of players with varying levels of experience and technical proficiency. This allows them to identify and address any issues that may affect the game's overall playability.

The second part of the methodology involves using an eye-tracking system to validate the game's UX/UI. This involves tracking players' eye movements as they play the game and analysing the data to determine which areas of the game are most engaging or problematic.

Co-funded by the Erasmus+ Programme of the European Union

This data can help developers identify which areas of the game need improvement and which elements are working well.

The third part of the methodology involves testing the game in a software environment. This involves running the game on different operating systems, hardware configurations, and software configurations to ensure that it performs consistently and reliably across a range of environments. By testing the game in this way, developers can identify and fix any bugs or compatibility issues that may arise.

The final part of the methodology involves using a CAWI online survey to gather feedback from students regarding the game's playability, quality, and the effectiveness of in-game scenarios related to cybersecurity. This survey can be distributed to a large number of students in a short amount of time, providing developers with a wealth of data about how the game is perceived by its target audience. The survey can also include open-ended questions that allow students to provide detailed feedback about their experiences with the game, providing developers with valuable insights into what is working well and what needs improvement.

Taken together, these testing techniques provide a comprehensive and rigorous methodology for evaluating the game's performance and identifying areas for improvement. By using a range of testing techniques that involve real-world players, software environments, and online surveys, developers can gain a thorough understanding of the game's strengths and weaknesses and make informed decisions about how to improve it. The results of this testing can be used to refine the game's mechanics, improve its user interface, and create more effective in-game scenarios related to cybersecurity, resulting in a better overall gaming experience for players.

3 Game Testing Results – Testing at schools

The most important part of the testing phase was the school testing. Testing of educational online games in a school environment with kids is crucial in ensuring that these games are effective tools for learning. By testing the games with real students, educators and game developers can assess the game's usability, effectiveness, and engagement level. The testing phase also allows for the identification of any potential technical issues and provides feedback on how the game can be improved to better suit the needs of both students and educators. The testing phase carried out in two schools in Estonia and Poland provides valuable insights into how well the games work in different cultural and linguistic contexts, and whether they are suitable for a range of age groups. This information is essential for ensuring that educational online games are effective, engaging, and accessible to all students, regardless of their background or educational needs. In Cyber4Schools testing was done in two schools:

1. Poland – Zespół Szkół nr 2 im. Przyjaźni Polsko – Norweskiej w Ostrzeszowie and Zespół Szkół nr 1 im. Powstańców Wielkopolskich w Ostrzeszowie.

In Poland, two schools took part in the tests School Complex No. 1 and School Complex No. 2. These were students from both the technical and high schools of these schools. Due to hardware limitations during the tests, students were divided into groups in which they solved a given scenario. At the beginning of the scenario, they were given an outline of the game and the idea of the whole project. They were informed what they had to do, where to look for

the answers after which they proceeded to solve the tasks. The students received the created game very positively. They were very involved in testing the scenarios. They had never had the opportunity to take part in such testing before, so they were eager to share their observations. They tried to find as many mistakes as possible, a kind of rivalry arose between the groups as to who would find more of them. Currently, the students are testing the next scenarios made available. As they themselves say, earlier they could only listen in lessons about cyber security, and now they themselves can take an active part in it, both on the side of attackers and defenders. A total of 15 classes and more than 300 people from both schools have taken part in the tests so far.

Figure 2 - Pictures from game testing in Poland

2. Estonia - Pelgulinna Gümnaasiumi

In Estonia, the possibility to test the game Cyber4School has been shared via several newsletters and national dissemination events. The game accounts have been shared with over 20 teachers from 7-12th grade, students' free time centres, and vocational schools, who have played the game with ~300 students. Around 160 of them also provided feedback and contributed to the development of the game directly. From the student's perspective - the overall experience has been that the game is interesting to the beginner, even if the cybersecurity topic itself can be daunting. The game environment is built up nicely to introduce both Linux and Windows. Students from Pelgulinna Gymnasium, which has been part of the game development since the storyline began were amazed that their ideas of STEAM events on the school premises and hackers versus crackers are life-like. Some clever students also found a way to swich the game base environment into their national language using browser translation tools, ad it was not bad at all! Teachers that have logged

Co-funded by the Erasmus+ Programme of the European Union

in and tested the game state it was easy and intuitive, and the technical issues that were part of the piloting (fewer numbers of players available, virtual machines staying problems) did not scare them away. Now the fans of the game look for more possible ways to implement the game into the informatics lessons and extracurricular activities. Schools are also using the lessons plans and possibility to give out diplomas for students that have participated the whole game.

Figure 3 - Pictures form game testing in Estonia

At the stage of finishing this report, in the system were registered 17 users (test users, teachers). There were 175 game sessions run involving 447 teams overall (see annex 1).

4 Game Testing Results – Eye-Tracking

One of the research techniques used in the testing phase of the game was Eye-tracking. Eye-tracking research is a powerful tool that can be used to understand how users interact with web-based games. By measuring where users look on the screen, researchers can gain insights into how players process information, make decisions, and engage with game mechanics. Eye-tracking tests were performed in the ASM Neurolab with the use of Tobii Pro Glasses 2. In the test 4 student took part. The idea behind the Eye-tracking was to check the game/platform interface weather the design of is aligned with the user requirements. The study confirmed that the placement of the icons and the interface was designed correctly.

Figure 4 - Eye-tracking session picture 1

Co-funded by the Erasmus+ Programme of the European Union

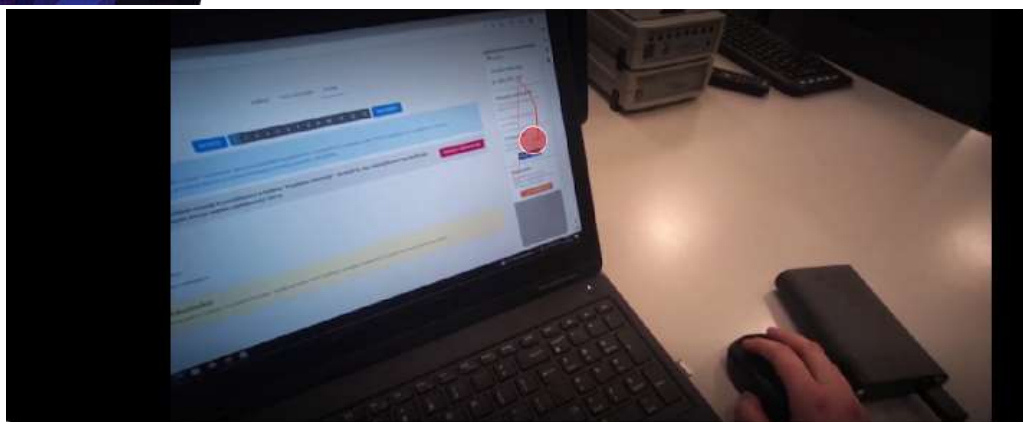


Figure 5 - Eye-tracking session picture 2

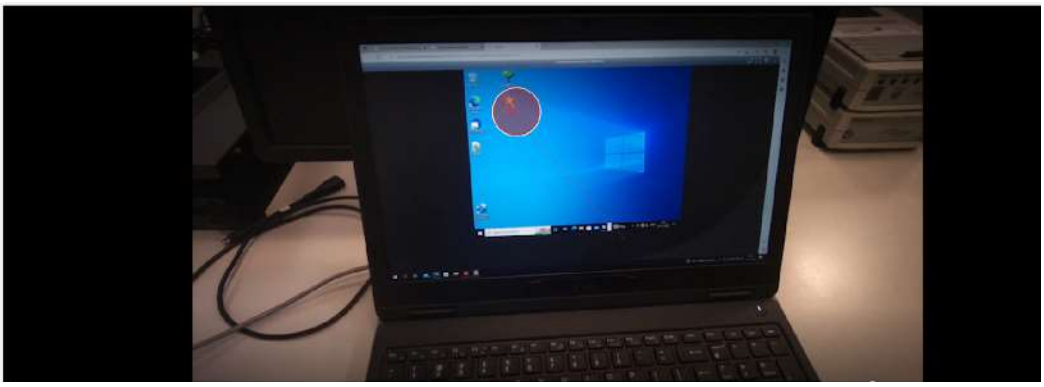
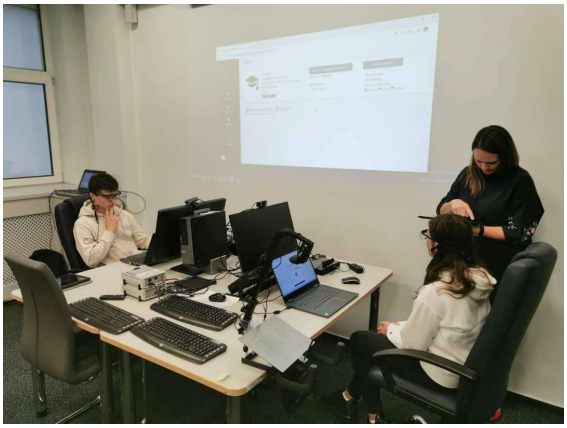


Figure 6 - Eye-tracking session picture 3



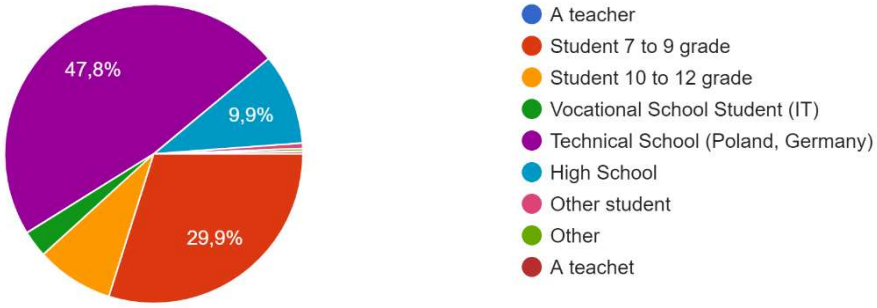
5 Game Testing Results – On-line survey (CAWI)

Co-funded by the Erasmus+ Programme of the European Union

Another part of the testing methodology was the on-line survey (CAWI – Computer Assisted Web Interview) with the students that have played the Cyber 4 School on-line game. As mentioned previously the aim of the survey was to gather feedback from students regarding the game's playability, quality, and the effectiveness of in-game scenarios related to cybersecurity.

135 students from Estonia and **203** students from Poland participated in the survey. Almost 70% of the students that participated in the survey are in age between 14 – 18, remaining 30% students (students 7 to 9 grade) are in age between 11 – 14.

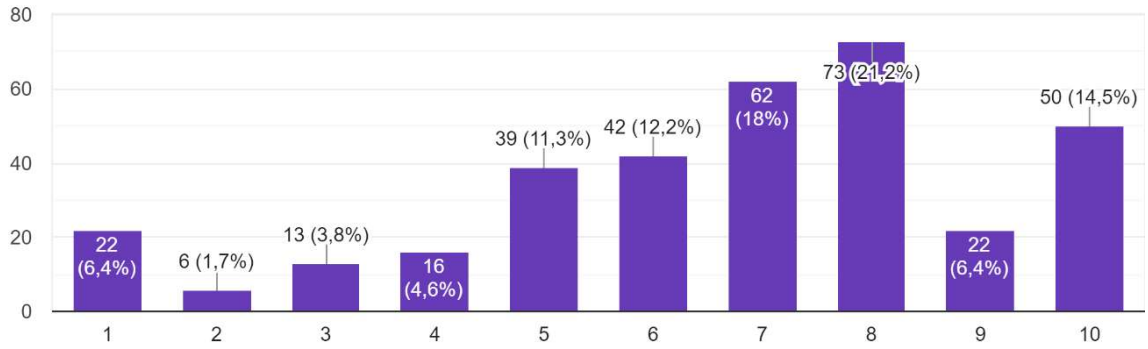
Figure 7 - Type of school



At the beginning of the survey we have asked “Would you recommend the game for others?” (where 1 means not recommend at all, and 10 means highly recommended). The answers to that question are very promising, as **83,6%** of respondents chose between **5** and **10** which means that on average the game would be recommended to others to be played.

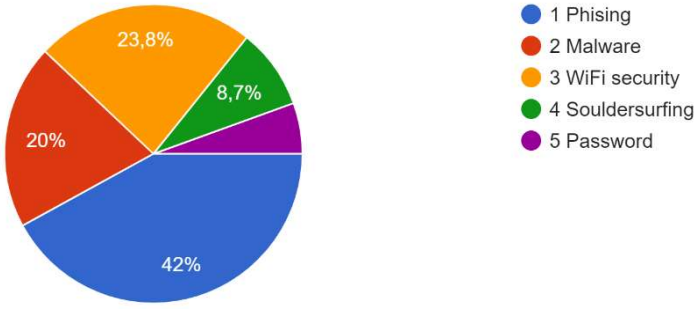
Figure 8 - Willingness to recommend the game to others

Co-funded by the Erasmus+ Programme of the European Union



Another two questions reflects on which scenario was played and in which team. As the testing phase has started before the launch of all 5 scenarios, most of the students played the first scenario (42%), second scenario (20%) and third scenario (23,8%). In terms of the chosen team we have equal division, 50% for blue team and 50% for red team.

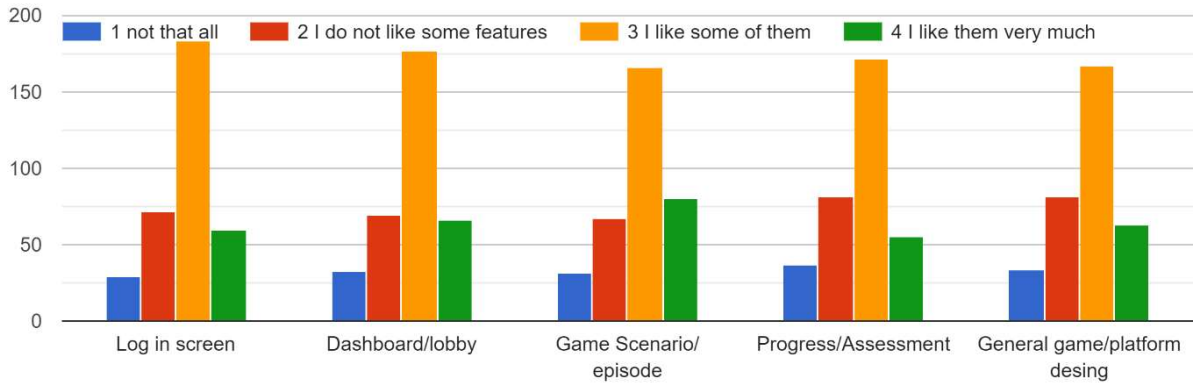
Figure 9 - Division of scenarios played by students



Following three questions were related with the in-game features and functionalities. The aim of the first question “How do you like the graphic design of the game” was to gather feedback aobut the graphic desing of the “log in screen”, “dashboard/lobby”, “game scenario/episode”, “progress/assesment”, “overall game and platform desing”. **50%** of the respondens said that they **like some** of the grpahics and **20%** said that they like them (graphics) **very much.** It gives us **70%** of the positive answers, while only **10%** respondent did not like them at all. That results shows that the majority of the graphic design of the game was done in a proper way.

Co-funded by the Erasmus+ Programme of the European Union

Figure 10 - Opinion on the graphic design

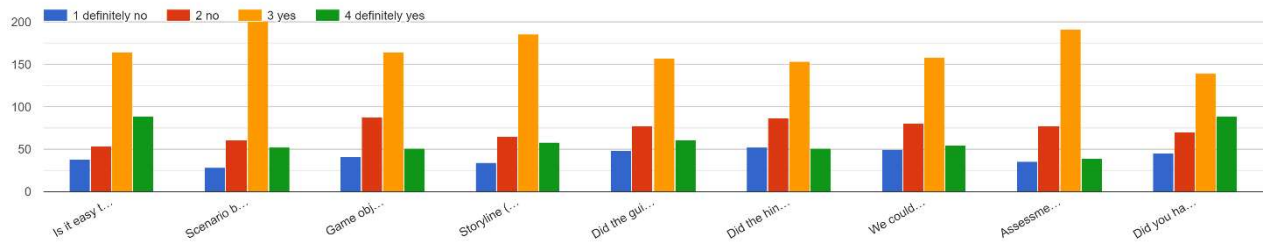


Second question was reffering to funcionality of the interface and the content on the platform, if it is clear or not at this stage:

1. Is it easy to use: log in page/start page
2. Scenario background was clear
3. Game objectives (episode) were understandable
4. Storyline (only for students) was easy to follow
5. Did the guidebook help you to find technical solutions
6. Did the hint system help you to find the right solution
7. We could play and navigate game without to much instructions (guidebook, hints)
8. Assessment/progress (was questions unerstandable)
9. Did you have enough time to finish the episode

Similar to previus questions, majority of the anwers (70%) were **yes or definitely yes.** Olny **30%** siad that it is **not clear** or **definitley not clear.**

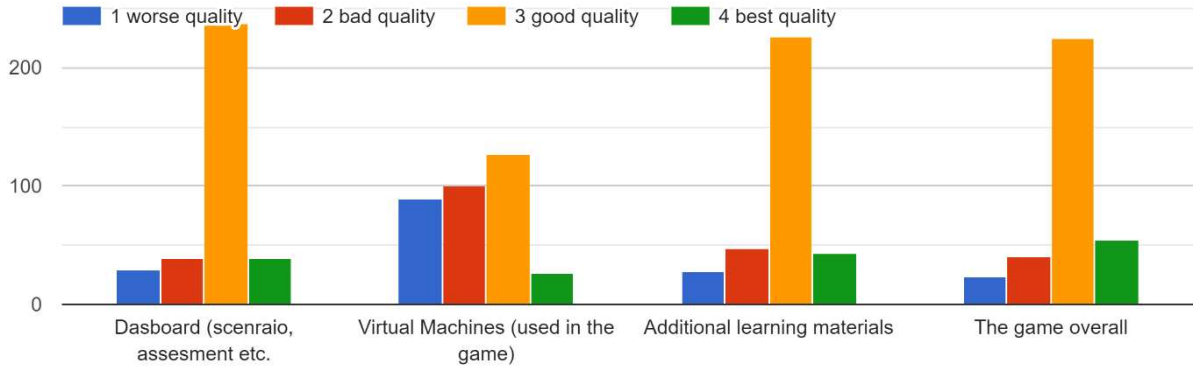
Figure 11 - Opinion on the game interface and content



Co-funded by the Erasmus+ Programme of the European Union

Last qestion in that section was reffering to the quality of the main game components: “dasboard (scenartios, assesment etc.)”, “virtual machines”, “additional learing materials” and “game overall”. In terms of the dashboard, learnig materials and game overall **67%** of respondents said that they are **good quality.** Only the virtual machines were rated worse. **50%** of the respondents said that the quality of virtual machines was bad or worse quality. It is important to mention, that during the testing face the virtual machines were in beta version and according to the feedback from the respondents they were replaced with the better one.

Figure 12 - General quality of the game and main components



The questionnaire also consisted of three open-ended questions, in order to gather more direct feedback from the students. In the fisrt question we have asked about any issues encountered during the assemsent phase. The purpose of that question was to check if there are any problems with the questions at the end of each scenario. According to the feedback few questions were not understandable in 100%. Analysis of the answers gave the opportunity to upgrade the assesment and to rewrite some questions to make them more understandable. Another to questions were related with the difficulty level of the game. We have asked what was difficult and how to make it easier, and on the other hand we asked what was the easy part that needs to be made more difficult. In general students said that the level of the game is accurate, and apart from slow virtual machinge the game was rated very good.

To summarise the results of the survey, the analysis shows that the game developed during the Cyber 4 Schools project meets the expectations of majority of students. Some technical problems were reported and were transferred to the technical partner to solve them.

6 Game Testing – Technical Test Environments

PHASE 1 – Start of Project: Pre-Testing

System: AWS (Amazon Web Services)
Specs: Dynamic Configuration

Test Description:
Testing setups on external hosting environments with Amazon Web Services (AWS). Tested multiple Endpoints with Unity Engine based content for performance and concurrent connections + stress testing.

PHASE 2 – Mid Project: Internal Test Server

System: Windows Desktop PC Optiplex
Specs: Windows 10 - 16 GB RAM, 1 TB HDD, CPU 8 Core (16 Threads) , VM-Ware Workstation 16, Debian 10 - MiniMega,

Test Description:
Running different configurations of virtual machines on a Windows 10 Test-Server running VM-Ware Workstation 16 hosting the game environment as a Debian 10 MiniMega instance. Test of performance, life sessions and bandwidth consumption for concurrent user access. Monitoring resource consumption using NoVNC remote access to Windows 10 and Kali Linux Clients.

PHASE 3 – End Project: Production Server

System: DELL Server PowerEdge R650xs
Specs: Windows Server 2019 - 64 GB RAM, 512 TB SSD, CPU 12 Core (24 Threads), VM-Ware Workstation 17, Debian 11 - MiniMega,

Test Description:
Running different configurations of virtual machines on a Windows 2019 Production Server with VM-Ware Workstation 17 hosting the game environment as a Debian 11 MiniMega instance.
Testing different CPU setups for VMs (2 CPUs, 3 CPUs, 4 CPUs), testing and monitoring bandwidth ,CPU consumption, SSD throughput for different setups using NoVNC remote access to different virtual machines hosting Windows 10 and Kali-Linux Clients.

7 Conclusions

The testing phase of the Cyber4Schools online educational game about cybersecurity was a rigorous and multi-faceted process. The testing phase consisted of four main testing methods: testing at school, eye-tracking testing UX/UI, CAWI survey, and technical environment testing including pre-testing, internal test server, and production server. Each method was carefully designed to ensure that the game was engaging, informative, and effective in conveying important concepts related to cybersecurity to students.

The testing at school involved the game being tested by students in real-world settings. This method was valuable in determining how the game performed in a classroom environment and how students interacted with it. The eye-tracking testing UX/UI was used to monitor how students were engaging with the game and to identify areas where improvements could be made to the user interface or user experience. The CAWI survey provided valuable feedback

Co-funded by the Erasmus+ Programme of the European Union

from students on how they felt about the game, its effectiveness, and its educational value. Finally, the technical environment testing was used to ensure that the game functioned properly in different technical environments.

The feedback from students during the testing phase was overwhelmingly positive. Over 70% of students positively ranked the Cyber4Schools game, indicating that it was engaging and effective in teaching them about cybersecurity. The feedback from the testing phase highlights the potential impact of the game in educating students about cybersecurity and the importance of safe online practices.

In conclusion, the testing phase was a crucial step in ensuring the effectiveness and usability of the Cyber4Schools game. The multi-faceted approach to testing ensured that the game was thoroughly evaluated from different angles. The overwhelmingly positive feedback from students suggests that the game is a valuable educational resource for teaching students about cybersecurity. The testing phase provides a solid foundation for the continued development and implementation of the game in schools.

8 Annex 1

Co-funded by the Erasmus+ Programme of the European Union

C4S Portal Statistics

Portal Users	Game Sessions Run	Total Teams Involved
Test-NL	87	155
Test-RO	22	97
TR-Litsitomy	16	62
TR-TMaulmans	12	32
CB	13	33
Test-CW	5	12
RK_upi	4	15
Hmay	3	7
TR-Bloment	3	9
TR-Kbamsndc	2	0
Test-3Biofork	2	7
Test-D	2	2
Acoodt Mkgi	1	4
Ioanija meier	1	2
Test-BL	1	4
TR-HBFIEVIEN	1	4
TR Logmann	1	2
TOTAL	176	447