CyberAgent

Co-funded by the European Union

CYBERAGENT COLLABORATION PLATFORM REQUIREMENTS REPORT

CYBER AGENT 06.2024

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

www.cyberagents.eu

Work Package 2: CyberAgent approach and structure design

Deliverable 2.5: CyberAgent collaboration platform requirements report

Leader of deliverable 2.5 – Prios

CONTENT

ABBREVIATIONS

EC – European Commission

EDEH – European Digital Education Hub

EDIH – European Digital Innovation Hub

KC– Knowledge Committees

WP – Work Package of the project

LIST OF FIGURES

INTRODUCTION

Information technology as one of the advanced tools of today's society has transformed the way professional development and learning occurs, especially in interceding cyber security. SMEs are now integrating sophisticated cyber protections into their business strategies and that asserts that cyber education and training is not an event that can be repeated once. To address this need, our project will seek to design a modern digital collaboration solution that addresses the need to enhance cybersecurity know-how of local and regional networks. That is why this initiative is not so much about improving SMEs' readiness to resist new forms of cyber threats but about building a professional community that would be constantly evolving.

The subject matter of this report revolves on the Prios need assessment done in a bid to create the CyberAgent collaborative digital platform in WP4. It is important to note that the analysis was intentionally designed to reveal certain objectives, characteristics, and the environment that would best support the proposed digital tool. This effort is important to position the platform to meet the current and future requirements of SMEs in cybersecurity.

Furthermore, it is believed that it will be possible to enhance other current and future European and national projects concerning digital learning and professional development. Another important component of the assessment was the exploration of partnership opportunities with the EDIH and the EDEH. By doing this, the CyberAgent platform is supposed to enhance the efficiency and volume of the project.

The information collected by the surveys of Prios is valuable when establishing a new form of platform that is not only a unique solution, but also compatible with a large environment for SMEs in Europe. The findings of the needs assessment process as well as the plan for the subsequent phases of implementation of the CyberAgent tool are presented in this report.

We gained useful insights over the course of one month, gathering 12 relevant responses from the Knowledge Committees (KC) of all the partners. The responses were from training providers as well as VET students.

Based on the main aspects of the future platform, we divided the analysis of the survey into the following chapters: 1. General features of Collaboration Platform: 2. Integration of the European Digital Innovation Hub (EDIH) into the Platform, 3. Implementation of the EDEH, 4. User Interface, 5. Proposal on Data Security and Privacy in the CyberAgent Collaboration Platform 6. Investigation of user feedback and the evaluation of the CyberAgent Collaborative Platform, 7. Technical solutions for the CyberAgent Collaborative Platform, and 8. Conclusion.

In this report, the results of needs assessment are provided and the future steps toward the further evolution of CyberAgent collaborative online platform are described.

KEY PURPOSE OF THE PLATFORM

In the CyberAgent project, different entities are participating such as SMEs, educational institutions, cybersecurity experts, and many other participants from different European countries.

The primary purpose of the online platform described in the CyberAgent proposal, is to create comprehensive environment for empowering SME employees, particularly focusing on women in the IT sector, to become proficient in cybersecurity. The platform is intended to serve several functions as:

- Educational resource, by providing a space where SME employees can access training modules to upskill and reskill in cybersecurity, with the aim to prepare them as "Cyber Security Change Agents." This includes technical, analytical, risk management and organisational skills.
- The platform will facilitate collaborations between Higer Education Institutions (HEIs), Vocational Education and Training (VET) providers and SMEs. This is important for the project, which is designed to foster sharing of best practices and innovative solutions in cybersecurity.
- The platform also has a purpose to act as a repository for sharing and accessing information on best practices and the latest developments in cybersecurity, encouraging lifelong learning and interaction among involved partners.
- With the focus of including women and providing targeted training, the platform aims to address the gender gap in the cybersecurity field and enhance the employability and expertise of all SME employees. Collaborative feature of platform is especially aimed at supporting this and making it easier to find women peers.
- Platform is planned to be sustainable and accessible during and after the project life end, expanding its impact by reaching wider audience across Europe.

In addition, the platform will increase possibilities for participants to do networking amongst each other, ideas and experience, as well as the best approaches to cybersecurity. The implementation of the above ideas will further enhance the pillars of this project through collaboration.

Added Value Proposition

At its core, the platform will significantly improve the access to the training materials and other resources that would benefit SMEs and their employees when it comes to improving their knowledge of cybersecurity. This is especially beneficial for SMEs which may lack the internal capacity to develop materials in-house.

In addition, the platform also involves the adoption of industry benchmarks and standards for cybersecurity, which helps SMEs learn from the experiences of the rest of the network. This form of peer learning will go a long way in increasing the take-up rate of proper cybersecurity measures across many different SME sectors.

Finally, the platform is expected to create a credible environment for conducting cybersecurity training. Through the allocation of multiple funds and the creation of a vibrant community of practice, it aims at maintaining project activity and continuance beyond the end of the project. This way, it acts as a reference tool for career progression in the field of cybersecurity.
CyberAgent Collaborative Platform is the projects solution for transforming SME's cybersecurity upskilling through an innovative and digital collaborative collaboration tool that set themselves apart through its features, integrability and customer-orientation.

CyberAgent collaborative platform It is on this platform that the objectives of learning and collaboration are achieved seamlessly. This allows participants to have access to training information, professional tools and equipment, and peer information exchange within the same system. This category of e-learning modules, combined with the discussion forum and real-time messaging and file-sharing capability, improves communication and productivity because people no longer have to move from one application to another.

Unlike the numerous websites that offer cybersecurity learning and upskilling opportunities, the CyberAgent will be designed for SMEs wherein, we consider their problems and resources when it comes to cybersecurity upskilling. It offers affordable packages, specific training, and community support, which are valuable yet may be unavailable without additional costs for small organizations.

Moreover, CyberAgent platform will have reliable networking capabilities where SMEs can get connected with Higher Education Institutions (HEIs), Vocational Education and Training (VET) providers, cybersecurity professionals, mentors, and other professionals. Industry-focused, user-generated content pages, collaboration networks, and virtual communities will help users share experiences, obtain advice, and advance their careers, creating a positive atmosphere.

Collaboration with EU-based schemes such as the EDIH and EDEH will allow SME consumers to engage with other digital platforms. This integration opens a repository of digital learning materials, events, and cooperative learning activities, thereby, adding significant environmental value to the platform. This connection provides a strong base for the positive environment within the context of cybersecurity training where the users are aware of their belonging to a large whole.

Who benefits from collaboration?

The platform aims to be a useful tool and source of information for all target groups identified in the project.

SMEs can access a wider range of resources, expertise, and best practices that they might not have internally. This is especially important for smaller businesses that according to "D2.2 - The SME Cyber Security Change Agents Training needs mapping report" often not have the budget or ordering competence to hire full-time cybersecurity specialists.

SME employees, which is the core target group as Cybersecurity Change Agent, will gain access to training and networking opportunities that improves their skills, competence and opportunity to fulfil their role better.

Also, **Higher Education Institutions (HEIs) and Vocational Education and Training (VET)** providers is expected to benefit by staying more connected to industry needs than the case is today. This connection helps them tailor their curricula and training programs to be more relevant and effective for their students and busies customers.

Cybersecurity experts and trainers can expand their reach, business and impact by engaging with a larger, more diverse audience. By spreading their knowledge and possibly developing new educational content based on user needs and feedback, they can make a greater difference in the field.

Trainers, especially those linked to the project, can improve their programs and support the project implementation by using the collaborative platform to share knowledge, conduct workshops, and receive feedback. This feedback helps enhance the effectiveness of their training programs, benefiting all participants.

Why collaboration is important?

For the target group of SMEs and the objectives of CyberAgent project, collaboration is important because it gives better learning and skill development. When users work together, they create a dynamic learning environment where they can learn from each other, share experiences, and solve problems together. This peer-to-peer learning helps users quickly gain new skills as they can directly apply the knowledge they learn from their peers to real-world situations.

Resource sharing is another important aspect of collaboration. A collaborative platform allows users to share valuable resources such as documents, templates, best practices, and training materials. This sharing reduces redundancy and ensures that everyone has access to high-quality, up-to-date information and tools.

Building a community is also a key benefit of collaboration. Creating a community of practice encourages continuous professional development and support. Users can network, form professional relationships, and establish a support system that goes beyond the platform itself.
Lastly, collaboration fosters innovation and problem-solving. When users collaborate, they bring diverse perspectives and ideas to the table, which can lead to innovative solutions. Together, they can brainstorm and develop new strategies to tackle cybersecurity challenges effectively.

Known challenges for SMEs related to reskilling and upskilling

Based on the "D2.2 - The SME Cyber Security Change Agents Training needs mapping report" and findings from open sources, the platform must meet several challenges.
SMEs often operate with tight budgets and don't have a dedicated training department. This limits their ability to provide comprehensive training programs themselves.[1]
Most SMEs do not have in-house cybersecurity experts capable of training other staff, leading to gaps in knowledge and skills.[2]
The extremely fast development in threats in cybersecurity, makes it challenging for SME employees to stay updated with the latest threats and defence mechanisms.[3]
Employees in SMEs typically wear multiple hats and may find it difficult to allocate time for training amidst their regular duties.[4]
There is often a lack of awareness about the importance of cybersecurity, and a culture that may not prioritize continuous education in this field and at same time the motivation among employees for lifelong learning is low, as example from latest report from Norway telling the fact that as many as 41% of the companies agree with the statement that employees do not want to participate in competence development activities is a reason for lack of participation. [5] [6]
All these and other country specific several more, is challenges the platform need to meet.

[1] https://www.oecd-ilibrary.org/sites/b404f7fc-en/index.html?itemId=/content/component/b404f7fc-en
[2] https://www.cyberagents.eu/resources
[3] https://www.oecd.org/cfe/smes/Digital%20Upskilling%20Reskilling%20and%20Finding%20Talent%20-%20Key%20Highlights%20-%20March%202022.pdf
[4] https://www.digitalsme.eu/digital-skills-for-smes-challenges-and-opportunities/
[5] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Adult_learning_statistics
[6] https://www.nho.no/contentassets/8e109c8e8c654fcbb74ec48cabf5a142/nhos-kompetansebarometer-2023.pdf

1. GENERAL FEATURES OF COLLABORATION PLATFORM

When it comes to the elaboration of CyberAgent – the collaborative platform – one of the most significant components to be provided is, thus, the general view on its characteristics. These features are important as they point out the interaction with the platform, it functionality, and the overall capacity in enhancing security combined with effectiveness in learning with the aim of upskilling in cyber-security. Organising the needs analysis with a specific focus on these aspects, we started this section with a general description of the overall format of the collaborative platform.

Specifically, this section included eight thoroughly designed questions for the purpose of illuminating a variety of expectations, needs and preferences of stakeholders. That is why the questions were formulated not only to identify the list of basic and additional features but to determine how they can meet the needs of SMEs in learning and correspond to the existing approaches to digital education in Europe.

The feedback that will be collected from this section will be used to inform the first stages of design and build for the platform to guarantee that the platform offers a full scope of features and services while also having a high degree of specificity in what is offered. From this standpoint, this part of the needs analysis is pertinent for establishing the framework compatible with the idea of the platform as the means of increasing the teams' cybersecurity literacy of SMEs from local and regional networks.

To pinpoint the specific functionalities required for the CyberAgent collaborative platform, we initiated our inquiry with a question directly addressing this critical aspect. This query was designed to identify the key features that stakeholders believe are essential for maximizing the platform's effectiveness in supporting continuous cybersecurity upskilling.

The initial part of our survey focused on identifying the essential communication and collaboration tools to integrate into the CyberAgent collaborative platform, aiming to enhance cybersecurity upskilling processes. Stakeholders were queried on their preferences for various tools and features that would facilitate effective group discussions and direct messaging capabilities.

1.1. GROUP DISCUSSIONS AND COLLABORATION TOOLS

The results showed that there was a moderate preference for the kind of tools required for teamwork and group discussions. Forum or discussion board and video conference also received an equal preference with 23% of the respondents who revealed the need for both synchronous and asynchronous technologies. Likewise, group chats and document collaboration tools both got 21% of the vote, proving that having multiple communication tools capable of supporting diverse types of interactions and work-related processes is essential.

1.2. DIRECT MESSAGING TOOLS

When it comes to direct messaging, the survey results indicated a clear preference of instant messaging, which was preferred by all the selected members, 35% of them, implying that fast and relatively informal means of communication are the most popular among users. Email Integration was the next with 32% of respondents pointing to it, showing that email remains a key tool of business communication. Two forms of messaging that recorded slightly lower ratings were voice messages and video messaging, with 19% and 12% ratings respectively, indicating that while people may not prefer as many forms of messaging, they may still occasionally appreciate options that offer other means of sending messages.

1.3. SOCIAL NETWORKING FEATURES

As for the implementation of social networking features to promote better collaboration and networking 45% of the respondents agreed that basic features like profiles and connections should be implemented. This means a certain level of affinity to social networking components that can be used for creating students' communities while preserving the main idea of the platform as an educational and professional resource.

1.4. NOTIFICATION SYSTEMS

When it comes to the types of notification systems, the participants' responses indicated that email is the most effective method of being notified on collaborations and communications with 44 percent of individuals choosing it. This preference was again topped by 28 respondents who preferred push notifications and with 16 respondents who chose in-app notifications. This is indicating people's willingness to incorporate the conventional but effective means of passing notifications within the online platform of email.

SUMMARY

It is evident from the survey findings that the users of the CyberAgent platform need a diverse array of communication functions that can foster both shallow and triangular communicational patterns. This includes a combination of asynchronous/synchronous communications tools, direct messaging functionality, and incorporation of social networking. Additionally, the fact that the respondents preferred the traditional way of receiving communication updates through email only shows that accessibility as well as reliability is paramount in notification systems. The results of this research will inform the design of a novel, communication-focused system to address identified challenges and foster a collaborative and learning experience to facilitate effective cybersecurity upskilling of SMEs.

2. INTEGRATION OF EUROPEAN DIGITAL INNOVATION HUB (EDIH) ON THE COLLABORATIVE ONLINE PLATFORM

The second part of the survey focused on the future integration with the European Digital Innovation Hubs (EDIHs) of the collaboration platform of CyberAgent. The integration is therefore necessary to improve and the effectiveness of the cyber agent upskilling intervention as well as promote digital transformation in SMEs. To that end, the survey questions were geared towards establishing the relevance of the following features that could facilitate collaborations and integration with EDIHs.

2.1. ESSENTIAL INTEGRATION WITH EDIHs

According to the survey, 60% of the respondents strongly stressed that the integration with EDIHs is crucial. This strong consensus suggests that EDIHs are playing a pivotal role in the digitalisation and cybersecurity of SMEs in the EU Member States, which makes it essential for the platform to be in sync with the objectives and available resources at the EDIH level.

2.2. PARTICIPATION IN EDIH-Led INITIATIVES

Of all the aspects in allowing platform users to engage and contribute to or co-lead projects and initiatives spearheaded by EDIHs, 50 percent of the respondents rated it as very important, and 40 percent said that it is essential. This suggests a lot of desire for direct interaction with the platform that may create effective educational settings for improved training processes and professional development in the context.

2.3. NETWORKING, MENTORSHIP, AND COMMUNITY BUILIDNG

The integration of networking features that facilitate mentorship and community building among SMEs was also highlighted as a priority. Half of the respondents rated this as very important, and 30% as essential. These features are viewed as fundamental to creating a supportive ecosystem that encourages information exchange, peer-to-peer learning, and professional connections across the digital landscape.

2.4. CALENDAR AND REGISTRATION FOR EDIH EVENTS

The need to address event, workshop, and webinar management through a shared and centralized calendar and registration system for EDIHs was also considered. It is important that the platform must allow with ease to attend such an event that makes the user benefited in terms of getting educations and meeting and interacting with other users that is the primary purpose of EDIH. The responses gathered from the survey reveal the need to have option such as these to allow for better encouragement of more interaction and commitment to learning and connectivity agendas.

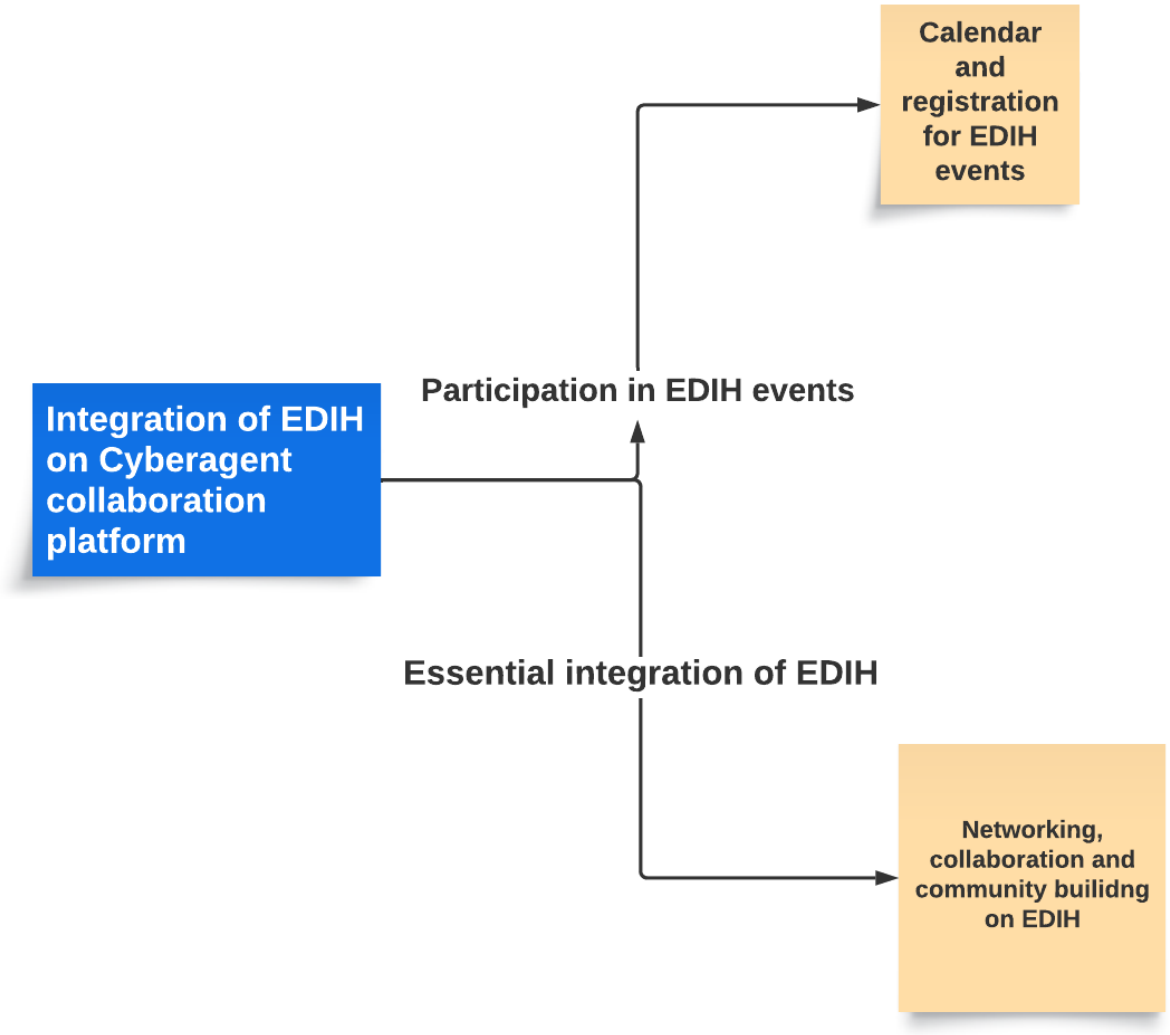

Figure 1 - Integration of EDIH on Collaboration platform

Summary

From the survey data it emerged a loud desire that the CyberAgent platform should be highly compatible with the EDIHs across Europe. It is considered as critical not only for the development of cybersecurity competencies but also for promotion of the overall digital transformation within SMEs. This is noticeable from the highlighted features that touch on the need to have direct participation in the EDIH-led projects, impressive networking, and event management solutions to make the platform effective. These insights will help in creating a platform that will not only be an educational tool but also a link that will bring the SMEs to the realm of the digital innovation in Europe.

3. INTEGRATION OF EUROPEAN DIGITAL EDUCATION HUB (EDEH)

Section 3 of our survey addressed the planned integration of the CyberAgent collaboration platform with the European Digital Education Hub (EDEH). This integration aims to promote digital education and ensure synergies with the European Education Area, vital for fostering a well-rounded digital education ecosystem. The survey questions in this section sought to evaluate the importance of various features that could enable effective integration with EDEH.

3.1. ACCESS TO DIGITAL LEARNING RESOURCES

70% respondents asserted that they want to be provided with direct access to digital learning resources, courses, and materials which are offered by EDEH. An additional 20% rated that this feature is important. Response highlights need for integration with educational content that enhances learning opportunities for users, making the EDEH key resource in the digital education landscape.

3.2. DISCOVERY AND PARTICIPATION IN EDEH EVENTS

When asked about the importance of including features for discovering, registering, and participating in events, workshops, and webinars organized by EDEH, the feedback was strongly positive. Eighty percent of the participants found this very important, indicating a high demand for engagement with ongoing educational activities. Additionally, 10% considered it essential, further emphasizing the relevance of this feature for user engagement and continuous learning.

3.3. NETWORKING, MENTORSHIP AND COLLABORATION

The survey also addressed the importance of facilitating networking, mentorship, and collaboration among learners, educators, and digital education stakeholders. 50% of respondents considered it very important, 30% essential, and 20% somewhat important. This distribution suggests an interest in features that support community building and collaborative learning environments.

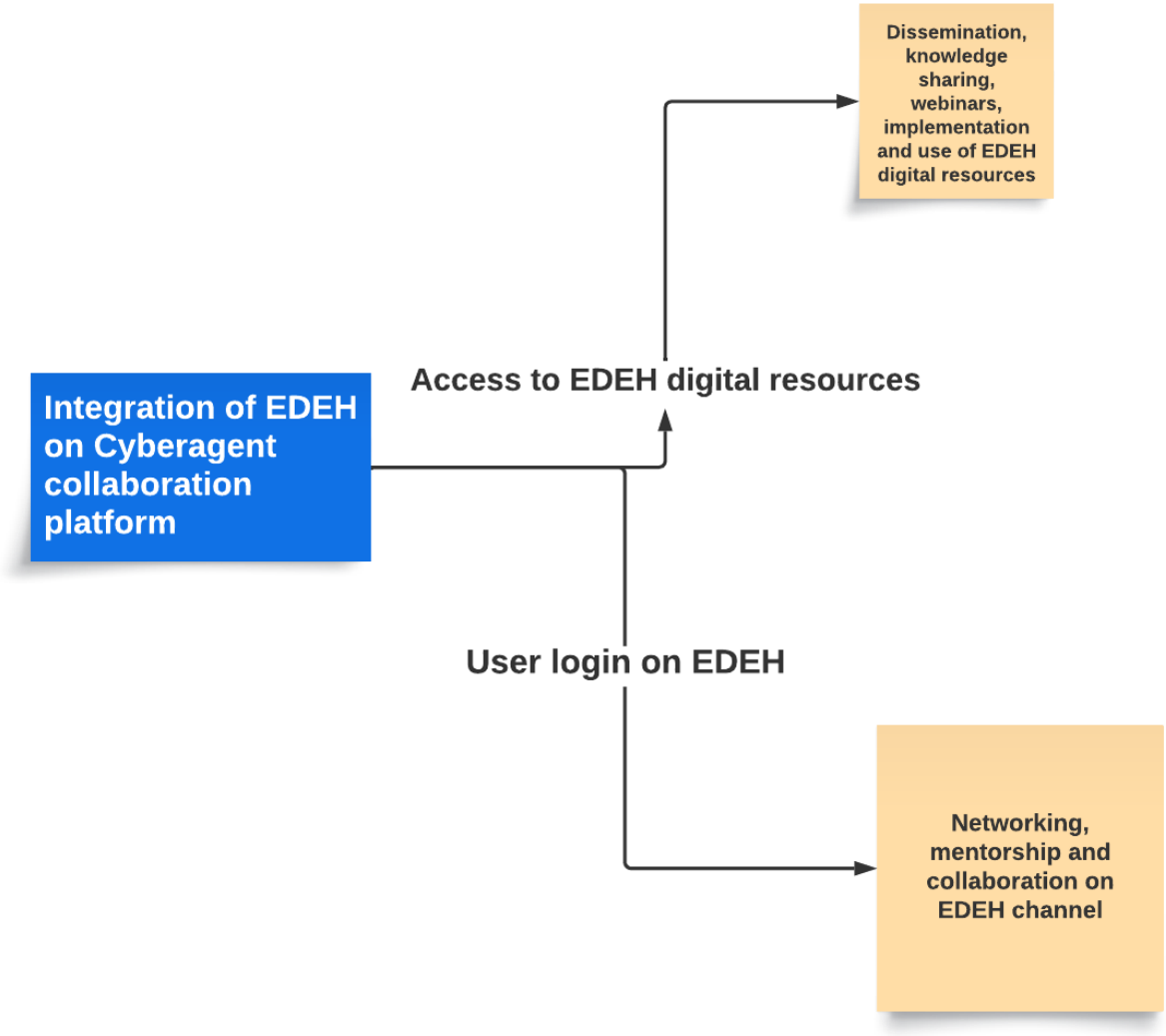

Figure 2 - Integration of EDEH on collaboration platform

Summary

The survey results from Section 3 clearly highlight the importance of integrating the CyberAgent platform with the EDEH. There is a strong response on the necessity of access to high-quality digital learning materials and participation in educational events. These insights will be pivotal in shaping a platform that not only supports cybersecurity upskilling but also contributes significantly to the broader digital education ecosystem in Europe.

4. USER INTERFACE

Section 4 of our survey concentrated on the user interface (UI) design, an important component that ensures engaging user experience on the CyberAgent collaboration platform. This chapter summarizes responses regarding the UI's intuitiveness, accessibility, and customization.

4.1. INTUITIVENESS AND EASE OF USE

Participants were asked to describe their vision for the platform's user interface. Common answers included "intuitive," "easy," "user-friendly," and "platforms." These terms highlight the importance of a design that is welcoming and easy to users, ensuring that the platform facilitates efficient navigation and interaction, which is crucial for maintaining user engagement and satisfaction.

4.2. ACCESSIBILITY FOR USERS WITH DISABILITIES

The question of accessibility for users with disabilities generated varied opinions. Some responses emphasized the critical importance of making the platform accessible by ensuring it is operable with a keyboard. Others considered accessibility as less critical, suggesting that many users likely already possess assistive tools that compensate for any platform shortcomings. However, a significant number of responses highlighted the ethical and practical necessity of designing with inclusivity in mind, pointing out that a platform which supports users with disabilities widens its usability and appeals to a more diverse audience. The sum-up underlines the need for a platform that have various solutions for disabilities, enhancing the user experience and ensuring that everyone, regardless of ability, can benefit from the platform's features.

4.3. CUSTOMIZATION OF THE UI

For users, there was mixed opinion about the customizability of parts of the UI such as the theme and layout. Fifty percent of the respondents consider this factor to be unimportant, while 30% consider it somewhat important and 20% consider it very important. This means that while customization may enhance the experience for some users, most do not consider it a priority. However, providing some flexibility and meeting individual preferences and needs can contribute to comfortable personal and user interactions.

Summary

The data collected in this section reflect a strong desire for an intuitive and accessible user interface, highlighting the need for simple, friendly design for all users Development appears to be an important concern, with many responses supporting the inclusion of features that ensure the platform is used by individuals with disabilities Apparently committed to inclusion and currently customizing the UI is seen as desirable but necessary. These insights will guide the design of a user interface that is not only functional and simple but also adaptable to the different preferences of users It is expected that this approach will provide a learning and collaborative environment an inclusive, fun and effective on the CyberAgent platform.

5. DATA SECURITY AND PRIVACY ON THE CYBERAGENT COLLABORATION PLATFORM

Section 5 of our survey examined important data security and privacy concerns for the CyberAgent Collaboration Platform. This chapter summarizes responses to these concerns, expectations, and measures needed to ensure strong data protection.

5.1. CONCERNS REGARDING DATA SECURITY AND PRIVACY

Respondents highlighted a strong emphasis on the importance of data security, saying it crucial for platform to protect against threats such as data theft, unauthorized access, exploitation, and disclosure. The need for a secure hosting environment was also highlighted, with a preference for providers like Amazon or Google that add up to certified methodologies for data security and management. Privacy concerns were focused on the minimal and secure handling of personal information, advocating for GDPR encryption and practices. Additional security measures like two-factor authentication were discussed, with opinions varying on their necessity but recognizing their potential to enhance security.

5.2. ADAPTING TO THE EVOLVING CYBERSECURITY LANDSCAPE

Responding to the evolving needs of SMEs and how the platform must adapt to the evolving cybersecurity landscape highlighted the need for proactive security practices. Respondents suggested that the platform must effectively integrate advanced technologies such as AI with user data to stay ahead of emerging threats. It is important to regularly update security systems to protect. The importance of user-friendliness of the platform was also highlighted, ensuring that all participants could easily access and participate in safety issues and in the materials.

5.3. IMPLEMENTATION OF TWO-FACTOR AUTHENTICATION

When asked about the implementation of two-factor authentication (2FA) for enhancing user account security, 50% of the respondents said it is essential, while 40% rated it as somewhat important, and 10% viewed it as not important. This suggests a strong recognition of 2FA as a valuable tool to improve account security, though not seen as mandatory.

Summary

The statistics collected on this segment underscores the paramount importance of robust statistics security and privateness measures on the CyberAgent collaboration platform. The expressed issues and guidelines highlight the want for a secure, compliant, and consumer-focused approach to statistics management and protection. As cybersecurity threats evolve, so the must platform evolve. Adapting via continuous upgrades and the combination of advanced technology. The implementation of two-factor authentication is largely supported, reflecting a proactive stance in the direction of enhancing safety protocols. These insights could be pivotal in developing a platform that now not most effective meets the modern-day security needs however is also equipped to handle future challenges, thereby making sure the accept as true with and protection of all customers.

6. USER FEEDBACK AND PLATFORM IMPACT ASSESSMENT ON THE CYBERAGENT COLLABORATIVE PLATFORM

Section 6 of our survey addressed user feedback mechanisms and the evaluation of the platform's impact, especially for SMEs' cybersecurity upskilling. This chapter summarizes the survey responses how the platform should engage with users to collect feedback and monitor its effectiveness.

6.1. COLLECTING AND INCORPORATING USER FEEDBACK

Participants suggested a variety of methods to collect user feedback effectively, with the main idea on the need for a multi-faceted approach. Methods included surveys, interviews, focus groups, usability tests, analytics, reviews, and monitoring social media interactions. Many responses emphasized the importance of integrating feedback directly within the platform, such as at the completion of learning modules or upon exiting the platform, to have immediate and relevant user experiences and opinions.

A recurring theme turned into the want for methodical collection thru structured remarks paperwork that help categorize and systematically analyse the data. Respondents additionally suggested that the platform need to offer summaries of feedback at everyday durations (each 1-6 months) to illustrate responsiveness and inspire continuous engagement through displaying users that their remarks is valued and acted upon.

6.2. MONITORING EFFECTIVENESS AND IMPACT

Regarding the evaluation of the platform's effect on SMEs' cybersecurity capabilities enhancement, responses highlighted the importance of implementing diverse monitoring gear and strategies. Suggested mechanisms covered the use of analytics to tune user engagement metrics along with session times, crowning glory fees, and interplay with special modules. Performance metrics, like quizzes and exams, were additionally regularly referred to as essential tools for measuring mastering outcomes and proficiency upgrades.

Several respondents encouraged for more qualitative strategies, which includes periodic surveys and interviews, to accumulate in-depth remarks at the platform's usability and effectiveness. This method might assist understand the practical benefits customers advantage from the platform and any areas where it could fall short.

6.3. ADDITIONAL COMMENTS AND SUGGESTIONS

There were some further suggestions that focused on technology as a means of improving feedback loops including AI and the partnership with social media to get a wide range of users' insights. The platform was suggested to be developed into a complex cyber security training centre and it was also proposed that general social collaboration should take place at existing social platforms which are more suitable for such purpose.

Summary

Feedback received from this section tells us that we need to take a step further in the development of interaction mechanisms to get all types of user feedback and using (also) this instrument for evaluation of the platform's impact on SMEs' cybersecurity competence. With applying feedback tools that depend on both quantitative and qualitative methods, such as direct users' feedback, performance metrics, social media monitoring, the platform can improve its goods and adapt its services, so they are more valuable for end-users. This approach is an adaptation which is important so that the shifting market of cyber security training will continuously remain effective system.

7. TECHNICAL SOLUTIONS FOR THE CYBERAGENT PLATFORM

The CyberAgent platform is designed with a robust and modern technical architecture, ensuring high performance, security, and scalability. The technical solutions chosen for both the front-end and back-end components of the platform leverage state-of-the-art technologies to deliver a seamless user experience and robust data protection.

FRONT-END DEVELOPMENT

The front-end of the platform will be developed using the Vue3 JavaScript framework. Vue3 is selected for its flexibility, ease of integration, and efficient rendering capabilities, making it ideal for building interactive and responsive user interfaces. To manage the state of the client's session, Pinya will be employed. Pinya provides a lightweight yet powerful state management solution, ensuring that the application state is consistently maintained across different components.

For styling and UI elements, the platform will utilize Tailwind CSS in combination with DaisyUI. Tailwind CSS offers a utility-first approach to styling, enabling rapid and efficient design customization without compromising on performance. DaisyUI extends Tailwind CSS with pre-designed components, streamlining the development of a visually appealing and cohesive user interface.

BACK-END DEVELOPMENT

The back end will be developed using Node.js and the Express framework. Node.js provides a scalable and high-performance environment for server-side applications, while Express offers a minimalistic and flexible framework for building robust APIs.

To manage user sessions and verify authorization, the back end will utilize JSON Web Tokens (JWTs). JWTs are created by the server and stored client-side, providing a secure method for session management and user authentication. Passwords created during user registration will be encrypted using Bcrypt before storage in the database, ensuring that user credentials are securely protected.

DATA MANAGEMENT AND STORAGE

The platform's data will be stored on a managed MongoDB NoSQL database, hosted by Digital Ocean in the Netherlands. This setup offers high availability and end-to-end SSL encryption, ensuring that no information is transmitted in plaintext. Additionally, data stored in the database will be encrypted at rest using LUKS, providing an extra layer of security. Access to the database is tightly controlled, with only whitelisted sources permitted, enhancing overall data protection.

Files uploaded to the platform will be stored in Azure Blob Storage, located in the Northern Europe region (Stockholm). Azure Blob Storage with locally redundant storage ensures data redundancy and availability, safeguarding against data loss.

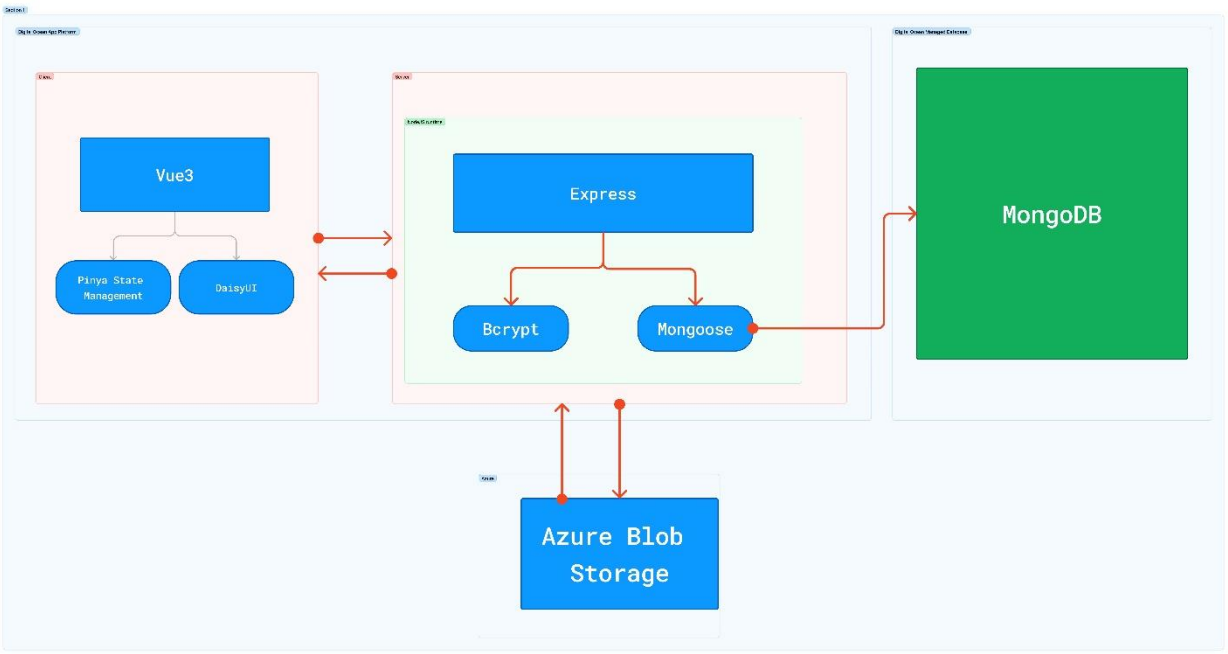

Figure 3 - CA tech stack

Summary

The technical solutions implemented for the CyberAgent platform are carefully selected to ensure a secure, efficient, and scalable environment. By leveraging advanced technologies like Vue3, Node.js, and Azure, the platform provides a seamless user experience while maintaining stringent security standards. This modern and robust technical architecture positions the CyberAgent platform as a reliable tool for cybersecurity upskilling and collaboration among SMEs.

8. CONCLUSION

CORE FUNCTIONALITIES FOR THE CYBERAGENT PLATFORM

The CyberAgent platform is developed to cover various needs of SMEs, institutions and security experts in Europe who participated in the many talks and analyses referred to in this report as well as identified such needs. The core functionalities that are reached through discussion require that the platform support good quality educational events, networking opportunities and grow organically without losing economic sustainability. Some attractive features often associated with more mature systems like cutting-edge AI-driven analytics, document collaboration tools, full CRM integrations etc., have been intentionally left out of the core system. Thanks to this resolution, the platform will stay on a course of education and collaboration as its main direction while joining financial constraints and specific requirements of both budget and the stakeholders of CyberAgent project. This concentration makes sure that it remains unnecessary for any complex service but offering essential services required for SME employees, which is consistent with contributing to creation of cyber environment based on training and collaboration principle.

8.1 Centralized communication tools

Messaging system

Enables direct messaging between individuals and groups to facilitate private and group discussions.

Discussion forums

Allows for threaded discussions on various topics related to cybersecurity, where stakeholders can post queries, share insights, and discuss challenges.

8.2 Resource sharing and management

Document management system

Provides a secure repository for training materials, guidelines, best practices, and other educational resources, with capabilities for version control and access management.

Downloadable resources

Enables users to easily download templates, toolkits, and other resources for offline use.

Search functionality

Helps users efficiently find resources and discussions relevant to specific cybersecurity topics.

8.3 Learning and development tools

E-Learning Modules

Supports interactive learning through courses that can be self-paced or instructor-led, complete with quizzes and certification.

Tracking and reporting

Allows users to track their progress through courses and report on their learning outcomes, facilitating the award of micro-credentials or certificates.

Webinar and workshop scheduling

Enables planning and registration for live sessions, integrating calendar functionalities for reminders and scheduling.

8.4 Community building features

Networking Profiles

Users can create and maintain profiles that highlight their skills, experiences, and interests to foster networking opportunities.

Social networking integration

The platform will facilitate the sharing of existing social media profiles, such as LinkedIn, Facebook, or other relevant platforms. This feature will allow participants to easily connect and network by linking their existing professional and social profiles directly within their user profiles on the CyberAgent platform.

Collaboration with EDIH and EDEH

Direct links or news feeds from EDIH and EDEH can be integrated in the platform, allowing users to easily access and participate in hub-related events, workshops, and discussions directly from their profiles. If the EDIH and EDEH platforms allow it, this could include calendar integrations that sync with EDIH and EDEH events, providing seamless access to hub activities and use it for dissemination.

Feedback and interaction tools

Includes like, comment, and share options to engage with content posted by others, as well as tools for users to provide feedback on resources and sessions.

8.5 Administration and analytics

User management

Allows administrators to manage access rights, monitor platform use, and control the distribution of materials based on roles and needs.

Analytics dashboard

Provides insights into how resources are being used, the effectiveness of training modules, and overall engagement levels across the platform.

Security features

Authentication mechanisms, secure data encryption, and compliance with relevant data protection regulations (like GDPR) in EU and partner countries to ensure the safety and privacy of all communications and data shared on the platform.

Mobile accessibility

Ensures the platform is responsive and accessible via mobile devices, enabling users to learn and interact on-the-go.

8.6 Potential alternatives

There is as this report is written a huge ongoing development related to reducing language barriers. Prios, as responsible partner for building the platform, will investigate the possibilities to integrate tools which simplifies the transnational communications and collaboration. Examples of such tools might be chat automatically translating messages and webinar stream automatically translate the speaker and provide real time speech in wanted language.

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau