Journey of Minds: Cybersecurity": Open-World Game Development for Cybersecurity Learning with GDLC Approach

Muhammad Ariestama Putra[1], Rizki Hikmawan[2*], Reisa Aulia Sodikin[3]

Universitas Pendidikan Indonesia, Jl. Dr. Setiabudi No.229, Isola, Kota Bandung, 40154, Indonesia Indonesia
[1] ariestamaputra04@upi.edu; [2] hikmariz@upi.edu; [3] reisaaulias@upi.edu*
** corresponding author*

ARTICLE INFO

Article history
Received April 22, 2026
Revised May 15, 2026
Accepted June 19, 2026

Keywords
Cybersecurity education
Educational game
Gdl
experiential learning
Adaptive scaffolding
Open-world game

ABSTRACT

The increasing number of cyber threats, including phishing, credential theft, and ransomware attacks, highlights the importance of cybersecurity education for young digital users. This study aimed to develop and evaluate Journey of Minds: Cybersecurity, an open-world educational game designed to introduce cybersecurity concepts through interactive and contextual learning experiences. The study employed a Research and Development (R&D) approach using the Game Development Life Cycle (GDLC), which consists of initiation, pre-production, production, testing, deployment, and assessment stages. The game was developed by integrating experiential learning, flow theory, and adaptive scaffolding principles into its gameplay design. Functional testing was conducted using the Black Box Testing method, while user validation was carried out through a one-on-one beta testing approach. The results showed that all game features functioned according to their intended design and that users were able to complete all testing scenarios. Differences in completion time were observed across gameplay segments, particularly in exploration and problem-solving activities, reflecting variations in user adaptation and interaction with the game environment. Interview results also indicated positive responses toward the learning content, storyline, and gameplay experience, although several suggestions related to navigation guidance and task instructions were identified. These findings suggest that Journey of Minds: Cybersecurity has potential as an interactive learning medium for introducing cybersecurity awareness through experience-based learning. Nevertheless, further studies involving larger participant groups and learning outcome measurements are required to evaluate its educational contribution more comprehensively.

I. Introduction

The increasingly pervasive digital transformation in everyday life has positioned information technology as a fundamental component of communication, education, financial activities, and organizational operations. While this transformation provides significant benefits in terms of accessibility, efficiency, and connectivity, it also introduces new cybersecurity risks that continue to evolve in scale and complexity. Contemporary cyberattacks are no longer limited to exploiting technical vulnerabilities within information systems; they increasingly affect service continuity, public trust, and organizational sustainability. Recent global threat reports indicate that ransomware remains among the most damaging forms of cyberattacks worldwide. The Sophos State of Ransomware Report revealed that 59% of surveyed organizations experienced ransomware attacks during the previous year, highlighting the persistent prevalence and impact of this threat across multiple sectors (Sophos, 2024). Similarly, ransomware, credential theft, and identity-based attacks continue to be identified as some of the fastest-growing cybersecurity challenges due to the increasing sophistication of attack techniques and the widespread dependence on digital services (Alliance, 2025; Deloitte, 2025). The consequences of these attacks extend beyond direct financial losses to include operational disruption, reputational damage, and the exposure of sensitive information, reinforcing the importance of cybersecurity awareness and competence as essential requirements for individuals and institutions operating within today's digital ecosystem (Sophos, 2024).

In practice, contemporary cyber threats increasingly exploit user interaction as an entry point for compromising systems. Phishing and social engineering techniques are commonly employed to establish false trust through seemingly legitimate messages, websites, or digital interfaces, encouraging victims to voluntarily disclose sensitive information. Such attacks frequently lead to credential theft, which can subsequently be used to gain unauthorized access to legitimate systems and facilitate further malicious activities, including ransomware attacks that encrypt data and generate substantial operational and financial losses (Gitnux, 2025). A threat intelligence report from Microsoft (2024) similarly highlights that social engineering remains one of the most common initial attack vectors, while ransomware continues to exploit compromised credentials as a critical stage in the attack chain. This trend is also evident in Indonesia, where the

National Cyber and Crypto Agency reported an increase in phishing incidents and cyber traffic anomalies that may contribute to broader attacks targeting organizational systems and public services (Negara, 2025). These findings suggest that cybersecurity incidents are influenced not only by technical vulnerabilities but also by user decisions and behaviors during digital interactions

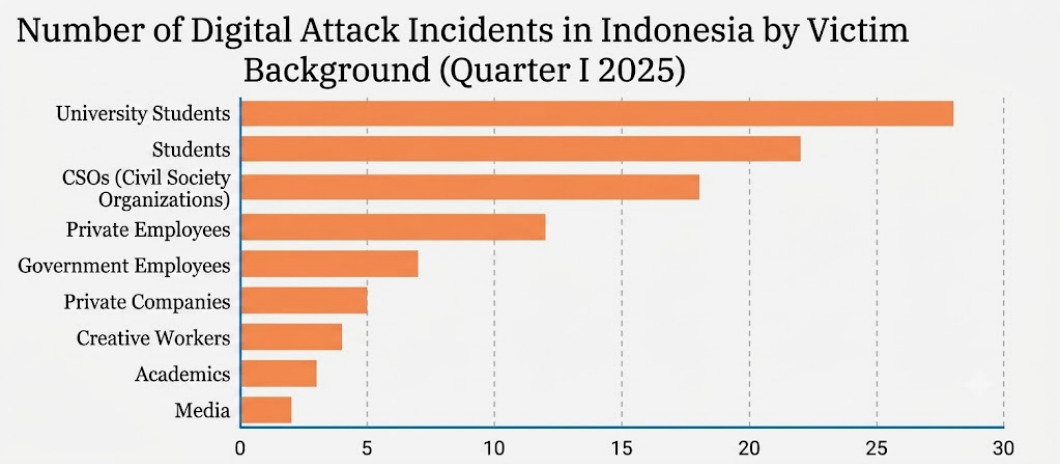


Fig. 1. Distribution of Digital Attack Victims Based on Background in Indonesia

[a] Source: Databoks (2025)

Actions that may appear simple, such as clicking suspicious links, entering credentials on unverified websites, or sharing authentication codes, can provide opportunities for attackers to gain unauthorized access. Consequently, educational interventions that strengthen cybersecurity awareness and decision-making skills have become increasingly relevant. This issue is particularly important for adolescents and young adults, who exhibit high levels of internet usage and mobile device adoption, making them among the most exposed groups to digital content and social engineering attempts (ANTARA News, 2024). To provide further empirical context, Figure 1 presents the distribution of digital attack incidents in Indonesia based on victim background during the first quarter of 2025. The data indicate that school and university students accounted for the largest proportion of reported victims, followed by civil society organizations and private-sector employees. This pattern suggests a relationship between intensive digital technology use and increased exposure to cyber threats among younger populations. Therefore, cybersecurity education initiatives specifically designed for students and young adults are increasingly necessary to equip them with the knowledge and skills required to recognize, prevent, and respond to cyber threats in their daily digital activities.

In response to the increasing complexity of cyber threats, various educational initiatives have adopted game-based approaches to improve cybersecurity awareness and skills among learners. Several systematic literature reviews have demonstrated that serious games and game-based learning can enhance learner engagement, motivation, and conceptual understanding compared to conventional instructional approaches (Gwenhure & Rahayu, 2024; Moumouh et al., 2025; Ng & Hasan, 2025). Existing cybersecurity games employ diverse learning strategies, ranging from quiz-based awareness games and phishing simulations to technical challenge-based environments such as capture-the-flag activities (Olzhas, 2024; Society, 2025). These studies indicate that game-based learning has considerable potential for supporting cybersecurity education across different learner groups and learning objectives. Despite these positive developments, several limitations remain evident in the existing literature. Many cybersecurity educational games primarily focus on introducing concepts or isolated technical skills, often emphasizing knowledge acquisition without providing opportunities for learners to experience the complete learning cycle consisting of concrete experience, reflection, conceptualization, and active experimentation as proposed in experiential learning theory (de Freitas et al., 2021). Furthermore, previous studies have reported that game design frequently prioritizes content delivery while giving limited attention to maintaining a balance between challenge and player capability, which is an essential requirement for achieving a state of flow that supports sustained engagement and meaningful learning experiences (Hamari et al., 2021). Another limitation concerns the implementation of adaptive scaffolding and incremental feedback mechanisms, where learning support is often delivered uniformly rather than adjusted according to learners' progress and needs (Resincen, 2025). These limitations suggest that, although cybersecurity educational games have demonstrated promising outcomes, opportunities remain for developing learning environments that integrate pedagogical and gameplay considerations more comprehensively. Therefore, this study proposes the development of an open-world cybersecurity educational game that combines experiential learning, flow theory, adaptive scaffolding, and narrative-based decision-making within a single learning environment. By allowing players to explore scenarios, make decisions, experience consequences, and receive structured guidance throughout

gameplay, the proposed approach aims to provide a more contextual and meaningful cybersecurity learning experience compared with approaches that focus primarily on content delivery or isolated technical exercises.

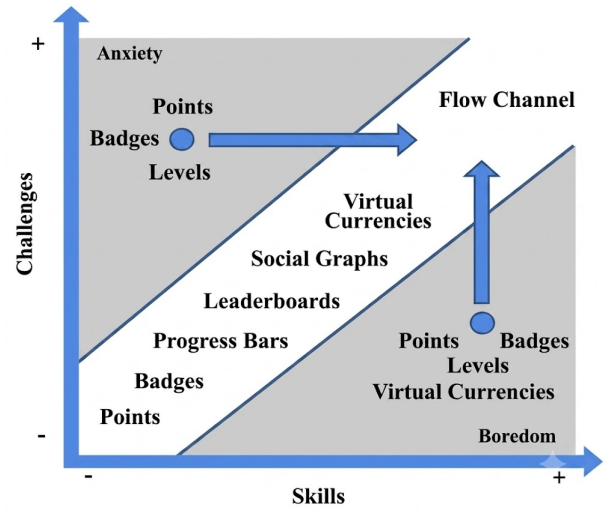


Fig. 2. Game-Based Learning Framework Integrating Flow Theory

Despite the growing number of cybersecurity educational games, several important limitations remain evident. Existing studies generally focus on conceptual awareness or isolated technical exercises and often do not fully integrate the complete experiential learning cycle, where gameplay experiences are systematically followed by reflection, conceptualization, and active application in meaningful contexts (de Freitas et al., 2021; Radianti et al., 2022). Furthermore, game mechanics are frequently designed without sufficient consideration of the balance between challenge and player capability, making it difficult to maintain a sustained flow state that supports long-term engagement and meaningful learning experiences (Hamari et al., 2021). Previous studies have also reported limited implementation of adaptive scaffolding mechanisms that gradually adjust learning support according to learners' evolving abilities, resulting in learning experiences that are less personalized and potentially less effective in supporting skill development (Resincen, 2025). Beyond these pedagogical limitations, existing cybersecurity games rarely represent the complete decision-making chain associated with real-world cyber threats, particularly the progression from phishing attempts and credential theft to ransomware incidents. These limitations indicate a need for a more comprehensive cybersecurity learning environment that combines pedagogical principles, contextual threat scenarios, and experience-based gameplay within a unified learning environment. Based on the identified gaps, this study addresses the following research questions: (1) How can an open-world cybersecurity educational game be developed using the Game Development Life Cycle (GDLC) framework while integrating experiential learning, flow theory, and scaffolding principles? and (2) How do users respond to the functionality, usability, and learning experience provided by the developed game during the initial evaluation stage? Therefore, this study aims to develop Journey of Minds: Cybersecurity, an open-world educational game designed to support contextual cybersecurity learning through the integration of experiential learning, flow theory, and scaffolding principles, and to conduct an initial evaluation of its functionality, usability, and user experience.

II. Method

A. Types and Approaches of Research

This study employed a Research and Development (R&D) approach to design, develop, and conduct an initial evaluation of a cybersecurity educational game. The development process was guided by the Game Development Life Cycle (GDLC), a framework that systematically organizes game creation through iterative stages of design, production, testing, deployment, and evaluation. GDLC has been widely adopted in both game development research and professional practice because it accommodates the complexity of game design, integrates technical and creative components, and supports continuous refinement throughout development (Marinho et al., 2022). In this study, GDLC provided a structured framework for integrating cybersecurity learning objectives with pedagogical principles, including experiential learning, flow theory, and adaptive scaffolding. Consequently, the combination of an R&D approach and the GDLC framework was considered appropriate for developing a cybersecurity educational game that is not only technically functional but also educationally meaningful and aligned with the objectives of cybersecurity awareness learning.

B. Research and Development Procedures (GDLC)

The development procedure in this study followed the Game Development Life Cycle (GDLC), which consists of six iterative phases: initiation, pre-production, production, testing, deployment, and evaluation. The GDLC framework was selected because it provides a structured process for integrating educational objectives, game design elements, and technical development activities within a single development cycle. Through these stages, the study not only focused on producing a functional cybersecurity educational game but also on examining the feasibility of integrating experiential learning, flow theory, and adaptive scaffolding principles into the gameplay design. The implementation of each phase enabled the systematic development of the game, from conceptualization and content design to functional validation and initial user evaluation. Figure 3 illustrates the GDLC stages applied in this study.

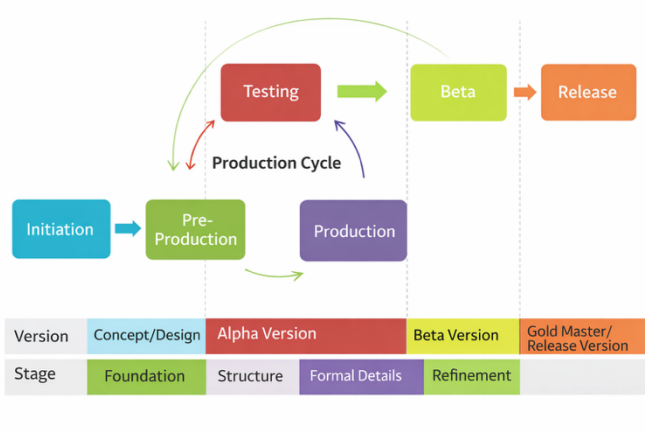


Fig. 3. Game Development Procedure Using the GDLC Model

1) Stage 1: Initiation

The initiation phase focused on identifying the educational problem, defining learning objectives, and establishing the core concept of the game. This process began with an analysis of contemporary cybersecurity threats that frequently affect digital technology users, particularly phishing, credential theft, social engineering, and ransomware attacks. Previous studies and cybersecurity reports indicate that these threats are increasingly associated with human decision-making errors rather than purely technical vulnerabilities, highlighting the importance of cybersecurity awareness and behavioral training among internet users (Gitnux, 2025; Microsoft, 2024; Negara, 2025).

Based on this analysis, adolescents and young adults were identified as the primary target users of the game because of their intensive use of digital technologies, online services, and mobile devices, which increases their exposure to cybersecurity risks. The educational objectives established during this phase included helping players recognize cyber threats, evaluate potential risks, make informed security decisions, and understand the consequences of unsafe online behavior. In addition, the game was conceptually designed as a narrative-driven open-world learning environment that enables players to explore, interact with virtual characters, and experience cybersecurity scenarios within meaningful contextual situations. The outputs of this phase included the definition of learning outcomes, game scope, target users, cybersecurity content coverage, and the initial gameplay concept that guided subsequent development stages.

2) Stage 2: Pre-production

The pre-production phase focused on translating the conceptual framework developed during the initiation stage into a detailed game design. Activities conducted during this phase included preparing the Game Design Document (GDD), designing the storyline, gameplay mechanics, quests, level progression, cybersecurity learning content, and user interaction flows. The objective of this phase was to ensure that educational goals and gameplay elements were integrated into a coherent learning experience. To support cybersecurity learning, the game design incorporated experiential learning, gamification, and scaffolding principles. Experiential learning was represented through direct engagement with cybersecurity-related situations, while gamification elements such as levels, rewards, and progression systems were used to maintain player motivation. Scaffolding principles were implemented through gradual progression from introductory concepts to more complex cybersecurity challenges. The conceptual integration of these components is illustrated in Figure 4.

Based on the learning framework, a gameplay flow structure was designed to organize player progression through cybersecurity topics and learning activities. Players begin with tutorial and introductory content before progressing through scenarios involving malware, phishing, and social engineering threats. Assessment activities were embedded throughout the gameplay experience to encourage active participation and contextual decision-making. The overall gameplay flow and pedagogical integration are presented in Figure 5.

The outputs of this phase included the Game Design Document, learning scenarios, quest structures, gameplay flow diagrams, and assessment mechanisms that guided the subsequent production phase.

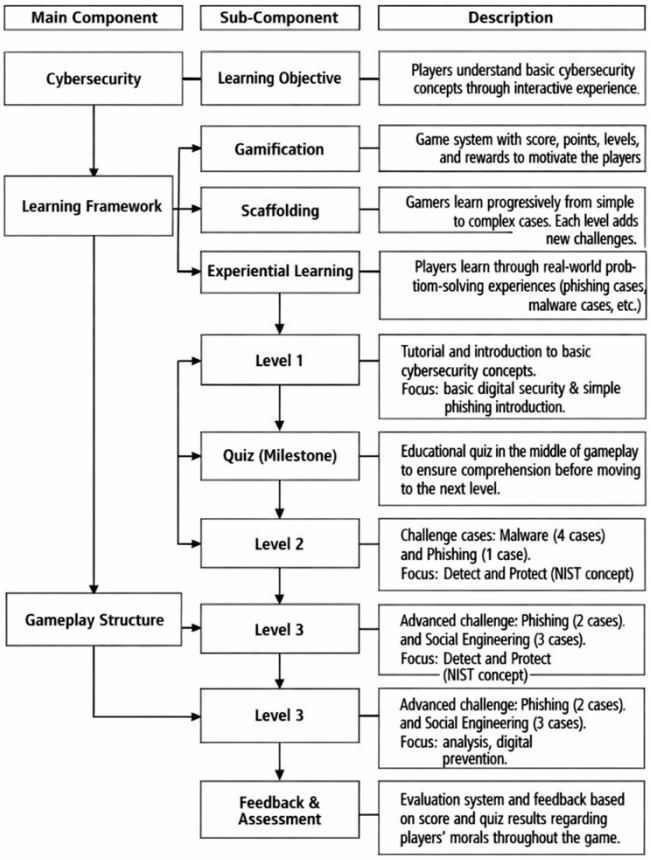


Fig. 4. Integrative Model of Game-Based Cybersecurity Learning with Experiential Learning and Adaptive Scaffolding Approaches

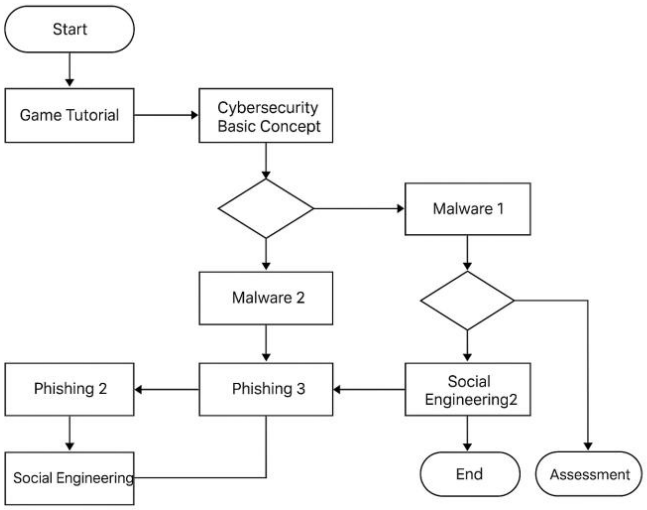


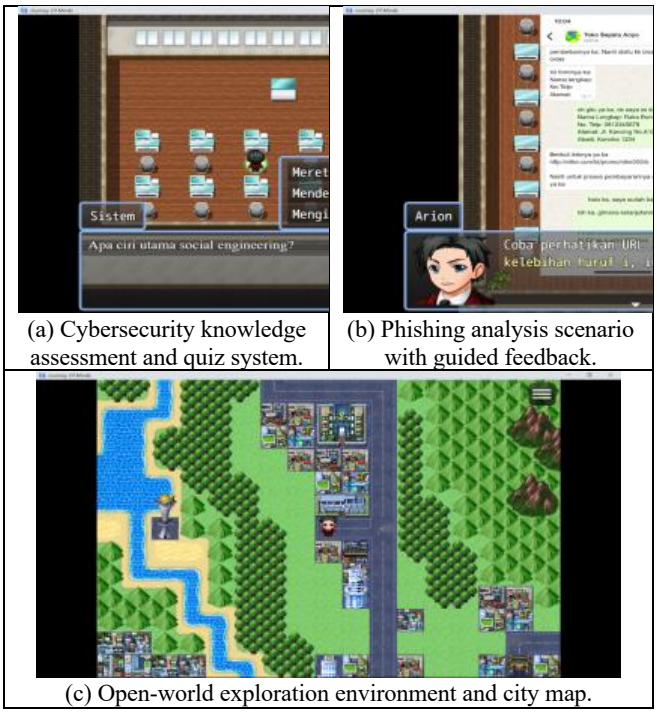
Fig. 5. Game flow design and integration of pedagogical principles in cybersecurity learning games.

3) Stage 3: Production

The production phase focused on transforming the design specifications developed during the pre-production stage into a functional educational game prototype. During this stage, visual assets, maps, character sprites, dialogue systems, quest structures, assessment mechanisms, and cybersecurity learning content were implemented using RPG Maker. The gameplay mechanics, progression system, exploration features, and educational scenarios were integrated into a unified game environment to ensure consistency between learning objectives and player experience. The output of this phase was a playable prototype of Journey of Minds: Cybersecurity that was ready for functional and user-based testing.

To support cybersecurity learning, various interactive features were implemented throughout the game. These features included exploration-based activities, dialogue-driven learning, scenario analysis, cybersecurity quizzes, phishing identification tasks, malware awareness challenges, and social engineering simulations. Learning content was distributed across multiple chapters and presented through contextual situations that required players to observe information, evaluate risks, and make decisions related to cybersecurity threats.

The implemented features demonstrate how cybersecurity concepts were embedded within gameplay activities. Figure X(a) shows the quiz mechanism used to assess players' understanding of cybersecurity concepts during progression. Figure X(b) presents a phishing case scenario in which players analyze suspicious messages and receive contextual guidance through in-game dialogue. Meanwhile, Figure X(c) illustrates the open-world environment that allows players to explore different locations and access learning scenarios distributed throughout the game world. These features collectively support the delivery of cybersecurity content through interactive and contextual gameplay experiences.



(a) Cybersecurity knowledge assessment and quiz system.

(b) Phishing analysis scenario with guided feedback.

(c) Open-world exploration environment and city map.

Fig. 6. Figure X. Selected Gameplay Features of Journey of Minds: Cybersecurity

4) Stage 4: Testing

The testing phase aimed to verify that the developed game functioned according to its design specifications and intended learning flow. At this stage, functional testing was conducted using the Black Box Testing approach to evaluate the performance of game features without examining the internal source code. The testing process focused on assessing whether gameplay components, navigation systems, dialogue interactions, quest progression, assessment mechanisms, scene transitions, and game-ending conditions operated as intended. Each feature was tested against predefined functional requirements to identify potential errors that could disrupt gameplay or interfere with the delivery of cybersecurity learning content. The testing procedure examined player interactions across different gameplay scenarios, including exploration activities, quizzes, cybersecurity case analyses, and mission completion processes. Successful execution of these functions indicated that the game was technically ready for user-based evaluation in the subsequent stage. The output of this phase was a functionally stable game prototype that satisfied the predefined system requirements and was considered suitable for deployment in a limited user evaluation environment.

5) Stage 5: Deployment (Implementation/Trial)

The deployment phase involved releasing the game prototype to a limited group of representative users for an initial evaluation. Three participants were recruited, consisting of two undergraduate students from non-cybersecurity-related academic backgrounds and one vocational high school student majoring in Computer and

Network Engineering. These participants were selected because they represent the intended target users of the game, namely adolescents and young adults who actively use digital technologies, online services, and communication platforms. The purpose of this stage was to identify usability issues, navigation problems, gameplay obstacles, and user perceptions of the educational game before broader implementation.

Each participant was asked to complete all gameplay segments independently. During gameplay, observations were conducted to record task completion, navigation behavior, and potential difficulties encountered by players. Completion times for each gameplay segment were also measured, while qualitative feedback was collected through semi-structured interviews conducted after gameplay. The collected data consisted of gameplay completion records, completion time measurements, observational notes, and interview responses, which were subsequently analyzed during the evaluation phase.

6) Stage 6: Evaluation

The evaluation phase focused on reviewing the outcomes of the development and testing processes to assess the feasibility of the developed educational game. Evaluation activities involved analyzing the results of functional testing, gameplay completion records, completion time measurements, observational data, and user feedback obtained during the deployment phase. The purpose of this stage was to identify the strengths and limitations of the game, evaluate its suitability as a cybersecurity learning medium, and determine areas requiring further refinement. The findings obtained during this phase served as the basis for assessing the overall quality of the game and informing future development efforts. The evaluation results are presented and discussed in the subsequent Results and Discussion section.

III. Results and Discussion

A. Alpha Testing Results

Alpha testing is conducted to evaluate the internal functionality of the system before the game is tested with users. This testing utilizes the Black Box Testing approach, a testing method that focuses on the compatibility between input and output without considering the system's internal structure (Salim & Rusdiansyah, 2025). Testing covers all key game features, such as navigation, interaction systems, quiz mechanics, visual elements, and system feedback.

Table 1. Alpha Testing Results Using the Black Box Testing Method

No	Feature	Testing Scenario	Expected Result	Test Result
1	Main Menu and Navigation Buttons	Accessing the Main Menu and selecting all navigation buttons	All menus open and function properly	As Expected
2	Map Navigation System	User opens the map and searches for Arion's House location	Directions are displayed on the screen after the map is opened	As Expected
3	Room Location Guide	User searches for Arion's room	Clear text directions indicate the room location	As Expected
4	Computer Room Guide	User is directed to the computer room	The system displays text directions to the computer room	As Expected
5	Gate Scene Transition	User presses the gate in the middle of the road	The transition animation runs normally and the area can be accessed	As Expected
6	Navigation to the Internet Cafe	After the dialogue with the teacher ends, the user exits the school	Text directions to the internet cafe appear	As Expected
7	Internet Cafe Direction System	User is outside the school	The system provides directions to the internet cafe location	As Expected
8	Character Naming Consistency	Mentioning the Principal in the dialogue	The character name consistently uses "Principal"	As Expected
9	Quiz and Retry System	User answers incorrectly and retries	User returns to the quiz question, not the chair position	As Expected
10	Scoring System	User completes the challenge	The score does not exceed the specified maximum limit	As Expected
11	Data Leak Visual Effects	The Principal announces that the data has been leaked	Character reaction emojis and blinking effects appear on the data	As Expected
12	Challenge Timer	Timed challenge	The timer appears for 10 seconds according to the design	As Expected
13	Ghoster Storyline	Ghoster directs the user to the Computer Lab	The storyline follows the storyboard	As Expected
14	Game Over System	User selects an unethical answer	The system displays Game Over or repeats the evaluation	As Expected
15	Arion Educational Dialogue	Arion reads an educational message	The text appears as if Arion is explaining to the user	As Expected
16	Conversation System	Interaction between Mrs. Vira and Arion	Dialogue matches the characters, with no self-dialogue bug	As Expected

No	Feature	Testing Scenario	Expected Result	Test Result
17	Notification System	User menyelesaikan misi	Notifications appear as feedback	As Expected

Based on the test results, all features performed as expected, resulting in no significant functional errors during the testing process. The navigation system, interactions, and evaluation mechanisms performed consistently according to the design.

These results align with research on the development of Visual Novel Interactive Game-based learning games, where alpha testing was used to ensure system stability before user testing (Sodikin, 2025).

B. Beta Testing Results

Beta testing involves end users to directly evaluate the system's user experience through a one-on-one validation approach. This approach allows developers to observe user interactions and identify any issues that arise during use (Melfionita, 2022).

Table 2. Beta Testing Results of Participant 1

No	Testing Scenario (Segment)	Expected Result	Test Result	Time Required
1	Segment 1 - Game Introduction & Initial Navigation (Scenario 1-5)	Users can start the game, understand the main menu, and use the basic controls properly without issues	As Expected	1 Minutes 20 Seconds
2	Segment 2 - Exploration Awal & Threat Introduction (Scenario 6-10)	Users can explore the initial environment and recognize early indications of cyber threats	As Expected	4 Minutes 31 Seconds
3	Segment 3 - Quiz Chapter 1 (Scenario 11-13)	Users can complete the quiz properly, and the system can display evaluation results accurately	As Expected	2 Minutes
4	Segment 4 - Exploration Chapter 2 & Interaksi (Scenario 14-17)	Users can perform advanced exploration and interact optimally with the environment or objects	As Expected	7 Minutes 56 Seconds
5	Segment 5 - Quiz Chapter 2 (Scenario 18-20)	Users can complete the Chapter 2 quiz, and the system provides results and feedback correctly	As Expected	2 Minutes 50 Seconds
6	Segment 6 - Simulasi Malware & Backup Data (Scenario 21-24)	Users can perform the investigation and data backup process correctly and understand the consequences of failure (Game Over)	As Expected	6 Minutes 14 Seconds
7	Segment 7 - Quiz Chapter 3 & Story Continuation (Scenario 25-30)	Users can complete the Chapter 3 quiz and continue the storyline smoothly to the next stage	As Expected	4 Minutes 39 Seconds
8	Segment 8 - Exploration & Quiz Chapter 4 (Scenario 31-36)	Users can perform advanced exploration, identify threats, and complete the Chapter 4 quiz properly	As Expected	3 Minutes 12 Seconds
9	Segment 9 - Transition to Chapter 5 & Exploration Awal (Scenario 37-39)	Users can move to Chapter 5 and understand the context and initial objectives in the final stage of the game	As Expected	3 Minutes 3 Seconds
10	Segment 10 - Final Quiz & Game Ending (Scenario 40-46)	Users can complete the final quiz, obtain an ending (success/failure), and exit the game without issues	As Expected	3 Minutes 53 Seconds

Table 3. Beta Testing Results of Participant 2

No	Testing Scenario (Segment)	Expected Result	Test Result	Time Required
1	Segment 1 – Game Introduction & Initial Navigation (Scenario 1–5)	Users can start the game, understand the main menu, and use the basic controls properly without issues	As Expected	1 Minutes 49 Seconds
2	Segment 2 – Exploration Awal & Threat Introduction (Scenario 6–10)	Users can explore the initial environment and recognize early indications of cyber threats	As Expected	6 Minutes 30 Seconds
3	Segment 3 – Quiz Chapter 1 (Scenario 11–13)	Users can complete the quiz properly, and the system can display evaluation results accurately	As Expected	2 Minutes 40 Seconds
4	Segment 4 – Exploration Chapter 2 & Interaksi (Scenario 14–17)	Users can perform advanced exploration and interact optimally with the environment or objects	As Expected	10 Minutes 27 Seconds
5	Segment 5 – Quiz Chapter 2 (Scenario 18–20)	Users can complete the Chapter 2 quiz, and the system provides results and feedback correctly	As Expected	3 Minutes 53 Seconds
6	Segment 6 – Simulasi Malware & Backup Data (Scenario 21–24)	Users can perform the investigation and data backup process correctly and understand the consequences of failure (Game Over)	As Expected	13 Minutes 4 Seconds
7	Segment 7 – Quiz Chapter 3 & Story Continuation (Scenario 25–30)	Users can complete the Chapter 3 quiz and continue the storyline smoothly to the next stage	As Expected	4 Minutes 4 Seconds
8	Segment 8 – Exploration & Quiz Chapter 4 (Scenario 31–36)	Users can perform advanced exploration, identify threats, and complete the Chapter 4 quiz properly	As Expected	3 Minutes 37 Seconds

No	Testing Scenario (Segment)	Expected Result	Test Result	Time Required
9	Segment 9 – Transition to Chapter 5 & Exploration Awal (Scenario 37–39)	Users can move to Chapter 5 and understand the context and initial objectives in the final stage of the game	As Expected	1 Minutes 43 Seconds
10	Segment 10 – Final Quiz & Game Ending (Scenario 40–46)	Users can complete the final quiz, obtain an ending (success/failure), and exit the game without issues	As Expected	5 Minutes 19 Seconds

Table 4. Beta Testing Results of Participant 3

No	Testing Scenario (Segment)	Expected Result	Test Result	Time Required
1	Segment 1 – Game Introduction & Initial Navigation (Scenario 1–5)	Users can start the game, understand the main menu, and use the basic controls properly without issues	As Expected	2 Minutes 16 Seconds
2	Segment 2 – Exploration Awal & Threat Introduction (Scenario 6–10)	Users can explore the initial environment and recognize early indications of cyber threats	As Expected	5 Minutes 38 Seconds
3	Segment 3 – Quiz Chapter 1 (Scenario 11–13)	Users can complete the quiz properly, and the system can display evaluation results accurately	As Expected	2 Minutes 29 Seconds
4	Segment 4 – Exploration Chapter 2 & Interaksi (Scenario 14–17)	Users can perform advanced exploration and interact optimally with the environment or objects	As Expected	6 Minutes 47 Seconds
5	Segment 5 – Quiz Chapter 2 (Scenario 18–20)	Users can complete the Chapter 2 quiz, and the system provides results and feedback correctly	As Expected	2 Minutes 0 Seconds
6	Segment 6 – Simulasi Malware & Backup Data (Scenario 21–24)	Users can perform the investigation and data backup process correctly and understand the consequences of failure (Game Over)	As Expected	6 Minutes 47 Seconds
7	Segment 7 – Quiz Chapter 3 & Story Continuation (Scenario 25–30)	Users can complete the Chapter 3 quiz and continue the storyline smoothly to the next stage	As Expected	3 Minutes 5 Seconds
8	Segment 8 – Exploration & Quiz Chapter 4 (Scenario 31–36)	Users can perform advanced exploration, identify threats, and complete the Chapter 4 quiz properly	As Expected	2 Minutes 21 Seconds
9	Segment 9 – Transition to Chapter 5 & Exploration Awal (Scenario 37–39)	Users can move to Chapter 5 and understand the context and initial objectives in the final stage of the game	As Expected	1 Minutes 50 Seconds
10	Segment 10 – Final Quiz & Game Ending (Scenario 40–46)	Users can complete the final quiz, obtain an ending (success/failure), and exit the game without issues	As Expected	5 Minutes 37 Seconds

Based on the beta testing results, all participants were able to complete the gameplay scenarios according to the intended game flow. All testing segments were successfully executed, indicating that the core gameplay mechanics, navigation system, interaction features, and assessment components functioned as designed. Although all participants completed the testing scenarios, differences in completion times were observed across several gameplay segments, particularly those involving exploration and problem-solving activities. Observational notes also identified several minor usability issues related to navigation guidance and task interpretation, which were subsequently explored through post-game interviews. Overall, the results indicate that the game prototype was sufficiently functional and usable for initial user evaluation.

These findings indicate that the developed game met its intended functional requirements and demonstrated acceptable usability during the initial user evaluation stage. Similar studies have also employed beta testing to verify whether educational game prototypes can be completed successfully by representative users before wider implementation (Sodikin, 2025).

1) Time Calculation Results

Table 5. Average Gameplay Completion Time Across All Participants

No	Testing Segment	Brief Description	Average Time (Minutes)
1	Segment 1 (Scenario 1–5)	Game introduction and initial navigation	1,9
2	Segment 2 (Scenario 6–10)	Initial exploration and threat introduction	5,5
3	Segment 3 (Scenario 11–13)	Quiz Chapter 1	2,7
4	Segment 4 (Scenario 14–17)	Advanced exploration and interaction	8,7
5	Segment 5 (Scenario 18–20)	Quiz Chapter 2	2,8
6	Segment 6 (Scenario 21–24)	Malware simulation and data backup	8,8
7	Segment 7 (Scenario 25–30)	Chapter 3 Quiz and transition	4,4
8	Segment 8 (Scenario 31–36)	Exploration dan Quiz Chapter 4	3,2
9	Segment 9 (Scenario 37–39)	Transition and Chapter 5 exploration	1,7

No	Testing Segment	Brief Description	Average Time (Minutes)
10	Segment 10 (Scenario 40–46)	Final quiz and game ending	5

Based on Table 4.X, the segment with exploration and practice activities has a longer completion duration than the evaluation segment, which is a quiz. The average time is calculated using the formula:

$$\bar{x} = \frac{\sum x}{n}$$

Information:
$\bar{x}$ = Average time
$\sum x$= Total Time of All Testers
n= Number of Teasers

The average completion time was calculated using the arithmetic mean to provide a general representation of the duration required for each gameplay segment. The results show noticeable variation across segments. Exploration-oriented and problem-solving activities required longer completion times than quiz-based evaluation segments. For example, Segment 4 (Advanced Exploration and Interaction) and Segment 6 (Malware Simulation and Data Backup) recorded the longest average durations, while introductory and transition segments required substantially less time. These differences suggest that gameplay activities involving environmental exploration, information analysis, and decision-making required greater user engagement and interaction than assessment-oriented activities.

C. Test Success Percentage

1) Test Case Executed

$$\text{Test Case Executed \%} = \left(\frac{Test\ Case\ Executed}{Test\ Case\ Written}\right) \times 100\%$$

$$= \left(\frac{10}{10}\right) \times 100\% = 100\%$$

2) Test Case Passed

$$\text{Test Case Passed \%} = \left(\frac{Test\ Case\ Passed}{Test\ Case\ Written}\right) \times 100\%$$

$$= \left(\frac{10}{10}\right) \times 100\% = 100\%$$

3) Test Case Failed

$$\text{Test Case Failed \%} = \left(\frac{Test\ Case\ Failed}{Test\ Case\ Written}\right) \times 100\%$$

$$= \left(\frac{0}{0}\right) \times 100\% = 0\%$$

To complement the beta testing observations, a test success percentage analysis was conducted based on the execution status of all predefined gameplay scenarios. The analysis adopted Black Box Testing metrics consisting of test cases executed, test cases passed, and test cases failed (Salim & Rusdiansyah, 2025).

A total of 30 test cases were evaluated during beta testing, representing ten gameplay segments completed by three participants. All test cases were successfully executed and achieved the expected outcomes. Consequently, the percentage of executed test cases reached 100%, the percentage of passed test cases reached 100%, and no failed test cases were identified during testing.

These results indicate that the game prototype functioned consistently across different users and gameplay situations. Nevertheless, although all scenarios were completed successfully, variations in completion time and several usability-related comments were observed during gameplay and post-game interviews. Therefore, the success percentage should be interpreted as evidence of functional reliability rather than as a measure of learning effectiveness or user satisfaction.

Based on the test results, no test cases failed in all tested scenarios. Therefore, the system's success rate reached 100%. These results indicate that all features and gameplay met the designed specifications. This is also consistent with previous research showing that beta testing of educational games generally yields high success rates when the system has undergone optimal alpha testing (Sodikin, 2025).

The testing results indicate that the developed cybersecurity learning game functioned in accordance with its intended design during the evaluation phase. Both alpha testing and beta testing demonstrated that the core gameplay mechanics, navigation features, interaction systems, assessment components, and learning scenarios operated as expected. All participants were able to complete the predefined gameplay segments, suggesting that the game prototype provided sufficient functional stability and usability for initial implementation. These findings are consistent with previous studies reporting that structured game development methodologies contribute to software reliability and support the successful deployment of educational games (Alshamrani et al., 2022; Calderón & Ruiz, 2021).

The use of the Game Development Life Cycle (GDLC) framework also appears to have supported the systematic integration of technical and educational components throughout the development process. Through iterative stages of planning, design, implementation, testing, and evaluation, the framework provided a structured approach

for incorporating cybersecurity learning content into a playable game environment. Rather than demonstrating learning effectiveness, the present findings primarily indicate that the developed prototype achieved its intended functional objectives and was suitable for initial user evaluation.

The completion time analysis provides additional insight into how participants interacted with different gameplay segments. The results show that exploration-based activities, malware investigation scenarios, and decision-making tasks generally required more time than quiz-oriented segments. These differences suggest that participants spent more time observing information, interpreting contextual clues, and considering alternative actions when confronted with realistic cybersecurity situations. In contrast, quiz segments were completed more quickly because they primarily focused on recalling and applying previously encountered concepts.

This interaction pattern is consistent with the principles of experiential learning, which emphasize learning through direct experience, reflection, and active engagement with authentic problems (Radianti et al., 2022). By placing players in simulated cybersecurity situations involving phishing attempts, malware incidents, and social engineering attacks, the game encourages learners to interact with contextual challenges rather than merely receive information passively. While the present study did not directly measure learning gains, the observed gameplay behavior indicates that participants actively engaged with the problem-solving and exploration components designed within the game environment.

The interview findings further complement the quantitative observations obtained during beta testing. Participants generally reported that the game provided an engaging learning experience by presenting cybersecurity concepts through interactive scenarios rather than conventional instructional materials. The open-world structure allowed players to explore different environments, interact with various objects and characters, and encounter cybersecurity challenges within a contextual narrative. This design approach appeared to increase participant interest and encourage exploration throughout the gameplay experience.

Several participants also highlighted that the integration of quizzes, decision-making scenarios, and contextual feedback helped them understand the consequences of different factions within cybersecurity situations. These findings align with previous studies suggesting that game-based learning environments can support learner engagement by combining narrative elements, exploration, and active participation (Gwenhure & Rahayu, 2024; Moumouh et al., 2025; Ng & Hasan, 2025). In addition, the game incorporated gradual guidance mechanisms and structured progression pathways as part of its pedagogical design. However, the present study only evaluated user perceptions during beta testing and did not directly measure the effectiveness of adaptive scaffolding or flow-based mechanics on learning outcomes and engagement. Therefore, the contribution of these design elements should be interpreted as a conceptual implementation within the game design rather than as empirically validated instructional interventions.

The findings of this study can also be viewed in relation to previous cybersecurity educational game research. Similar to Your Zero Hour, which utilized a visual novel approach to introduce ransomware awareness through adaptive learning mechanisms, the present study demonstrates the potential of integrating cybersecurity content within an interactive narrative environment. Likewise, the findings are consistent with RansomForge, which reported that the application of the Game Development Life Cycle (GDLC) contributed to the successful development and functional implementation of a cybersecurity educational game. In addition, the role-playing game developed by Ardiansyah (2023) highlighted the value of narrative-driven interactions in helping users understand cybersecurity-related situations through direct participation in gameplay. While these studies employed different game genres, learning strategies, and implementation approaches, they collectively indicate that interactive game environments can provide meaningful opportunities for introducing cybersecurity concepts through active user engagement. The present study extends this body of work by combining an open-world RPG structure with experiential learning, flow-oriented design considerations, and scaffolding principles within a single cybersecurity learning environment.

Nevertheless, several limitations should be acknowledged. First, the initial user evaluation involved only three participants and was intended as a formative assessment rather than a large-scale effectiveness study. Second, the study did not employ pre-test and post-test measurements or a control group; therefore, conclusions regarding learning improvement cannot be drawn from the current findings. Third, although scaffolding principles were incorporated into the game design, their specific contribution to learning and user engagement was not evaluated independently. Consequently, future research should involve larger participant groups, incorporate experimental evaluation methods, and investigate the impact of individual pedagogical components on cybersecurity learning outcomes.

IV. Conclusion

The study demonstrated that the cybersecurity learning game developed using the Game Development Life Cycle (GDLC) approach successfully met functional and performance requirements with a 100% success rate in alpha and beta testing, while also engaging users through experiential learning activities that fostered decision-making and problem-solving; pedagogical strategies such

as experiential learning, flow, and adaptive scaffolding enhanced user engagement, though interviews revealed the need for clearer instructions and task objectives, leading to recommendations for improving navigation, task indicators, and interactive guides, as well as strengthening adaptive scaffolding to provide responsive support; future research is encouraged to employ more comprehensive evaluation methods, such as pre- and post-tests of user understanding, and to expand the scope of development with diverse cybersecurity threat scenarios and larger respondent groups, thereby increasing the generalizability and practical application of the findings in advancing cybersecurity education..

References

Badan Siber dan Sandi Negara. (2024). Laporan tahunan keamanan siber Indonesia 2024. BSSN.

Badan Siber dan Sandi Negara. (2025). Peningkatan ancaman siber dan modus phishing di Indonesia. https://-bssn.go.id/

de Freitas, S., Morgan, J., & Gibson, D. (2021). Will MOOCs transform learning and teaching in higher education? Engagement and learning through game-based approaches.

Gwenhure, A. K., & Rahayu, F. S. (2024). Gamification of cybersecurity awareness for non-IT professionals: A systematic literature review. International Journal of Serious Games, 11(4). https://journal.seriousgames-society.org/index.php/IJSG/article/view/719

Hamari, J., Shernoff, D. J., Rowe, E., Coller, B., Asbell-Clarke, J., & Edwards, T. (2016). Challenging games help students learn: An empirical study on engagement, flow and immersion in game-based learning. Computers in Human Behavior, 54, 170–179. https://doi.org/10.1016/j.chb.2015.07.045

Hwang, G. J., & Sung, H. Y. (2022). Effects of a contextualized game-based learning approach on students' learning achievements and motivation. Interactive Learning Environments, 30(3), 503–518. https://doi.org/10.1080/10494820.2019.1583163

Kashefi, H., Ismail, Z., & Yusof, Y. M. (2010). Obstacles in the learning of two-variable functions through mathematical thinking approach. Procedia - Social and Behavioral Sciences, 8, 173–180. https://doi.-org/10.1016/j.sbspro.2010.12.024

Marinho, M., Barbosa, L., Conte, T., & Rocha, L. (2022). Game development processes: A systematic literature review. Journal of Systems and Software, 184. https://doi.org/10.1016/j.jss.2021.111120

Melfionita, M. (2022). One-on-one validation in educational media evaluation. Educational Technology Research Journal.

Microsoft. (2024). Feeding from the trust economy: Social engineering fraud. Microsoft Threat Intelligence. https://www.microsoft.com/en-us/security/security-insider/threat-landscape/feeding-from-the-trust-economy-social-engineering-fraud

Microsoft Security. (2024). Microsoft Digital Defense Report 2024. Microsoft Security Intelligence.

Moumouh, A., El Guemmat, K., & Berrada, K. (2024). Game-based assessment: Enhancing learning outcomes through interactive evaluation. Education and Information Technologies. https://doi.org/10.-1007/s10639-023-12000-0

Moumouh, C., García-Berná, J. A., Chkouri, M. Y., & Fernández-Alemán, J. L. (2025). Serious games to improve privacy and security knowledge for professionals: A systematic literature review. International Journal of Serious Games, 12(1). https://journal.seriousgamessociety.org/index.php/IJSG/article/view/825

Ng, S., & Hasan, H. (2025). Cybersecurity serious games development: A systematic review. Computers & Security. https://doi.org/10.1016/j.cose.2024.104307

Olzhas, S. (2024). Game-based learning for cybersecurity education: A literature review. Research Result. Applied Research and Development, 10(2). https://-ojs.publisher.agency/index.php/RRAL/article/view/3174

Plass, J. L., Mayer, R. E., & Homer, B. D. (2021). Handbook of game-based learning. MIT Press. https://-doi.org/10.7551/mitpress/9427.001.0001

Radianti, J., Majchrzak, T. A., Fromm, J., & Wohlgenannt, I. (2020). A systematic review of immersive virtual reality applications for higher education: Design elements, lessons learned, and research agenda. Computers & Education, 147, 103778. https://doi.-org/10.1016/j.compedu.2019.103778

Resincen, A. (2025). Adaptive scaffolding and feedback design in serious games for learning. Education and Information Technologies. https://link.springer.com

Serious Games Society. (2025). Effectiveness of serious games for cybersecurity learning. *International Journal of Serious Games, 12*(2). https://journal.-seriousgamessociety.org

Sodikin, R. (2025). *Your Zero Hour: Visual Novel Interactive Game Berbasis Adaptive Learning sebagai Media Pembelajaran Keamanan Siber Ransomware* (Skripsi). Universitas Pendidikan Indonesia.

Sophos. (2024). *The state of ransomware in education 2024*. Sophos. https://www.sophos.com/en-us/partner-news/2024/07/resources/the-state-of-ransomware-in-education-2024

Taha, M., Dahabiyeh, L., & El Khatib, M. (2023). Cybersecurity awareness and behavior: A systematic literature review. *Computers & Security, 128*, 103134. https://doi.org/10.1016/j.cose.2023.103134

Tsani, A. (2024). Aplikasi RansomForge sebagai game edukasi untuk mengoptimalkan kesadaran keamanan siber. *Journal of Educational Game Development*.