NTNU
Norwegian University of
Science and Technology

Department of Computer Science

MACS490 - Master Thesis

Gamifying the MITRE ATT&CK for Cyber Security Training using the COFELET Framework

Author:
Lama Amro

Supervisor:
Christopher Frantz

December, 2022

Acknowledgement

I want to express my sincere thanks to my supervisor Christopher Frantz for his help and guidance from the beginning to the end of my journey with the thesis, where he never failed to offer his full attention and help whenever I needed that. I also want to thank everyone who helped me in completing this thesis, starting from Simon McCallum for supervising and helping me in the early stages of this project, and all the students and professors who participated in the evaluation. Last but not least, Ahmed Amro, who despite his busy schedule, never failed to be the cyber security expert I needed.

Abstract

Cyber-attacks are becoming more sophisticated and changing rapidly. Well-trained cyber security employees are needed to keep track of these attacks, and this begins with a well-educated and well-trained graduate. As cyber security students struggle in finding knowledge that is scattered over the internet, frameworks like MITRE ATT&CK are trying to solve this issue by collecting as much information as possible about tactics, techniques, and procedures (TTPs) of adversary groups, to make it easier for those who are interested to find the data they need in one place. Unfortunately, this huge amount of information can be overwhelming for early-career professionals and students, and not knowing how to use such frameworks challenges their ability to operate efficiently in cases of crises. This thesis proposes a serious game designed and evaluated based on a framework for cyber security serious games called COFELET, to investigate the effectiveness of using a COFELET-based serious game in introducing the ATT&CK framework, as an effective method for teaching and training, where complex knowledge is presented in an engaging and pedagogically informed way. The game was evaluated qualitatively and quantitatively, by researchers, teaching staff, and students from the Norwegian University of Science and Technology (NTNU), where the learning, instructional, and gaming components of the game were tested and evaluated, and the results were collected via questionnaires. The evaluation resulted in the conclusion that by combining field-related methodologies with educational theories in a game, students will gain a better learning experience with positive learning outcomes. It was found that beside the field-related methodologies and educational theories, light should be led on the gaming components to make the learning experience more fun and engaging.

Contents

Figures

Tables

Chapter 1

Introduction

Protecting data in cyberspace is very challenging. Cyber security is continuously trying to protect digital systems from cyber attacks, but cyber attacks are becoming increasingly sophisticated and evolving rapidly. This points to the need to educate people and train cyber security personnel to decrease the risk of cyber attacks [1]. This needs to be done not only on a general public level but most importantly, for security professionals. Katsantonis et al. [2] mentioned in their study that the cyber security workforce needs to grow by 145% to meet the market demands. This starts with a well-educated and well-trained graduate. However, cyber security education is facing some challenges in meeting this desired result. One of these challenges is not particularly related to cyber security education but higher education in general, which is that students tend to focus on tasks that are assessed, at the expense of other tasks and literature study. Starcher et al. [3] conducted an experiment, where they had ten computer security students, who were noticed to engage very well in their assessed task, but spent very limited time on their allocated weekly reading, some of them even did not do any reading, and same with their work lab. This can prevent them from taking full advantage of the knowledge presented to them. One solution for that is to find new teaching methods that increase the student's engagement and motivation for learning, in which serious games or game-based learning are constantly trying to achieve promising results [4]. Also, cyber security students have faced the challenge of filtering and prioritizing cyber security information that is scattered over the internet [5]. What has also been considered a challenge in cyber security education is the fact that cyber security needs to be reshaped to adapt to new technologies and threats. This dynamic nature requires responsive cyber security education, that produces experts with the ability to quickly establish new insights that provide the basis for a response [6].

In an attempt to solve the last mentioned points, frameworks like the ATT&CK framework from MITRE [7] are trying to solve this issue by collecting as much information as possible about tactics, techniques, and procedures (TTPs) of adversary groups, to make it easier for those who are interested to find the data they need in one place. But, as useful and important as the ATT&CK framework can be, it can be considered extremely complex for those who are new to it [8], and there should be a way to simplify it for them.

Through the past decade, serious games were receiving increasing attention and interest in many different areas [9], and education is one of them. A study performed by Zhonggen [10] showed that the number of publications in serious game-assisted education rose steadily between the years 2009 and 2018. This rising heat in the educational serious games sector affected cyber security education where studies discussed game-based learning as an effective way to be used in cyber security education [2, 11]. In order to develop a successful game that fulfills the desired goals, serious games need to be developed carefully, considering learning theories, learning outcomes, and game designs [12]. For the cyber security serious game field, it was found that it lacks common methodologies and design standards, and only one framework named COFELET was presented and tested in this matter [13].

1.1 Thesis objectives

So, for the huge knowledge, the ATT&CK framework can offer, and the effectiveness of serious games; this project proposes a novel idea that intends to introduce ATT&CK to undergraduate students in a new, more entertaining, and engaging way via a COFELET serious game in which they are encouraged to browse through the ATT&CK framework whilst training their cyber security knowledge.

1.2 Thesis target audience

Since the core topic of this thesis is a serious game to educate about a new topic, this thesis is aimed at Applied Computer Science personnel, who are familiar with or interested in educational serious games. A principal knowledge of some cyber security concepts is of benefit, but not essential.

1.3 Research questions

The literature review, and the design, implementation, and testing of the proposed serious game were conducted in an attempt to support or discard the hypothesis: **A COFELET serious game is an effective approach for introducing the MITRE ATT&CK framework to university cyber security students**. To achieve that, the following research questions (RQs) are investigated:

- RQ1 How effective is using the COFELET framework in designing a cyber security serious game? To answer this question, the effectiveness of COFELET is assessed from two perspectives.
    1. From the developer's perspective: how helpful is the framework for the development of the game?

  2. From the player perspective: How valuable are the insights derived from the game when played?

- RQ2 How effective is using serious games to introduce the MITRE ATT&CK to students?
  Answering this question depends on the evaluation of the learning, gaming, and instructional components of the game, from both the teachers' and the student's points of view.

1.4 Contribution

The main contributions of this thesis are:

1. A web based game that introduces the ATT'CK framework for undergraduates.
2. An empirical study that assesses the effectiveness of using a COFELET-based serious games to introduce the MITRE ATT&CK to students.

1.5 Outline

Chapter two provides the **Background**, in which important concepts and information are provided to understand the rest of the thesis. Followed by discussing other work that is related to the topic, either a game or a model, with a critical analysis of the state of the art of the field in chapter three the **Related work**. A detailed **Methodology** can be found in chapter four. Chapters five, six, and seven are dedicated to the **Design**, **Implementation**, and **Evaluation** of the game. The last two chapters of the thesis are the **Discussion** and **Conclusion**, in which the research questions are discussed and answered, alongside the limitations of the study and planned future work.

Chapter 2

Background

This chapter is essential for understanding the rest of the thesis, it presents an explanation of the main subjects that form the essence of the thesis, and understanding these concepts, makes it easier for the reader to follow the study.

2.1 Cyber Security

Cyber security as defined by Thakur et al. in [14] is "a measure protecting computer systems, networks, and information from disruption or unauthorized access, use, disclosure, modification or destruction". In the world we live in, almost every aspect of our lives, from individuals' data to governmental institutions is carried out in cyberspace, where adversarial malicious acts thrive, trying every possible way to control and violate this data. Cyber security is a wide and huge topic, which can be found in critical infrastructures, applications, networks, the cloud, the internet of things (IoT), and many other aspects of digital infrastructure that can be a victim of cyber attacks. Since adversarial threats affect all sides of cyberspace, it is infeasible to address them all in one project. In this thesis, it was chosen to address the attacks that are related to traditional enterprise systems, industrial control systems, and mobile systems, where different cyber security principles are applied to protect the assets of these systems. It is important for those who are responsible for protecting these systems to be prepared and ready to respond to the attacks that might jeopardize the system, so, they need to be aware of the potential threats, and analyze the threat's characteristics, to know what precautionary measurements should be applied, and to mitigate the attacks in a process called threat modeling. In a threat modeling process, the main assets of the system are identified along with the threats to these assets. This process can be used in two forms, either to assess the current state of the system or in the design phase, to design a secure system [15]. In order to do their job efficiently, and reach their goal of sustaining the system's security, security personnel needs to acquire a huge amount of information, and keep themselves up-to-date with all the possible risks. What makes this less complicated, is the availability of such information in an accessible and reachable place, something threat modeling frameworks are trying

to achieve.
Next, the MITRE ATT&CK framework will be introduced as one of the main open-source threat modeling frameworks.

2.2 MITRE ATT&CK Framework

The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is an innovative framework that provides a rich knowledge of adversarial tactics, techniques, and procedures (TTPs). It is considered a repository that has been broadly welcomed and adopted by the cybersecurity community. ATT&CK provides security vulnerabilities mapped to specific adversary behaviors and patterns and exploiting them opens possibilities for new scientific directions.[16] The reason behind the wide adoption of this framework besides that it is open-source, and its knowledge is accessible worldwide, is that it contains categorized real-life observations of adversary behavior, reflecting the various phases of an adversary's attack life-cycle and the platforms they are known to target [17]. ATT&CK offers their knowledge under different categories that answer the **Why**, **How**, and **Who** questions related to any cyber attack, some of which were used in this project. The following are the ATT&CK's categories used in this project:

- **Tactics**: Tactics are the **Why** part that indicates the progress of the attack. It shows the reason or the tactical goal behind using the attacker some techniques. Examples of tactics addressed by the ATT&CK framework and used in this project are initial access (i.e., gaining initial access to the system) and execution (i.e., running adversary-controlled code).
- **Techniques**: This part represents the **How** part of the attack, meaning, how an attacker reaches his/her tactical goal, and which actions are performed for this matter. Each tactic has different techniques that can be used to reach the goal behind it. For example, Phishing, in which adversaries send electronic messages, containing malicious attachments or links to execute malicious code on the victim's system [18], and External Remote Services, in which adversaries use remote services like VPN to control a system from outside the system [19], are different techniques that can be performed to achieve the Initial Access tactic.
- **Mitigations**: This represents the security control that can be used to prevent a technique to be performed successfully, or detect its occurrence.
- **Groups**: This is the **Who** part of the adversarial attacks. The ATT&CK framework has a huge database that contains many adversary groups with detailed information about these groups, their name, origin, tactics, and techniques used by them, and their targeted victims.
- **Campaigns**: This describes a group of intrusion activities with common targets that were performed over a specific period.

All previous points are presented in the ATT&CK framework for three different technology domains named: **Enterprise**, **Industrial Control Systems (ICS)**, and **Mobile**. ATT&CK offers a visual mapping and representation for the tactics and techniques mentioned earlier in different matrices. Each technology domain is represented in a matrix showing the tactics and techniques used in this domain. For better understanding, a snapshot of the Enterprise Matrix is shown in Appendix A. Other than the matrices, each tactic has its web page, that contains the techniques used for it, and each technique has a corresponding web page that contains potential mitigations for it. In order to introduce the ATT&CK framework entertainingly, it was decided to use serious games for that matter in this thesis, but first, we need to understand what are serious games, where they were used, and for what purpose, as will come in the next section.

2.3 Serious Games

There is no one specific definition for serious games, and many researchers have defined those in different ways. However, most definitions lead to the same meaning, that they are games designed for the main goal other than pure entertainment [20]. This means that different from designing entertainment games, in which the main goal would merely be entertaining the player; when designing a serious game, the developer should consider other objectives that have an impact on the player [9], like training, behavior change, educating, etc. For years, serious games were used in many sectors, such as Health, Education, the Military, and others. In health sectors (physical and mental), serious games were used for many purposes by everyone. for example, professionals use games to train in a virtual environment to reduce the number of medical errors, also, games were used with patients to monitor and change a behavior, and they were used by people to increase their health awareness [21]. Serious games were also used in the military as a training and education tool that allowed trainees to practice real-life scenarios virtually [22], as in the game Spearhead and America's Army [23]. As was mentioned before, serious games are receiving considerable attention in the education area. Educational serious games were found that they make learning more enjoyable, interactive, and motivational [24], and they can be effective especially if they were integrated with educational theories and methodologies. Many other cases exist where serious games were used in different settings and environments to make an impact on players, and this study is trying to have its impact on students that leaves them with more knowledge about the ATT&CK framework, with possible side results where they can practice their cyber-security knowledge.

To develop a cyber security serious game that adopts not only educational theories but also cyber security methodologies and models, it was decided to use the COFELET framework. The next section explains the COFELET framework, with the theories and the methodologies it adopts.

2.4 COFELET Framework

The Conceptual Framework for e-Learning and Training (COFELET) was made for the design and implementation of cyber security serious games. COFELET adopts modern teaching approaches and learning theories and conforms with cyber security standards and models [13]. The framework was presented by Katsantonis et al. [13], as an attempt to create common methodologies and standards for cybersecurity game-based learning approaches. COFELET complies with the activity theory-based model for serious games (ATMSG), which is a framework that complies with and adopts the activity theory in education and is made to understand the structure of serious games components, and the relation between the gaming elements with the learning goals of the game, where those who play the game or use the game to teach something are considered a part of a complex, interactive system with the game. Activity theory is a social constructivism learning theory, that considers educational games as dynamic, interactive systems that are analyzed under different perspectives like gaming, learning, and instructional [25]. COFELET uses both, modern educational methodologies that comply with modern learning theories, and traditional teaching methodologies and training paradigms. This is done by combining realistic environments to give the players the ability to improve their critical thinking, problem-solving and analytical skills, while they need to recall concepts, use tools, and practice on tasks as in traditional methods.

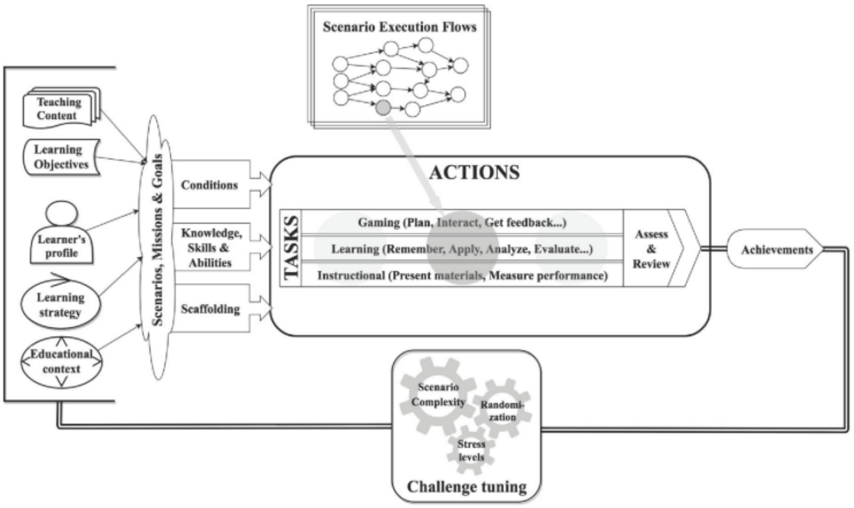


Figure 2.1: The COFELET Framework
[13]

As shown in Figure 2.1, this framework's ontology has four key elements:**Tasks, Conditions, Goals, and Scenario Execution Flows (SEF)** [2]. Tasks represent actions directed to reach the game goal, while conditions are prerequisites needed to perform the task, and SEF is the sequence in which tasks are performed, and it is presented in an analogy of an attack pattern. An extension ontology for COFELET presented additional elements, to analyze the elements that facilitate the learning and instructional aspects. These elements are **Learning objective (LO), Grade scheme, and Roles**. As in ATMSG, serious game activities are divided into three main activities, Gaming activity, Learning activity, and instructional activity, and each component in the game can serve all three activities. Other than educational theories, COFELET utilizes methodologies, models, and strategies that are used in well-known threat modeling and analyzing approaches which are: Mitre's CAPEC [26], Lockheed Martin's Cyber Kill Chain (CKC) [27] and National Cybersecurity Workforce Framework (NCWF) [28]. Below is an explanation of the cyber security models and methodologies of COFELET.

- **Lockheed Martin's Cyber Kill Chain (CKC)**: There is a type of cyber threat actors of groups called **advanced persistent threat (APT)**, where adversaries need to have deep knowledge of the system before starting the attack, and it requires sophisticated and long-term actions [13]. CKC explains the phases and steps adversaries follow from the beginning of the attack until the attack is performed successfully.

- **MITRE's CAPEC (Common Attack Pattern Enumeration and Classification)**: Although this exact model was not used in this project, the MITRE ATT&CK was used and there are a lot of similarities between them. Both CAPEC and ATT&CK are frameworks provided by MITRE, that offer classification taxonomy of attack patterns (APs), but CAPEC focuses on the application security level, whilst ATT&CK focuses on the network security level and explains the adversary's life cycle, which is the main focus of this thesis.

- **National Cyber Security Workforce Framework (NCWF)** This framework provides a common definition for the different cyber security workforce roles depending on their tasks, knowledge, skills, and abilities (KSAs). NCWF helps educators to connect between education programs and the production of the workforce.

In addition to educational theories and cyber security concepts and models, COFELET uses a methodology used in serious game design and implementation, which is, **Adaptation**. Adaptation in education as defined by Darrow in [29] is "any adjustment in the environment, instruction, or in materials for learning that enhances the students' performance". This is a very important feature in educational games, for its role in increasing the effectiveness of the teaching process, by adjusting and adapting the game's challenges to the learners' knowledge, goals and needs [30].

Chapter 3

Related Work

Carvalho et al. [31] proposed the ATMSG to help game designers to assess their game design in the prototyping stages, to evaluate if the game structure will fulfill the pedagogical desired outcome or not. This model divided the serious games activities into three main activities, Gaming activity, Learning activity, and Instructional activity, and focused on the importance of the explicit distinction between the learning and the instructional activity. Where the learning activity is compatible with the learner's point of view, and the instructional activity illustrates the instructor's side. By that, the instructional components can be evaluated to know whether they support the desired learning outcomes or not. In this paper, Carvalho et al. proposed some steps to help apply ATMSG when analyzing and designing serious games, both steps are much in common with small differences:

- Describe the activities: In which more understanding is offered for the game activities by highlighting the main related aspects.
- Represent the game sequence: In which, unlike the analysis process, this phase should be done in conjunction with the prototyping techniques, which are at a higher level than low fidelity prototyping.
- Identify actions, tools, and goals, and Description of the implementation: Here, the designers identify components related to each node of the game sequence and a more complete description of their implementation.

This model was made to help with serious games design and analysis and was found to be highly helpful and efficient because it provides a detailed way to investigate the structure of the serious games at early stages, also, the decomposition of the game's components offers an explicit analysis model, and was adopted in many cases to meet specific objectives. One of those is the COFELET framework which this project depends on for designing the game, not to mention evaluating it. But the limitation of this paper is that it is an abstract model, an example application of the model on a game, in designing and evaluation could be very useful in understanding how to use it, as in the study conducted by Katsantonis et al. [2] that will be mentioned later.

In a study on different types of games, Hart et al. [32] explored Risiko, a cyber security serious game that, in contrast to many investigated games, was created as a board and card game, rather than a video game. The game helps the players to think both like attackers and defenders and contains a wide range of cyber security attacks and related countermeasures from industrial and government cyber security standards. The design of Risiko uses fundamental ideas from constructivism learning theory and game design to encourage engaging, active learning. Risiko designers target two different audiences, employees without any technical background as the primary audience, and cyber-security university students who want to practice what they have been taught in the university as the secondary audience. They designed their study based on the Technology Acceptance Model (TAM) which divides the perception of the technology by users into three constructs: **perceived ease of use (PEOU)**, **perceived usefulness (PU)** and **intention to use (ITU)**. These constructs were assessed by both audiences. They took into consideration that the primary audience is a non-technical audience, so they designed the attacks to be accessible and easy to understand. Constructivism learning theory was the only sound theory used in designing the game, no cyber security theories or models were used to design the attacks and mitigations for the game, instead; they relied on cyber security reports, and practices. Although the game encourages critical thinking and decision-making, the fixed information that is available in the game through the cards form makes it hard to adapt to newly available attacks, mitigations, and security measurements which, in turn, are changing rapidly and continuously. But, using industrial and government cyber security standards helps with connecting education with these standards, which in turn increases the adaptability of the game.

Yamin et al. [33] developed a multi-layer system, that contains a Strategy game, and domain-specific language (DSL) for cyber-security exercise scenario modeling in a cyber-security exercise environment. Their system was made in an attempt to create an efficient way to conduct cyber-security exercises with unique scenarios for each exercise, to increase the participants' skills in decision-making, which is a skill they noticed that the teams involved in the European cyber-security challenge were lagging. In this multiplayer game, players can play in multiple roles besides the traditional defenders (i.e Blue-team), and attackers (i.e. Red-team), the game offered a White-team option, where members create a complete network with interconnected components and a Green-team that monitors the team's performance in live-action representations of Red and Blue teams. Different cyber-security methodologies and theories were considered in the game design, like the Penetration testing methodology and Cyber kill chain. For the game evaluation, they conducted a case study in the context of the Norwegian Cyber Security Challenge (NCSC), to evaluate both the developed game and the scenario language toolset, and they collected the data for the study through **Post-game survey**, **Game recordings** to record the participant gameplay, and **Post-game interview**. This game was implemented to enhance critical thinking and decision-making in a real-time environment, where also the dynamic nature of the scenario modeling is an advantage in favor of the game's adaptability since the game observes the gameplay session and creates a unique scenario based on it. Also, the multiple roles that were considered in the game, were adapted to the players' preferences. But, counter to Risiko, the players need to have high technical skills in order to play the game, which results in a limited audience that can benefit from the game.

Katsantonis et al. [2] introduced an extended version of the COFELET framework ontology that was presented by Katsantonis and Mavridis [34], where they noticed that the first ontology only provided an analytical description for the key elements of the COFELET game, which are Goals, Conditions, Tasks and SEFs and Knowledge, Skills and Abilities (KSAs), with less focus on the elements that facilitate the learning and instructional aspects. For that reason, they extended the ontology to include Learning objectives (LO), Grade schemes, and Roles.

They also introduced HackLearn, a cyber-security serious game that lies under the hacking simulation game genre and is used for teaching cyber-security concepts with a hands-on hacking experience for players. HackLearn is a scenario-based game with a Unix-like terminal where players type and execute text-based commands to emulate real-life tools. HackLearn developers used the COFELET framework to support different aspects of the game, like the learning and instructional aspects by using modern learning theories, such as the activity theory in ATMSG, and also the cyber-security aspect by modeling strategies and cyber-attacks. Different cyber security models and standards were incorporated into the game such as CAPEC from MITRE and CKC. ATMSG was used for evaluating the game as well. According to their activity, the developers divided the game's components into three main categories **learning activities**, **instructional activities**, and **gaming activities**. The game's evaluation revealed a few limitations related to the lack of multiple players and multiple modes in the game, as the game presented a single-player game with only a hacking simulation mode. This study is the most related to this thesis, where the same design and evaluation framework is used in both. The game part of the game was found to be highly helpful in understanding how to apply the COFELET framework in both the design and the evaluation. But, the textual form of the game, where the players need to insert text commands may intimidate some players with less programming skills.

In a different area of security, Jordan et al. [5] presented Countermeasures, a game that teaches computer security to people with general technical backgrounds but not necessarily computer security experience. The game they presented teaches techniques that are used by security experts. The purpose of their study was to test the following hypothesis:

1. Simulation that emulates a real-world system is better for training than reading.
2. Learning practical knowledge via a game is more engaging than learning from a book.

The game provides a real interactive shell and an environment resembling currently deployed security systems, allowing them to exploit a real server. Countermeasures were designed as a single-player game, with a client-server architecture, where the player is guided through several missions through a command-line interface, with a form of a score that is increased with each successful mission. Countermeasures provides a cyber security sandbox environment by blacklisting some of the commands that may cause damage to the test environment if used by the players. The game used a summative assessment by providing help and hint options, but with a price that is deducted from the score. The game-play was divided into two types of missions, Training and Live missions. Training mission focuses on one specific security aspect, whereas live missions are more complicated and combine several security aspects. Having two sets of missions where one is simpler than the other adapts to the different skills of the players, where they can train in the training missions, and build their skills up to the live missions. Evaluating the game showed that the amount of taught knowledge in both the game and reading was the same, but with the game, it took half the time, also, the participants found the game more engaging and entertaining, and those who participated in the experiment were the only ones who sought additional computer security learning. But the limitation noticed in this study is that the game design did not utilize any educational theories, instead, they used specific theoretical knowledge from books and turned it into scenarios. also, same as HackLearn, the textual commands may intimidate players with less programming skills.

It was noticed while reading the literature that there are numerous educational theories available that can elevate the teaching process, but the field of educational cyber-security games lacks standardized models that integrate both educational and cyber-security models and theories. In this case, only one framework (COFELET) was found. Additionally, it was noticed that cyber-security games tend to ignore the requirement to impart fresh knowledge that can energize students' minds in favor of reinforcing the knowledge they already possess.

Compared to the previous work, our approach is the first to consider the whole and complex MITRE ATT&CK framework in one serious game directed toward university students. The game for this project is designed using the COFELET framework as in the work of Katsantonis et al. [2]. It allows the players to practice their knowledge and skills in cyber-security, through several scenarios as in what Yamin et al. [33], and Jordan et al. [5] have done. Both attacker, as well as defender roles, can be trained by having the possibility to play either role as in the work of Hart et al. [32]. For the game to serve its purpose as a serious game, ATMSG is used to design the game mechanics " nature of the tasks, scoring, assessment ...etc ". The game overcomes the limitation found in Risiko, by offering information provided by the MITRE ATT&CK, and not providing fixed data on cards, and the limitation found in Yamin's study, by making the game playable by anyone, regardless of the knowledge level they have. Unlike HackLearn and Countermeasures, the game is simple and easy, no textual commands are asked. But the lack of different roles and play modes in HackLearn was an inspiration for this thesis, to try to overcome these challenges by offering different roles with different scenarios.

Chapter 4

Methodology

To offer solutions for the challenges mentioned in chapter 1, this project is aiming to introduce MITRE ATT&CK framework for cyber security students in a serious game setting. An empirical research methodology is conducted, and the project work is divided into three main phases to either support or discard the hypothesis: **A COFELET serious game is an effective approach for introducing the MITRE ATT&CK framework to university cyber security students**.
The main three phases for the project are **Investigation, Implementation, and Evaluation**, and by the end of the last phase, the research questions mentioned in Section 1.3 should be answered.

4.1 Investigation

- **Literature review**: This phase is done by searching through libraries and scientific databases for articles and papers to gain more knowledge about the serious games in the cyber-security field, as well as theories and design patterns for such games.
  The literature review also includes searching for resources containing learning theories and methods used in educational serious games in general, and serious games for cyber security in particular.
  Academic databases searched included Science Direct, Google Scholar, and Scopus, with keywords cyber security, Serious games, education, training, and Game Design patterns to create the following queries:

  1. ((cyber OR information) AND security) AND serious game AND(education OR training).
  2. cyber security AND education AND serious games.
  3. Cyber security AND serious games AND design.

  The inclusion criteria were related articles and papers published in English.
- **Game investigation**: To have a clear idea about the state of the art in serious games in cyber security, research is conducted for existing serious games,

and the games are investigated analytically to extract the main game mechanics used and the learning theories applied. This research was done on a literature level (papers about games) and actual gameplay. The literature game investigation was conducted using the same libraries and scientific databases. Few games were found to be related to cyber security as indicated by Hart et al. [32], and Yamin et al. [33], other games were found to be related to other aspects of security as proposed by Jordan et al. [5] which was about computer security, and by Thompson & Irvine in [35] which was for network security. In the game-playing phase, the focus was highlighted on the gaming aspects more than the educational and pedagogical, where the author played multiple games in an attempt to observe and collect ideas for the game design, in terms of game genre, number of players, scoring, and other game mechanics. This phase was challenging due to the lack of available access to such games. At first, the author attempted to find the games found in the literature, which turned out to be challenging. A Google search was conducted to find other cyber security serious games using the query "cyber security serious game portal", one website found to be very helpful that contained multiple accessible games [1] and the following were played:

- Targeted Attack: The Game by Fugle Inc. (Desktop game)
- Cybersecurity Lab (Desktop game)
- Keep Tradition Secure (Desktop game)
- Cyber Awareness Challenge. (Desktop game)
- Defend the Crown (Mobile game)

4.2 Implementation

After collecting literature that is sufficient to allow the author to develop the game with the needed outcome, the rationale behind the implementation methodology and chosen design pattern are discussed hereafter:

- Implementation Platform: In which platform the game should be implemented, and what programming languages are used? Can be web-based, or a game engine.
  The following factors were considered for this decision:
  - The game distribution for the testing.
  - Ease of improving and changing in the implementation.
  - Feasibility for the author to learn a new programming language if needed.

  To facilitate game distribution for the user evaluation, as well as the capabilities of the developer, the decision was made to build a web-based serious game, using the Django framework building on Python as the programming language [36].

[1] https://www.helpsystems.com/blog/8-online-cybersecurity-games-that-test-your-cyber-skills

- Design Patterns: From the literature, a design pattern/framework should be adopted for the game design to produce a game that fulfills the intended learning goals and good user experience (UX) .
  For this purpose, the COFELET framework was used for designing the game, since it was made for cyber-security serious games, and it embraces modern learning theories and innovative teaching approaches, combined with cybersecurity models and methodologies in one framework. [13] Then, its suitability as a design pattern is investigated in this thesis.

4.3 Evaluation

Two evaluation methods were employed, qualitative and quantitative evaluation:

- Expert evaluation: Researchers and teaching staff from the Norwegian University of Science and Technology (NTNU) who are involved in relevant teaching activities were contacted to test the game and provide their feedback. This feedback was considered for the qualitative evaluation, specifically as professional feedback for the effectiveness of the game in delivering the desired learning material if conducted as a secondary learning activity. The feedback was collected through a post-game questionnaire containing statements about the game's pedagogical aspects, learning outcomes, assessment criteria, and the gaming aspects like the fun factor and the user interface. The participants should choose whether they agree with the statement or disagree, they were offered 5 choices "Highly disagree, Disagree, Neutral, Agree, and Highly agree". There were some optional open-ended questions, to give the participants the chance to elaborate on their opinions.
- Student evaluation: This process was done for the quantitative evaluation, to test the effectiveness of the game in increasing the student's knowledge about the ATT&CK framework and how to use it. This process was done in three phases, a pre-game questionnaire, a gameplay session, and a post-game questionnaire. The pre-game questionnaire collected information about the level of knowledge students already have about the ATT&CK framework. A game session was conducted after the pre-game questionnaire, so the students try the game. The session took place in a lab setting, and incentives were offered to ensure as many participants as possible are participating in the experiment. After the game session, the students were given a post-game questionnaire that focuses on different serious game elements. The questions in the questionnaire were divided into three categories representing the three different serious games activities, Learning, Gaming, and Instructional activities, as mentioned in 2.4.

Chapter 5

Design

For this game, the name ATT&CK To Defend was chosen. ATT&CK To Defend can be put in the (Operational) game genre, where players need to make decisions to answer specific questions related to tactics, techniques, and mitigations. The game allows the player to play as a defender but in two different mindsets. A defender from a defender's perspective (Blue-team), and a defender that thinks as an attacker (Red-team). the player will go through different scenarios for each role. Scenarios are designed as a group of multiple-choice questions, each question represents a step of an attack that in the end represents a Cyber Kill Chain (CKC) scenario. Scenarios were taken from different domains in the ATT&CK framework. COFELET framework was used to build the game Sequence for the game ATT&CK To Defend. Influenced by the game sequence that was presented in [13]. Figure 5.1 shows the game sequence implemented for the project.

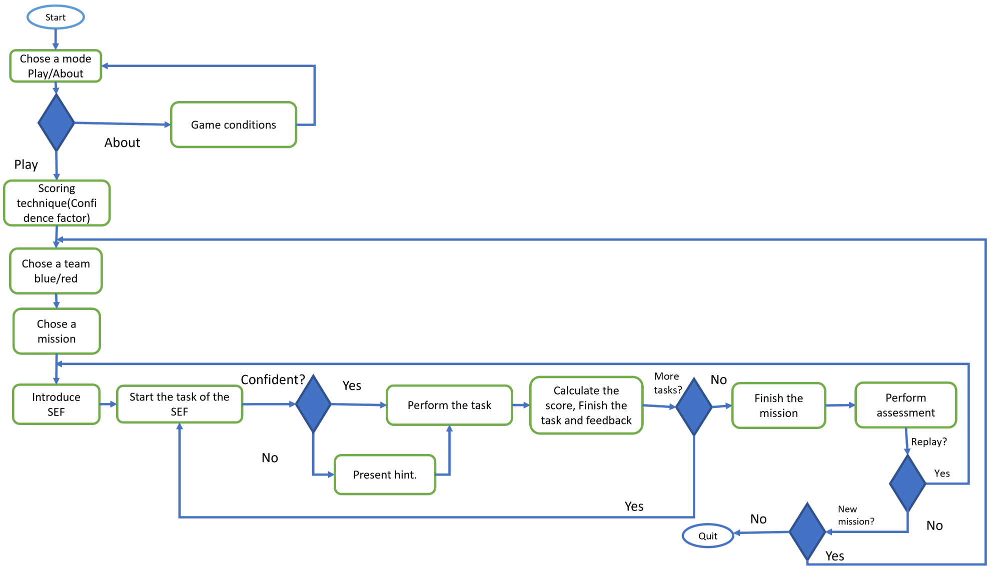


Figure 5.1: ATT&CK To Defend game sequence

5.1 COFELET Usage

This section is dedicated to explaining how the COFELET framework was used in many stages of the game's design and implementation, including the framework's key elements, models, and methodologies used in education and cyber security.

5.1.1 Usage of key elements

As mentioned in 2.4, COFELET has four key elements which were used to design the game:

- **Conditions**: When the game was designed, two different types of conditions were taken into consideration, Pre-game conditions and In-game conditions.
    - **Pre-game conditions** are what the players need to be able to play the game: Internet connection, a device to play the game on "Laptop, phone, etc." and some prior knowledge about cyber security.
    - **In-game condition** where the player needs to inform the game about how confident he/she is in the answer. This confidence factor affects the score. Also, the player needs to answer all tasks' questions in the mission to be able to finish it.
- **Goals**: To be able to understand the game goals, a tutorial section was added to the design to explain these to the player. Understanding the scoring technique is crucial to understand how to play the game, and to make sure that the players read it, a quick tutorial was added to the game-play section before starting to play, and not to the game tutorial section, since, from the previous experience, it was noticed that the players tend to skip the tutorial, and jump immediately to playing.
- **Scenario Execution Flow**: The flow of the scenarios were designed to start with the main characters introducing themselves, their jobs, and what they need. This was made to add a story feature to the game. Then the player chooses which mission to play, finally, the game starts with tasks that gradually increase in difficulty and several choices for answers.
- **Tasks**: In this game, each task was designed to handle either a specific attack that an adversary group is usually performing and their mitigations, or, tactics performed in malware or a campaign and their techniques. The player needs to complete all of the tasks in one mission at least, to finish the game. Feedback is given to the player after each task, with a help option, to emphasize the learning objectives. The tasks were designed to have more than one correct/incorrect answer.

  At the end of each mission, feedback is given to the player, about the score and how many questions were answered correctly. Also, the player will be given a **replay**, **New mission**, and **Quit** options, to choose how he/she wants to move forward.

5.1.2 COFELET Educational models and methodologies

ATMSG

As mentioned in 2.4, COFELET adopted the ATMSG model, which adopts the activity theory. Carvalho et al. [31] defined the activity theory as the interaction between a subject and object in a process. In this project, the players were considered the subjects, that interact with the object (the game), to learn about MITRE ATT&CK by solving a group of tasks. The activity can be divided into smaller units called Actions moving toward a specific goal, in this case, the activity of playing was divided into two types of missions, Blue-team, and Red-team actions. Further division for these actions can be done to produce lower-level units called Operations, which are performed under some conditions [13].

Figure 5.2 shows the division of Activities, Actions, and Operations in the game.

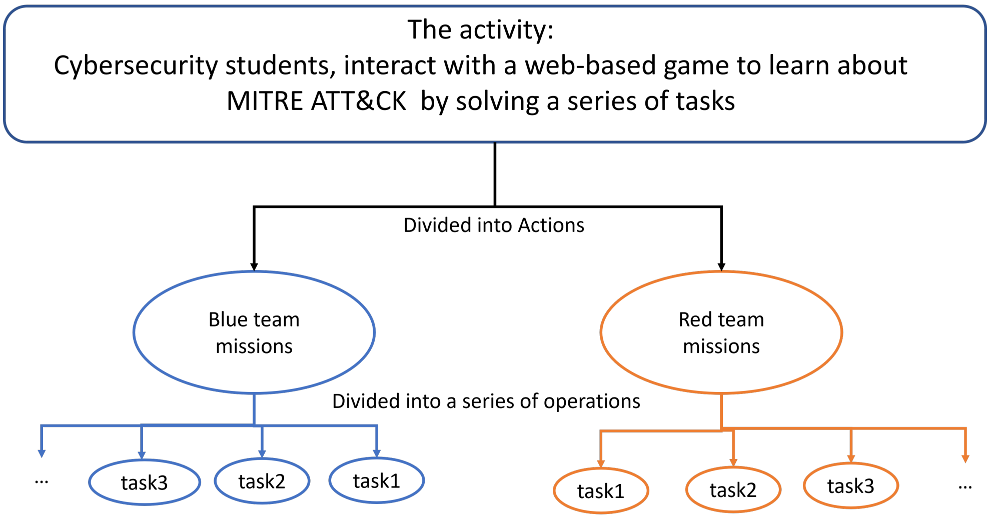

The activity:
Cybersecurity students, interact with a web-based game to learn about MITRE ATT&CK by solving a series of tasks
Divided into Actions
Blue team missions
Red team missions
Divided into a series of operations
...
task3
task2
task1
task1
task2
task3
...

Figure 5.2: Activity theory decomposition

ATMSG was also used to classify the game's components that need to be considered in the game design into gaming, learning, and instructional.

Game's Adaptation

Game adaptation as mentioned in 2.4 is a very important methodology to be applied in serious games to increase the game's effectiveness as an educational game. In ATT&CK To Defend, adaptation was considered in three features:

- Scoring Technique:
  Since this game wasn't designed to assess the knowledge of the players but

to introduce a new topic to them, a **formative assessment** was applied to calculate the score. Dixson et al. [37] (a reference to Wiggins [38]) defined the formative assessment as "An assessment used primarily to educate and improve student performance, not merely to audit it". The scoring scheme was inspired by [39], where the author used an extra factor that affects the player's decision and score which is the confidence factor. This was implemented in a form of a question about how confident the player is with their answer, and this needs to be answered before solving the task. By using this method, it is confirmed to the players that they can seek help before answering without any cost, so it is guaranteed that they gained the required knowledge. The scoring technique considered the different levels of knowledge the players may have, it gave those with good knowledge the privilege of having two points as an award for answering without help. At the same time, it gave those with a lower level of knowledge the option to get help and get one point as a reward, without worrying to lose any points for incorrect answers.

- Different roles
  It was thought that using different roles as Blue-team and Red-team, would adapt to players' preferences. Some may find themselves preferring thinking as a defender and thinking of mitigations, others may have other preferences, seeing themselves better in thinking of techniques and applying attacks. This gives them the chance to choose what they find more suitable for them, or they can try both to discover their preferences.

- Different scenarios:
  Adaptation in the scenarios of ATT&CK To Defend was applied by considering the different technology application domains in the ATT&CK framework into them. The ATT&CK framework includes adversarial behaviors from several application domains, enterprise, mobile, and Industrial Control Systems (ICS). Consequently, the approach here can be adapted to introduce the subjects to such features in ATT&CK. In this regard, scenarios from different application domains, enterprise, ICS, and mobile were integrated respectively. Integrating campaigns as well into the game demonstrates its adaptability to new cyber security concepts introduced by MITRE since Campaigns were the newest and most recent feature added to the ATT&CK framework at the time of writing this thesis.

5.1.3 COFELET Cyber Security models and methodologies

Lockheed Martin's Cyber Kill Chain (CKC)

In ATT&CK To Defend, the missions were based on CKC, tasks start from the first phase of a specific attack of an adversary group, Malware, or a Campaign, which was taken from ATTCK, and each task after represents the next phase of the attack in the same sequence of the attack phases. This will be explained further in the Implementation chapter.

MITRE ATT&CK Framework

The whole idea of the project revolves around the ATT&CK framework, other than introducing it through the game, ATT&CK was the main source of information for building the Scenario Execution Flows (SEFs), correct answers for tasks, and hints.

5.2 Scenarios' Design Process

ATT&CK To Defend was designed to have two playing roles, with multiple scenarios for each role. The design process went through a series of phases as shown in figure 5.3:

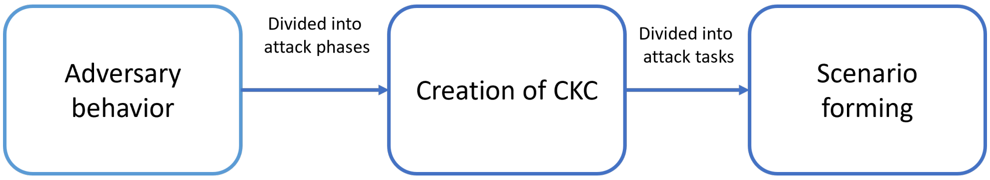


Figure 5.3: Scenarios' Design Process

- **Blue-team Scenarios**:
  The Blue-team scenarios were designed based on documented real-world adversary groups. Scenarios were designed taking into consideration a known behavior of the groups, with techniques they use to achieve an objective (i.e. tactic). To form a scenario, the sequence of tasks was designed to form a CKC. The questions for each task in these scenarios are asking about a specific technique that is used by the group for performing a tactic. The answers' options are mitigations that can be used to stop the attacks.
- **Red-team Scenarios**
  For the Red-team, scenarios were designed in a way that increases the adaptability of the game. One scenario is taken from the **Mobile** domain, and the other is taken from the newly added feature in the ATT&CK framework, the **Campaign**. Same as the Blue-team scenarios, the tasks' sequence of the Red-team scenarios form a CKC. But, instead of asking about mitigations for techniques, questions are asking about techniques to achieve an attacker's objective (i.e tactic).

Chapter 6

Implementation

This chapter will discuss the choice of tools, and the implementation process of the previous chapter, that resulted in a web-based serious game.

6.1 Choice of tools

- **Web-based game**:
  The final decision to implement a web-based game was based on both technical and personal preferences.
  - **Personal reasons**: Due to the author's desire to develop better web development skills as a full stack developer, and to improve familiarity with python as a programming language.
  - **Technical reasons**: Developing a web-based game instead of using a game engine was due to 1- The nature of the game. The game is simple and doesn't need the usage of heavy gaming engines. 2- Ease of game publishing: According to [40], it is very easy to publish a web-based game to reach more users, only a device and an internet connection are needed, without the need for additional plug-ins, which makes it perfect for mobile and web-browsers. Also, since it was planned to test the game in an open experimental setting,—i.e., a lab session, or lecture in a classroom, web-based games are easier and more flexible to be used.
- **Django**:
  For web development, many effective and powerful frameworks exist, Django was chosen due to the following points:
  - **Popularity**: Django is the most popular Python-based framework, according to the 2020 JetBrains Developer's Survey, and second most popular according to the 2021 JetBrains Developer's Survey [41].
  - **Independent of external libraries**: According to [42], Django has many benefits, first of all, being independent of external libraries and

  packages or as it is called, batteries-included framework, which means that for many functionalities, instead of writing code from scratch, a library can be imported.
  - **Python**: Django is using Python, which is considered to be one of the easiest programming languages to learn according to [43].
  - **Flexibility**: The most important feature of Django is Flexibility, especially for this project, because it has different roles and different scenarios for each role, it was easy to just add new functionalities and features without the need to repeat the whole process every time.

- COFELET
  COFELET was chosen to design and implement the game because it is a framework that is specializing in serious games for cyber security. As mentioned in 2.4, COFELET adopts the activity theory in education and uses modern educational methodologies that comply with modern learning theories, and traditional teaching methodologies and training paradigms. Using such a framework helps with increasing the learning outcomes of the game. From a designing perspective, dividing the framework into its key elements, gave the impression that it is easy to draw the flowchart of the game flow, and design the game.

6.2 1st version of ATT&CK To Defend

Working on this project was done over two periods of time, the first version of the game was implemented as a course work in a previous semester, containing only one character "Alti", and one Blue-team scenario, the **APT3**. The scenario was the same as presented in this version of the game.

Figure 6.1 shows the game sequence for the first implemented version of the game.

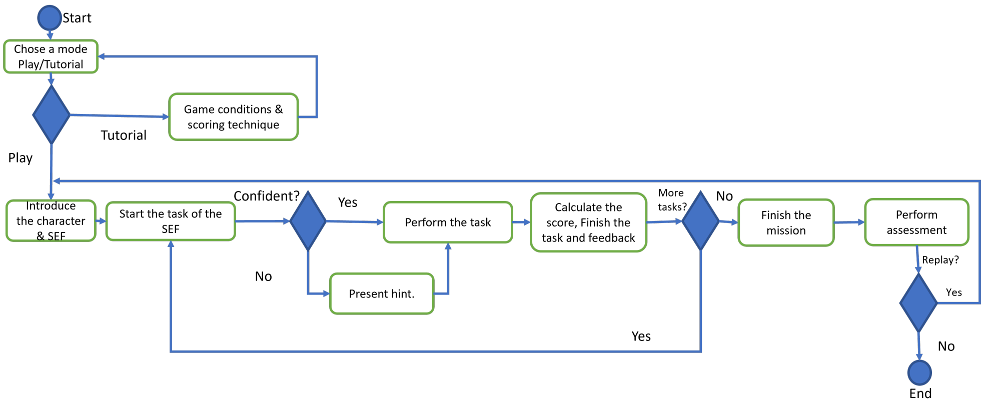

Start
Chose a mode Play/Tutorial
Tutorial
Game conditions & scoring technique
Play
Introduce the character & SEF
Start the task of the SEF
Confident?
Yes
No
Perform the task
Present hint.
Calculate the score, Finish the task and feedback
More tasks?
No
Yes
Finish the mission
Perform assessment
Replay?
Yes
No
End

Figure 6.1: Previous game sequence

The game was evaluated qualitatively by two professors from NTNU, who

played the game and answered a Post-game questionnaire.
The evaluation showed some limitations that were considered in implementing the full version of this thesis. These limitations were:

- The user interface was not friendly, the images and the text were out of scale, and the interface was confusing for having too many images and text. This was solved in the new version, by making sure that the content fits the screen, The questions were labeled and numbered, so the user knows where to start.
- The players were confused about the confidence factor, which was concluded that they did not read the tutorial. This was fixed by putting the scoring technique and the confidence factor explanation as a part and at the beginning of the game-play, so the players read it before start playing.

It was planned to continue working to develop the full version of the game containing the Red-team role, and more scenarios for each role, as will be explained in the next sections.

6.3 Scenarios' Implementation Process

Implementing the scenarios went through a series of sequential steps. Figure 6.2 shows the Blue-Team Scenario Implementation Process:

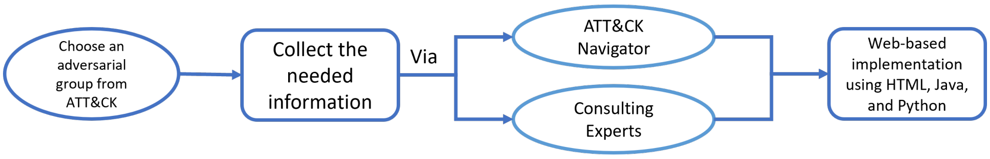

Choose an adversarial group from ATT&CK
Collect the needed information
Via
ATT&CK Navigator
Consulting Experts
Web-based implementation using HTML, Java, and Python

Figure 6.2: Blue-Team Scenario Implementation Process

- Choosing an adversary group from ATT&CK:
  The ATT&CK framework has a huge amount of information about many adversary groups, there were no specific criteria for choosing the groups other than trying to build the scenarios from different technology application domains in the ATT&CK. The choice fell on a Chinese group called **APT3** [44] and a Russian team called **Sandworm** [45].
  The same process was held for the Red-team scenarios, but instead of choosing a group from the ATT&CK framework, malware and a campaign were chosen. Followed criteria for choosing were to choose scenarios for different technology domains in ATT&CK. The choice fell on **Stealth Mango**, a malware targeted Android mobile systems [46], and **FunnyDream**, a campaign that targeted government and foreign organizations in Malaysia [47].
- Collecting the needed information:
  Information were collected from the following sources:

  1. ATT&CK navigator: To create a visual mapping for each group's tactics,

techniques, and mitigations, ATT&CK navigator was used, which is a tool offered by ATT&CK to present this information in a form of a matrix, to make it easier for people to collect data. Appendix B shows the matrix of APT3 after using the navigator, the techniques marked in blue are the techniques used by the group to perform a tactic, some of the used techniques are not shown here because they are sub-techniques that are shown when expanding the matrix.

2. Expert: As mentioned in 5.2, an expert was consulted to collect information about wrong mitigations, cause this type of information does not exist in the ATT&CK framework, and it is out of the author's scope to acquire this knowledge. In addition to the wrong mitigation, the expert also provided justifications explaining why these mitigations are wrong. Last, the expert provided information regarding the sequence of the attack phases that are known to be done by the group.

For the Red-team scenarios, mitigations were not considered, the collected data was tactics and the techniques used to perform each tactic. Information provided by the expert for this stage were, wrong techniques to be used for the tactics, and justifications explaining why they are wrong, in addition to the correct sequence of the tactics.

After collecting the needed information, the data was structured into a table, mapping the attacks' sequential steps, with their techniques, correct, and incorrect mitigations. Tables 6.1 and 6.2 are the ones created for the Blue-team scenarios, and tables 6.3 and 6.4 are the ones created for the Red-team scenarios

Table 6.1: Blue-team Scenario 1: APT3 Scenario's tasks and mitigations

Attack	Correct mitigation/s	Wrong mitigation/s
Account Discovery	- Operating System Configuration	- User training
Privilege Escalation	- Auditing - User Account Management	- Limit Hardware Installation
Credential Dumping	- Encrypt Sensitive Information - Force password policies	- Network Intrusion Prevention - Data Backup
Account Manipulation	- Domain administrator accounts management - Multi-factor Authentication	- Data Loss Prevention - Boot Integrity
Exfiltration	- Data Loss Prevention - Network Intrusion Prevention	- Execution Prevention - Encrypt Sensitive Information
Lateral Movement	- Filter Network Traffic - Limit Access to Resources Over Network	- Data Loss Prevention - Data backup
Malicious Link	- Restrict Web-Based Content - User training	- Boot Integrity - Update Software

Table 6.2: Blue-team Scenario 2: Sandworm Scenario's tasks and mitigations

Attack	Correct mitigation/s	Wrong mitigation/s
External Remote Services	- Network Segmentation	- Safety Instrumented Systems
Scripting	- Application Isolation and Sandboxing - Execution Prevention	- Static Network Configuration
External Remote Services	- Limit Access to Resource Over Network - Disable or Remote Feature or Program	- User training -Watchdog Timers
Masquerading	- Restrict File and Directory Permissions - Code Signing	- Minimize Wireless Signal Propagation - Mechanical Protection Layers
Connection Proxy	- Filter Network Traffic - Network Allowlists	- Data Backup - Limit Hardware Installation
Device Restart/Shutdown	- Communication Authenticity - Authorization Enforcement	- Data Loss Prevention - User Training
Unauthorized Command Message	- Software Process and Device Authentication - Network Segmentation	- Restrict Web-Based Content - SSL/TLS Inspection
Valid Accounts	- Application Developer Guidance - Access Management	- Redundancy of Service - Safety Instrumented Systems

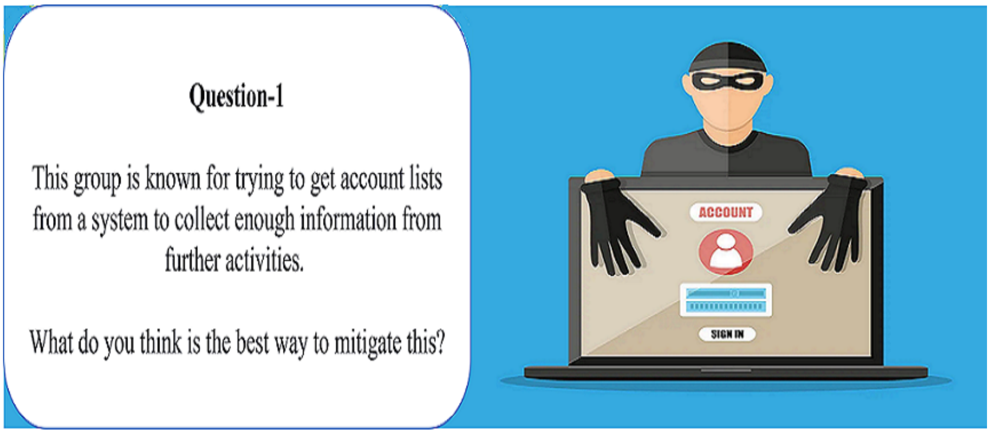
Table 6.3: Red-team Scenario 1: Stealth Mango Scenario's tactics and techniques

Tactics	Correct technique/s	Wrong technique/s
Initial Access	- Replication Through Removable Media - Drive-By Compromise	- Process Injection
Discovery	- System Network Configuration Discovery - Software Discovery	- Data Manipulation - Input Injection
Collection	- Location Tracking - Audio Capture	- Replication Through Removable Media - Boot or Logon Initializing Scripts
Command and Control (C2 or C&C)	- Encrypted Channel - Out of Band Data	-Lockscreen Bypass -Credentials from Password Store
Impact	- Network Denial of Service - Account Access Removal	- Scheduled Task/Job -Process Discovery

Table 6.4: Red-team Scenario 2: FunnyDream Scenario's tactics and techniques

Tactics	Correct technique/s	Wrong technique/s
Resource Development	- Compromise Accounts: Email Accounts - Develop Capabilities: Malware	- Command and Scripting Interpreter - Adversary in the Middle
Execution	- Command and Scripting Interpreter: Windows Command Shell - Windows Management Instrumentation	- Lateral Tool Transfer -Disk Wipe
Discovery	- System Network Connections Discovery - Process Discovery	- Compromise Infrastructure: Botnet - Loss of View
Collection	- Archive Collected Data: Archive via Utility - Input Capture: Keylogging	- Activate Firmware Update Mode - Drive-by Compromise
Command and Control	- Ingress Tool Transfer - Encrypted Channel	- Scheduled Task/Job - Process Discovery

- To add a better visual representation for the tasks, a search was conducted for images that can be representative of the techniques used in each task. Figure 6.3 shows an image added to the task asking about how to mitigate stealing accounts from a system.



Question-1

This group is known for trying to get account lists from a system to collect enough information from further activities.

What do you think is the best way to mitigate this?

Figure 6.3: Task's related image

- Web-Implementation: At this stage, the implementation starts by coding the web pages using **HTML** and **Java**. Rendering the pages, collecting and calculating the scores, and moving from one page to another were coded using Python. **Visual Studio Code** was used as the code editor of the project.

Through the previous process, COFELET's models and methodologies were applied in the implementation as follows:

- Using the ATMSG to label the interaction elements in the game. Who are the players (the students), why they are playing,(to learn about the ATT&CK framework), and how (through solving a group of tasks that leads to finishing the mission). Also, ATMSG was used in classifying the game's components to make sure that the game includes all the important elements or components of a serious game, including learning components by specifying the desired learning outcomes, and their connections with the game, also, adding gaming elements to make it engaging and fun and finally making sure that the game has instructional components, like the tutorial, feedback, and scoring scheme.
- The usage of the ATT&CK framework as the main reference and source of information. Since as mentioned in section 2.2, the ATT&CK framework offers a standardized taxonomy of attack patterns, which helps to envisage the attack steps.
- Applying CKC to create the SEFs. This was done by ordering the tasks in the same order in which a CKC is performed in real-life.

- Finally, as mentioned in 5.1.2, the game's adaptation. The game's adaptation was applied in the scoring technique, the different roles, and the different scenarios from the different technology application domains in ATT&CK.

6.4 Game's Scenario Execution Flows (SEFs)

6.4.1 APT3 SEF

APT3 group starts its attack by getting to know and understand the system with the **Discovery** tactic, up until they gain execution over the system. These phases are known to be performed by APT3 in the following sequence:

1. Discovery
2. Privilege Escalation
3. Credential Access
4. Persistence
5. Exfiltration
6. Lateral Movement
7. Execution

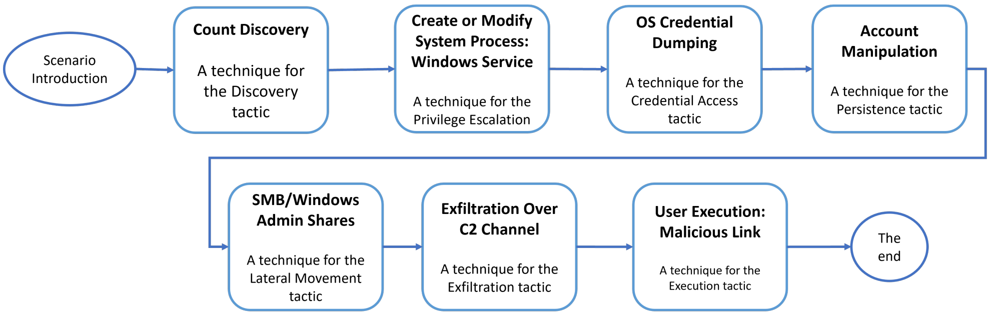

Scenario Introduction
Count Discovery
A technique for the Discovery tactic
Create or Modify System Process: Windows Service
A technique for the Privilege Escalation
OS Credential Dumping
A technique for the Credential Access tactic
Account Manipulation
A technique for the Persistence tactic
SMB/Windows Admin Shares
A technique for the Lateral Movement tactic
Exfiltration Over C2 Channel
A technique for the Exfiltration tactic
User Execution: Malicious Link
A technique for the Execution tactic
The end

Figure 6.4: APT3 SEF

The scenario for the APT3 group was built to cover tactics in the same sequence as listed above as shown in figure 6.4. The scenario starts with the main character of the Blue-team "Alti" giving some information about the group, and asking the player to help him mitigate the group's predicted attack. After the introduction, the player is given an explanation of the discovery tactic and how it is done by APT3 and is asked about the best way among the given options he/she thinks is best to mitigate the tactic. The next task in this flow is given by explaining how the APT3 are known to perform the privilege escalation tactic, and asking the player what he/she thinks should be done to prevent the group from performing the tactic successfully, and the player needs to choose the answer amongst three choices. Next, the player is told that this group usually steals credentials within the system, which helps them to get access to the systems while being hard to detect, and the player is asked to advise Alti to stop this tactic. The scenario continues to walk the player through the remaining tactics, passing from the persistence tactic to the exfiltration, followed by the lateral movement, and finally the execution.

Throughout the scenario flow, the tactics and the techniques that are used to perform the tactics are explained, and the player is asked for help to mitigate the attacks while given four choices to choose from.

6.4.2 Sandworm SEF

Sandworm is known with starting the attack by trying to get access to the system with the **Initial Access** tactic until it gets to the stage where they can manipulate accounts on that system. These phases are known to be performed by Sandworm in the following sequence:

1. Initial Access
2. Execution
3. Persistence
4. Evasion
5. Command and Control
6. Inhibit Response Function
7. Impair Process Control
8. Lateral Movement

Same as the SEF in section 6.4.1, and as shown in figure 6.5, the Sandworm scenario was designed to address the tactics and techniques in the same sequence as listed above. Starting from asking the player to choose amongst two choices what he/she thinks can prevent the attempt of gaining initial access, followed by giving the player three choices to choose from, to mitigate the execution of the tactics. Same as 6.4.1, the game walks the player through all the tasks that cover all the tactics until the last one. For each task, an explanation of the tactic and the used technique is presented.

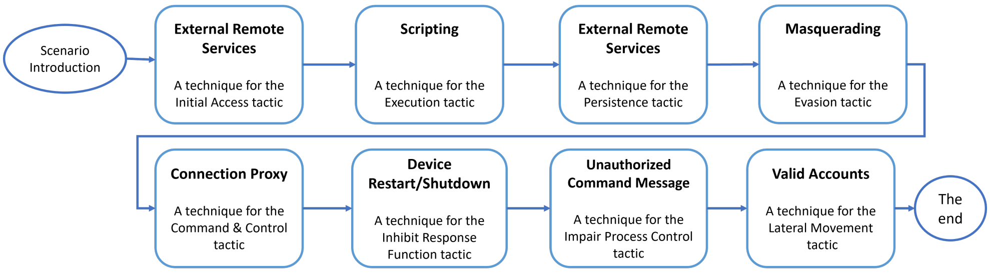

Scenario Introduction
External Remote Services
A technique for the Initial Access tactic
Scripting
A technique for the Execution tactic
External Remote Services
A technique for the Persistence tactic
Masquerading
A technique for the Evasion tactic
Connection Proxy
A technique for the Command & Control tactic
Device Restart/Shutdown
A technique for the Inhibit Response Function tactic
Unauthorized Command Message
A technique for the Impair Process Control tactic
Valid Accounts
A technique for the Lateral Movement tactic
The end

Figure 6.5: Sandworm SEF

6.4.3 Stealth Mango SEF

Stealth Mango Malware's behavior starts with the **Initial Access** tactic and moves up until it could have an impact on the system, the sequence of its behavior is as follow:

1. Initial Access

2. Discovery
3. Collection
4. Command and Control
5. Impact

As one of the Red-team scenarios, the main character here is Alma, the scenario starts with Alma talking about the Stealth Mango malware, and how she is planning to emulate the behavior of the malware. As the first tactic known to be performed by Stealth Mango malware is the initial access, the player is asked to choose a technique amongst three, to perform the tactic. Same as in the Blue-team scenarios, the first question has fewer options than the others. The flow continues to the next task, asking about techniques to perform the discovery tactic, in which the player is choosing amongst four choices. The same applies to the remaining tactics, where the name of the tactic in addition to the tactic's explanation is offered to the player for the collection, command & control until it reaches the Impact tactic. Figure 6.6 shows the SEF of the Stealth Mango scenario depending on the previous points.

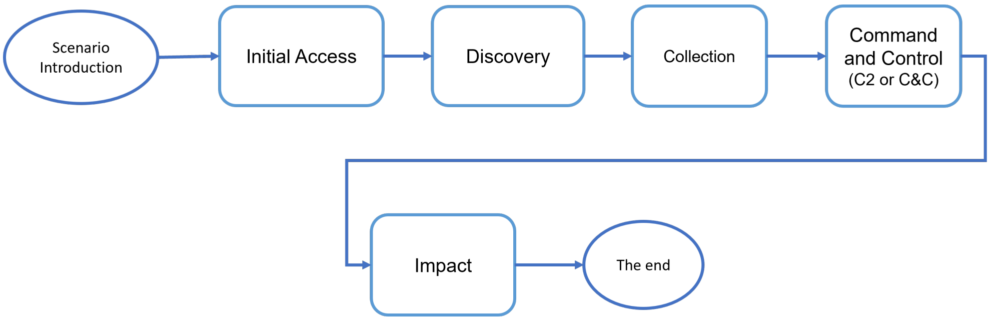


Figure 6.6: Stealth Mango SEF

6.4.4 FunnyDream SEF

FunnyDream campaign's behavior starts with the Resource development tactic and moves up until the Command and Control phase, the sequence of its behavior is as follows:

1. Resource development
2. Execution
3. Discovery
4. Collection
5. Command and Control

This scenario starts with Alma explaining the concept of campaigns and talking about the FunnyDream campaign. Walking through the same sequence as listed above, the first task in this scenario is to emulate what was done in this campaign to perform the resource development tactic, explaining the tactic, and giving three choices to the player to choose from. The next task would be asking the player to emulate the execution tactic, by choosing one technique out of the four choices presented to the player. Same as all the previous scenarios, the game walks the player through all the tasks by explaining all the tactics, and explaining that these tactics are performed in the same sequence as presented in the game. The player emulates one tactic after another until the sequence is over. Figure 6.7 shows the SEF of the Stealth Mango scenario depending on the previous points:

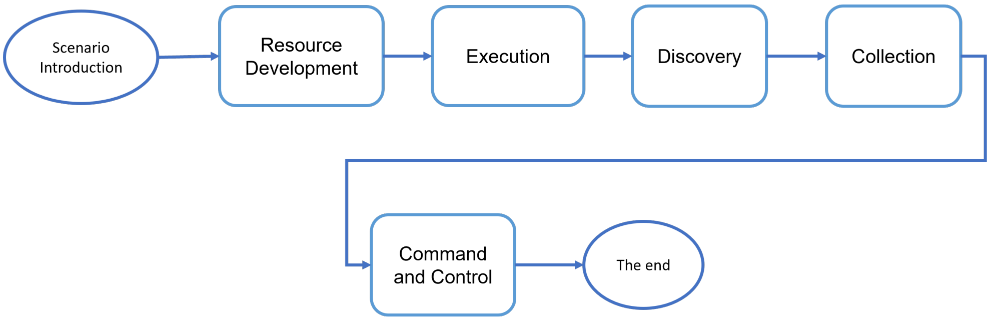


Figure 6.7: FunnyDream SEF

The following steps summarize the general game flow for each scenario"

1. After the player chooses which team to play with, the associated character will appear with an introduction about the character, name, job, and the help needed from the player.
2. The player needs to choose a mission out of the two available, where only the mission names are offered at this stage.
3. A quick introduction about the mission is given to the player, this introduction includes information about the adversary group, Malware, or Campaign, depending on which mission the player chose.
4. The first task is offered in a form of a question about the first phase of the performed CKC of the mission, in addition to the task's question, the player will be asked about how confident is he/she in their answer, also, the answers' choices will be shown, without the possibility to answer.
5. The interface will change depending on the player's choice for the confidence factor. If confident, only the answers' choices will be shown. If not confident, in addition to the answers' choices, the player will be offered a hint option, that redirects him/her to the related web page in the ATT&CK framework to look for the correct answer. The answers' choices can contain more than just one correct answer for the question.
6. Depending on the correctness of the answer, feedback will be given to the player justifying why the answer was correct or incorrect, with an extra option that can redirect the player to the related web page in the ATT&CK framework, to read more if they are interested.
7. The same process happens for the following tasks, with the score showing to the players.

8. After finishing all the tasks in the mission, final feedback is given to the player, containing the final score, the number of correct answers, and other extra options to replay, start a new mission, or quit the game.

Figure 6.8 shows an example of the previous steps that are applied to the Stealth Mango scenario.

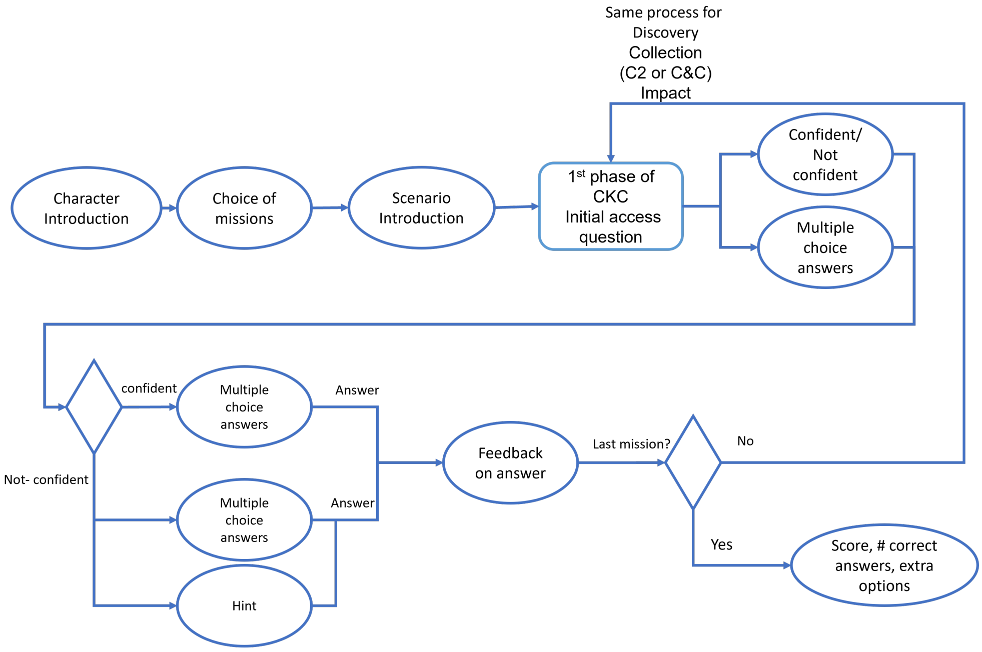


Figure 6.8: Stealth Mango scenario flowchart

6.5 Deployment

In order to distribute the game amongst players, it needed to be hosted on a server. For this matter, the game's code and all related files were uploaded into a repository in GitHub, and the repository was connected to a Heroku app. Heroku was used because it is compatible with Python, and it provided a free service during the period of the evaluation. Instead of using command lines to Pull, Commit, and push the changes to the remote repository, GitHub Desktop was used to update the GitHub repository with any changes on the project with only a click.

Figure 6.9 shows an overview of the deployment process.

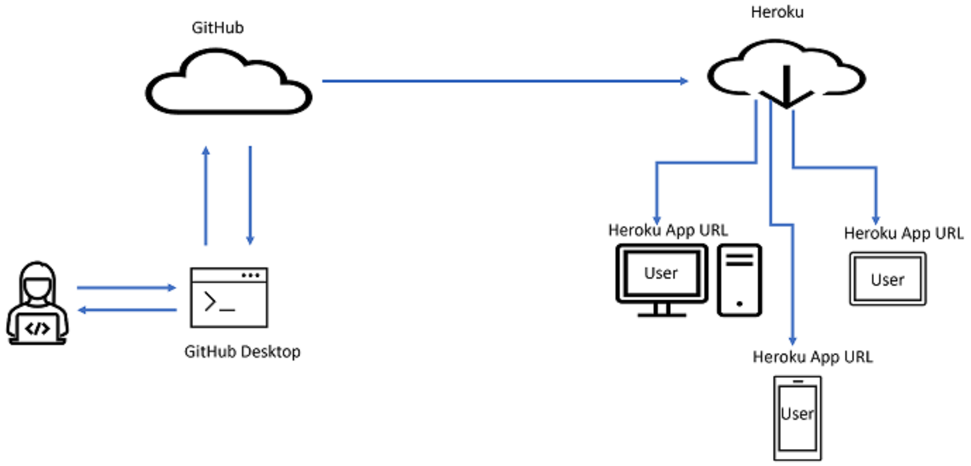


Figure 6.9: Game's deployment process

The source code of the game can be found in the author's GitHub repository. [1].

The game can be reached and played via its link. [2]

[1] https://github.com/MACSLama/webGame

[2] https://macsgame.herokuapp.com/

Chapter 7

Evaluation & Results

Game testing was conducted in two different methods, **Qualitatively**, by professors and teachers involved in relevant teaching in NTNU, and **Quantitatively**, by bachelor-level cyber security students.
The qualitative evaluation was conducted over two phases, the first was for the participants to play the game, and the second was to answer a Post-game questionnaire, that contained a group of statements about the game. The answers' options were given based on a **Likert-type Scale**, a psychometric response scale that scales the level of agreement on a statement [48]. The options given were:

1. Highly disagree
2. Disagree
3. Neutral
4. Agree
5. Highly agree

The questionnaire's statements considered the three serious games activities as divided by ATMSG: **Learning activities**, **Instructional Activities**, and **Gaming activities**. Some of the activities can overlap between more than one category, but for the sake of simplicity, each mentioned component will be evaluated only in the activity it was mentioned in.

The quantitative evaluation method was conducted over three phases, and it was held during a lab session at NTNU, Gjøvik campus. First, the students were asked to answer a Pre-game questionnaire, then try and play the game, and finally, they were asked to answer a Post-game questionnaire.
The Pre-game questionnaire was designed to collect information about the student's knowledge of the ATT&CK framework, whether they were taught the framework in a course, their experience in learning the framework, their study level, and their interests as video game players (if any).
The Post-game questionnaire was a combination of statements with the Likert Scale as in the Qualitative evaluation and questions with multiple choice answers. Same to the Qualitative evaluation, the questionnaire was divided into three serious games activities.

The following sections will be as follow: The first section will present participation in the evaluation sessions, followed by the results of the Pre-game questionnaire that was given to the students, Followed by sections that present the questions and the collected answers to the professors, and students' Post-game questionnaires, divided into the three serious game components.

7.1 Evaluation sessions Participation

Twelve second-year students from the cyber security bachelor's program participated in the quantitative evaluation. All of them finished the three phases of the experiment. The game's link and the questionnaire were shared amongst eight professors and teachers, that are involved in bachelor's cyber security teaching. Five out of the eight participated in the testing, four of them answered the questionnaire, and one gave general feedback on the game, about what he thinks is good and what needs to be improved. All questionnaires with the result report can be found in Appendix C, D, and E

7.2 Students' Pre-game Questionnaire & results

Table 7.1 shows the Pre-game questionnaire. Followed by the responses collected from the students. The column "Label" in the table represents the reference of the questions in the results' figures.

Table 7.1: Quantitative Pre-game Questionnaire

Questions	Label	Answers' options
Have you heard about MITRE ATT&CK framework before?	"Heard about ATT&CK "	- Yes - No
If Yes		
Were you taught the MITRE ATT&CK framework in one of your courses?	"Studied ATT&CK"	- Yes - No
How can you describe your experience in learning the ATT&CK framework in a class?		-Unsatisfactory -Satisfactory - I don't know
How would you describe your Knowledge of the ATT&CK framework?	"ATT&CK Knowledge"	- None - Simple - Medium - Very good - Expert
At which level are you in your study?	"Study level"	- 1st Year - 2nd Year - 3rd Year - Higher level
Do you play video games?		- Yes - No
If Yes		
What type of video game player do you consider yourself? (Can choose multiple)	"Type of player"	- It is all about points and status for me - I like to see new things and discover new secrets - I experience fun in games through interaction with other players - I like to see other people lose
What type (Genre) of video games do you prefer to play? (Can choose multiple)	"Genre"	- Strategy Games - Role-Playing Games - Educational game - Other
What other game Genre do you prefer to play?		Open-ending

All twelve students have heard about the ATT&CK framework before, but only nine of them were taught it in a course, as shown in figure 7.1.

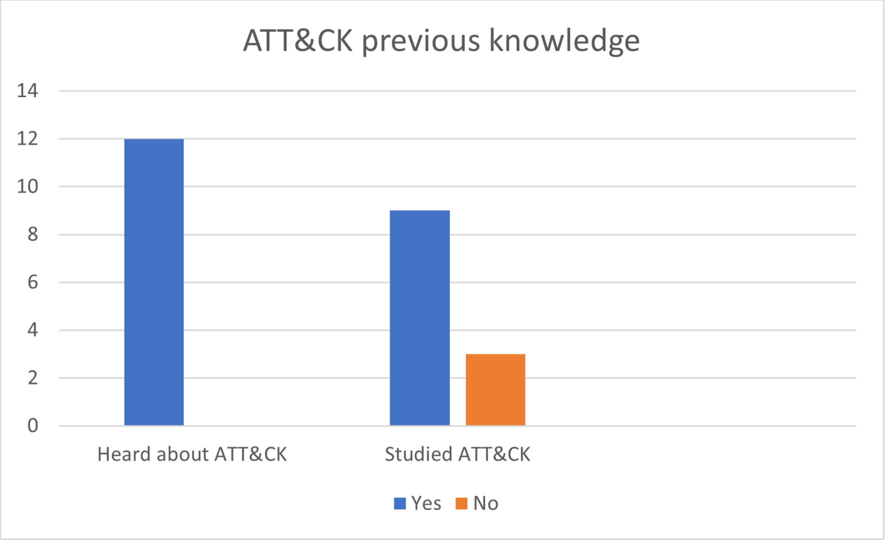


Figure 7.1: ATT&CK previous knowledge

They were asked about the level of knowledge they think they have about the ATT&CK framework, eleven answered: Simple, and one answered: Medium.

For those who answered that they were taught the framework in a class, they were asked to describe their experience in learning the ATT&CK framework in a class. Figure 7.2 shows the results.

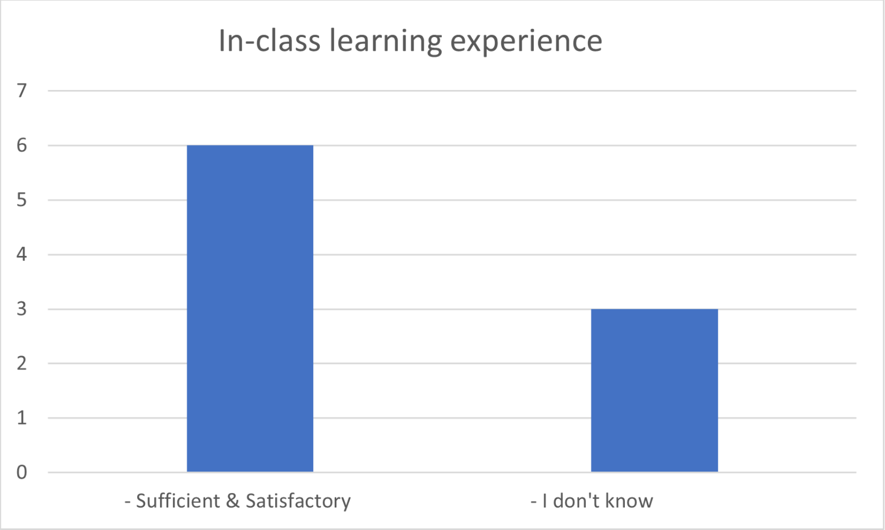


Figure 7.2: In-class learning experience

When asked about whether they play video games or not, nine of them answered

Yes and the other three answered No. Those who play video games were asked what type of players they considered themselves, they were given the description of the players' type classified according to Bartle's Player Types for Gamification as presented by Tuunanen et al. [49], which classifies the players based on observations on their behavior while playing as:

1. The Achiever: all about points and status.
2. The Explorer: wants to see new things and discover new secrets.
3. The Socializer: experiences fun in games through interaction with other players.
4. The Killer: wants to see other people lose.

They were given only the description of the types without the name of each type, to avoid making the students uncomfortable with labeling themselves under certain categories. They were not limited to a number of answers as the previous answers, and the results were as shown in figure 7.3.

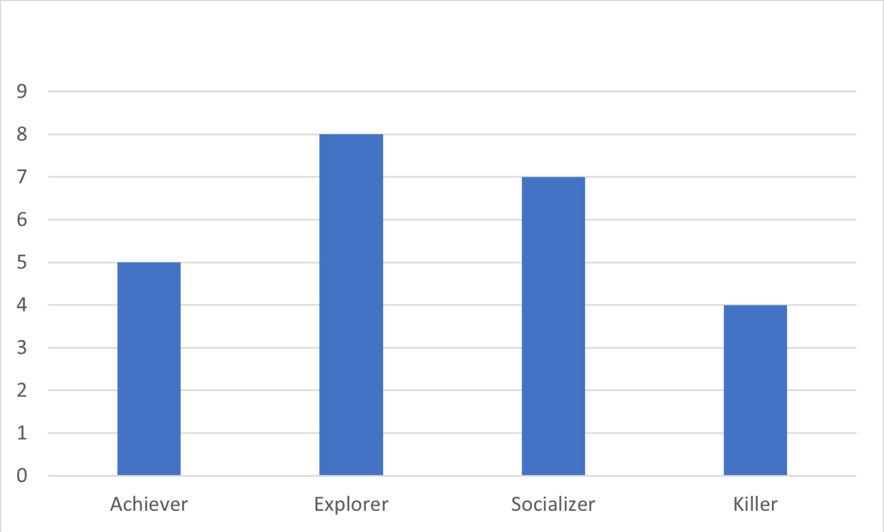


Figure 7.3: Player's types

The students had many preferences when asked about the game genre they prefer to play, but mostly, they preferred Racing, Competitive, Adventure, and Fighting.

7.3 Post-game Questionnaires & Results: Learning Components

For evaluation of the game's learning components, the content was divided into two categories, Pedagogical considerations and Gameplay connections with Learning Outcomes (LOs). The content and the results are presented in the following sections.

7.3.1 Professors

[1] For the pedagogical considerations, the following statements were given.

- The game promotes active learning. ("Active learning")
- The game promotes continuous learning .("Continuous learning")
- The game provides students with good cyber security “knowledge and skills” practice. ("Practice")

The results for the active learning statement varied between highly agree, and agree, with three professors who replied with agree and one replied with highly agree as shown in figure 7.4.

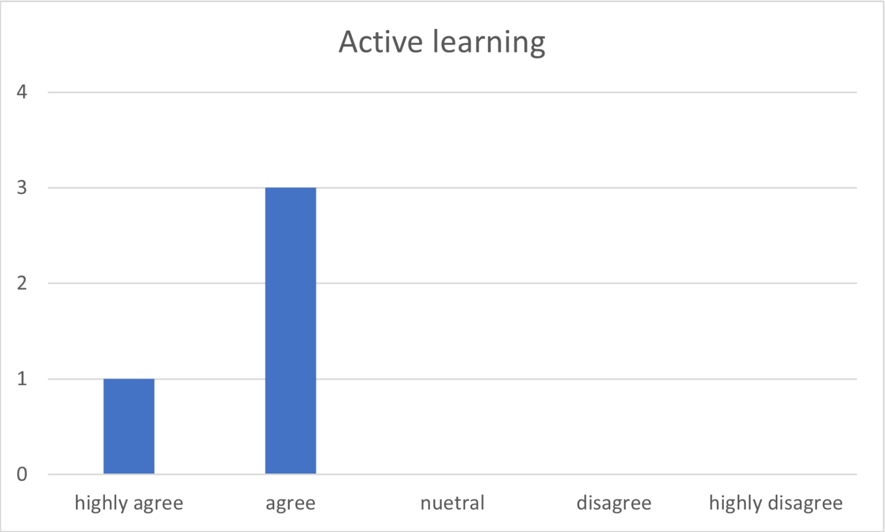


Figure 7.4: Active learning: Professors

As for the continuous learning statement, one of the professors was skeptical about the idea and replied with neutral, while the remaining three replied with agree, as shown in figure 7.5.

The third statement got unanimous approval, with the four professors agreeing that the game offers good practice for students, as shown in figure 7.6

[1] Labels of statements are between quotation marks

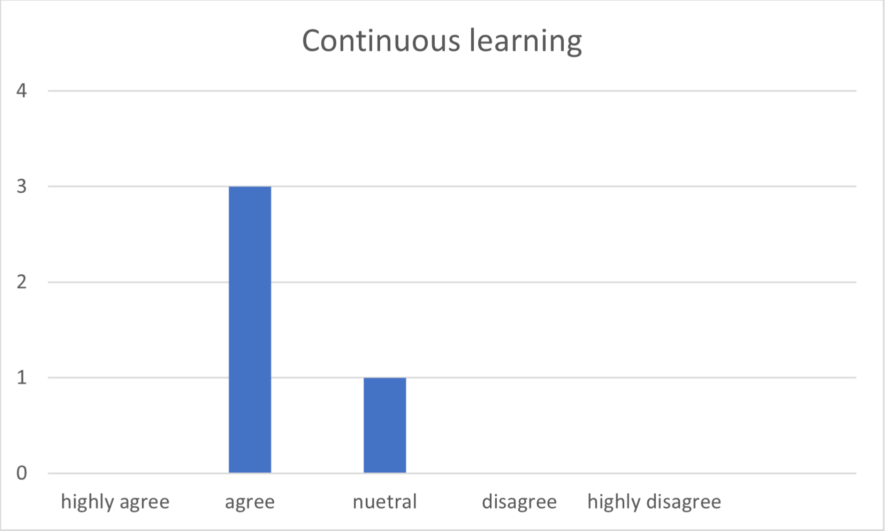


Figure 7.5: Continuous learning: Professors

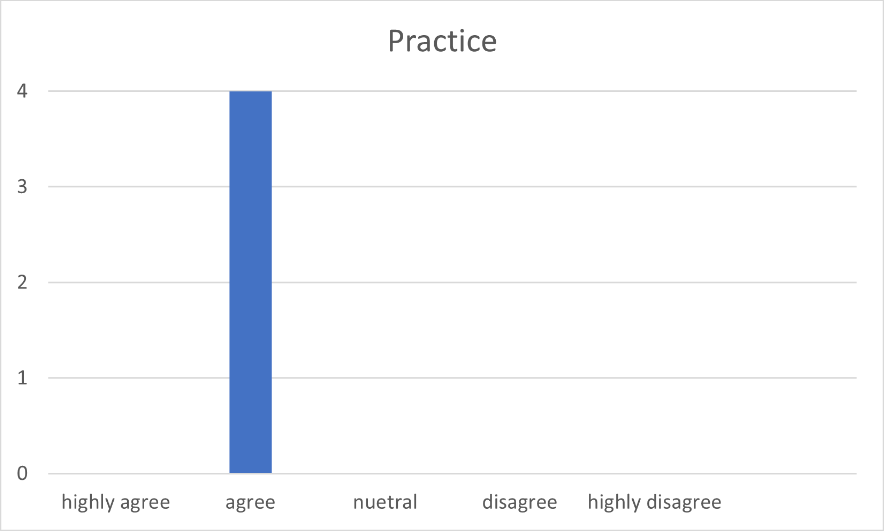


Figure 7.6: Practice: Professors

Moving to Gameplay connections with Learning Outcomes (LOs), the related Statements were the following:

- The confidence factor would motivate students to use the Hint option and visit the ATT&CK framework. ("Conf. factor motivation")
- The confidence factor increased the game's adaptability (adapting the options and scoring to the student's level of knowledge). ("Conf. factor adaptivity")
- The different scenarios increased the game's adaptability (adapted to include scenarios from different domains in ATT&CK). ("Diff. scenarios ad-

aptability")

- The game would be a successful secondary tool to be used in teaching the ATT&CK framework. ("Secondary teaching tool")

As for the effect of the confidence factor in motivating the players to use the Hint, the professors agreed that it can have this effect, The same was for the effect of the confidence factor on the adaptability of the game, where three agreed and one had a neutral opinion for this. The results for both statements were combined and shown in figure 7.7

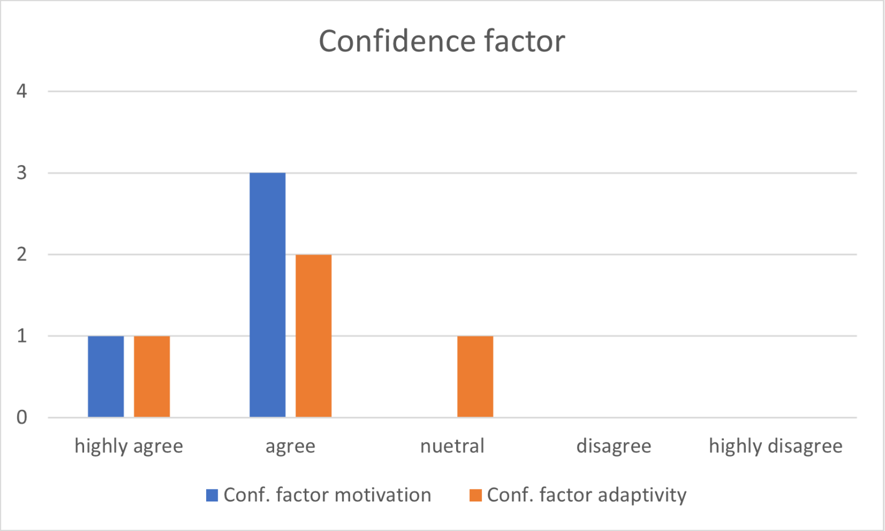


Figure 7.7: Confidence factor: Professors

All four professors agreed on the third statement which suggests that the different scenarios increased the game's adaptability, as shown in figure 7.8.

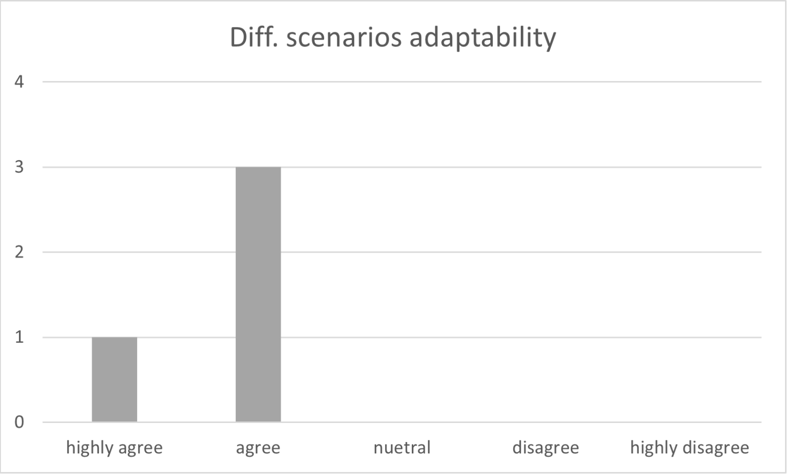


Figure 7.8: Different scenarios adaptability: Professors

The responses of professors for the last statement varied, as shown in figure 7.9

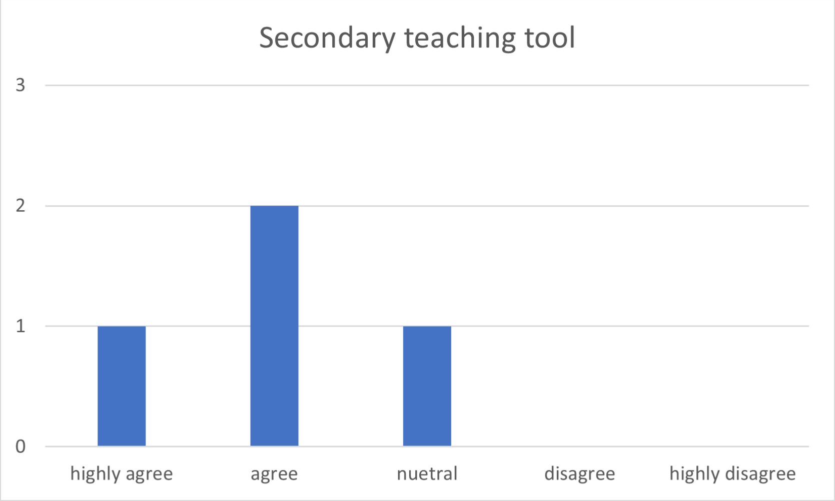


Figure 7.9: Game as a secondary tool: Professors

7.3.2 Students'

Statements for the pedagogical considerations with their results are listed below.

- The game promotes active learning. ("Active learning")
- The game provided me with good cyber security (knowledge and skills) practice. ("Practice")

The students' responses for both statements varied, as shown in figures7.10 and 7.11.

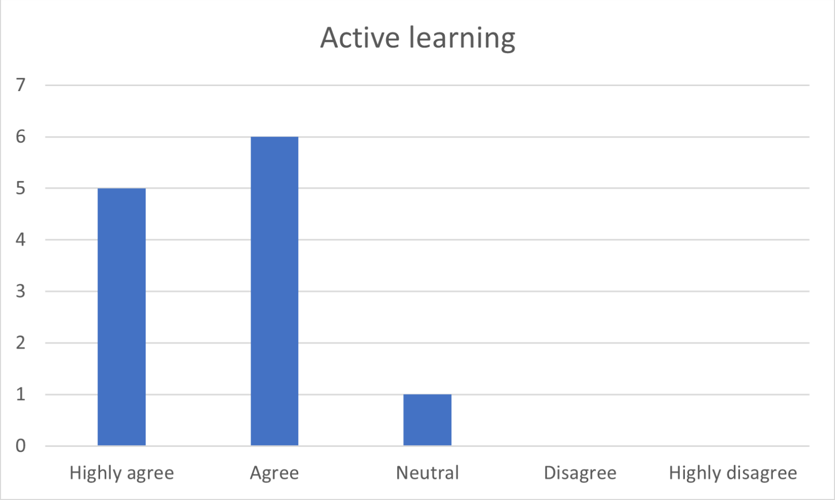


Figure 7.10: Active learning: Students

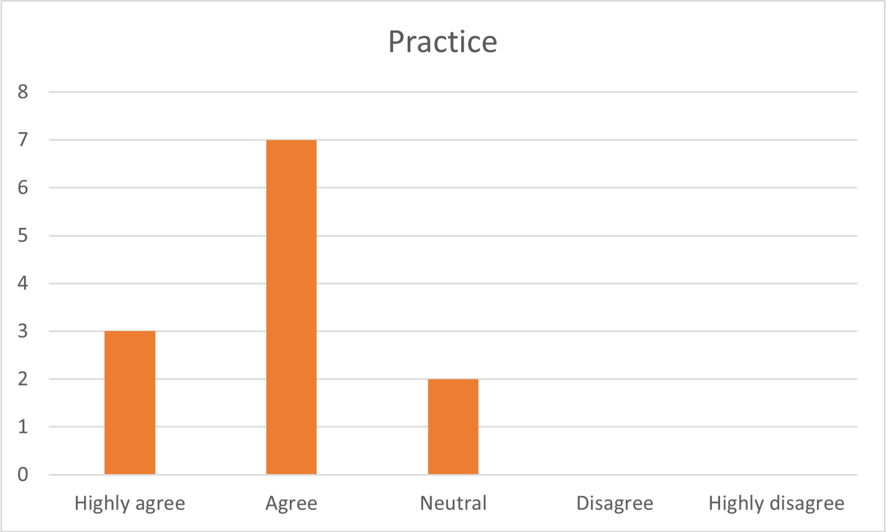


Figure 7.11: Practice: Students

Moving to Gameplay connections with Learning Outcomes (LOs), the related Statements were the following:

- Redirecting to the ATT&CK webpage helped me with finding the correct answer. ("Redirect to ATT&CK")
- Redirecting to the ATT&CK webpage helped me with getting familiar with the ATT&CK framework. ("Redirect to ATT&CK for familiarity")
- Dividing the missions into several tasks made it easier for me to focus on learning about each one. ("Mission division")
- By designing the scenarios to include every stage of an attack, from the first to the final, I was better able to understand the attack as a whole. ("Understanding the CKC")
- How would you describe the level of knowledge you gained about the ATT&CK framework after playing the game?

Redirecting the player to the ATT&CK webpage was intended for two reasons, to help the students find the correct answer, on which the majority agreed, as shown in figure 7.12 The same figure shows the results of the second reason, which is to get familiar with the ATT&CK framework, on which the responses varied as shown in the figure.

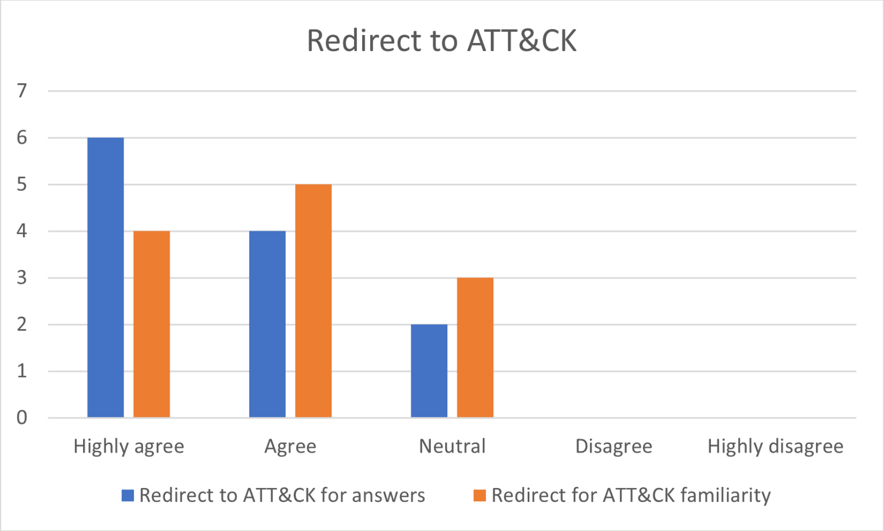


Figure 7.12: Game play connections with (LOs): Redirect to ATT&CK

The division of missions into several tasks was made for a better understanding of each task individually. Figure 7.13 shows how the students responded to this.

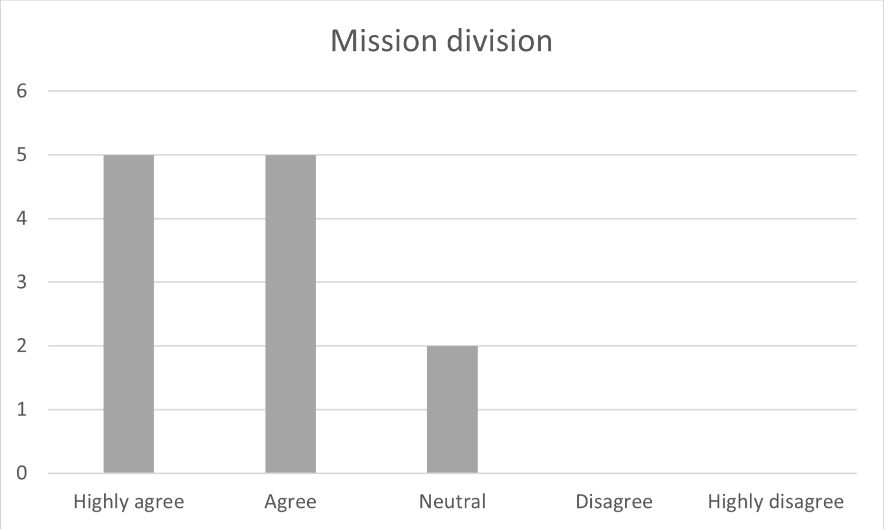


Figure 7.13: Game play connections with (LOs):Mission division

As for designing the scenarios to include all steps of the CKC, figure 7.14 shows how the students responded.

The last question collects data about how much knowledge the players gained after playing the game, figure 7.15 shows the results.

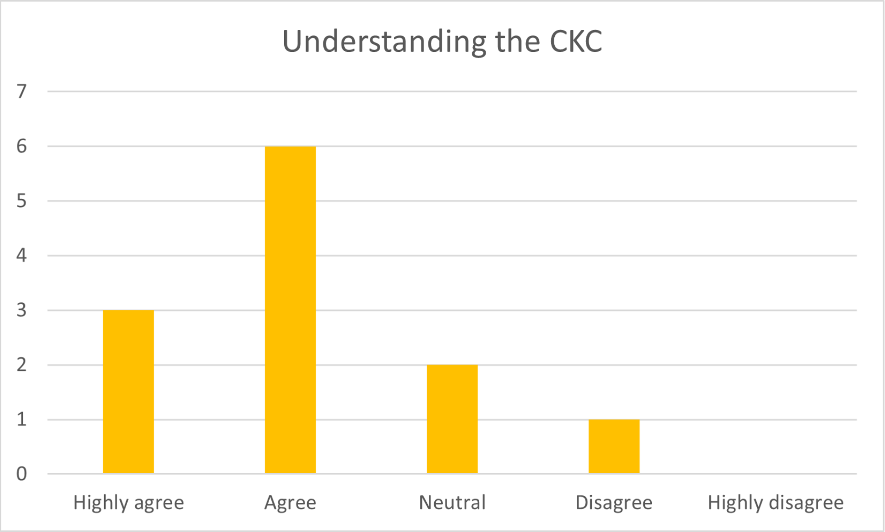


Figure 7.14: Game play connections with (LOs): Understanding the CKC

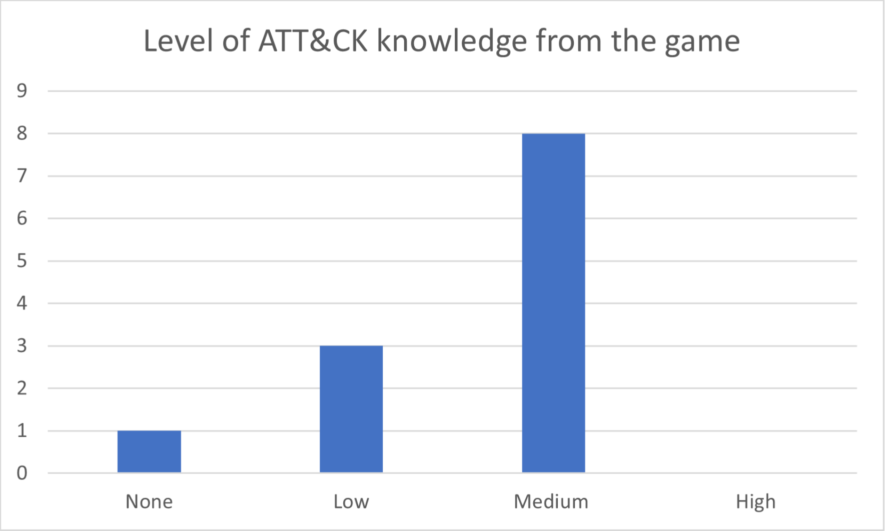


Figure 7.15: Game play connections with (LOs): Level of knowledge from game

7.4 Instructional Components: Professors & Students

The instructional components of the game were divided into three categories: Assessment, Feedback, and Tutorial. The content and the results are presented in the following sections.

7.4.1 Professors

Statements related to the Assessment and Feedback are listed below:

- The scoring scheme of the game helps to decrease the stress level and results in better learning outcomes. ("Scoring scheme & Stress")
- The instance feedback would affect the student's decision in choosing hints for the next mission. ("Instant feedback")
- The information in the feedback was found sufficient. ("Feedback Info")

Figure 7.16 shows that the majority of professors agree that the scoring scheme would have an impact on decreasing the stress level of players.

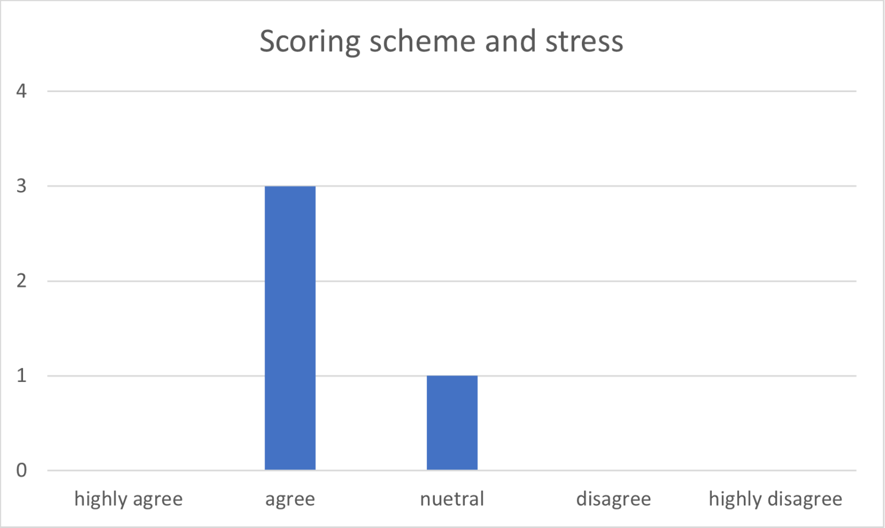


Figure 7.16: Assessment: Professors

The professors were also asked about the feedback quality of information and its' effect on players' decisions, the responses are shown in figure 7.17.

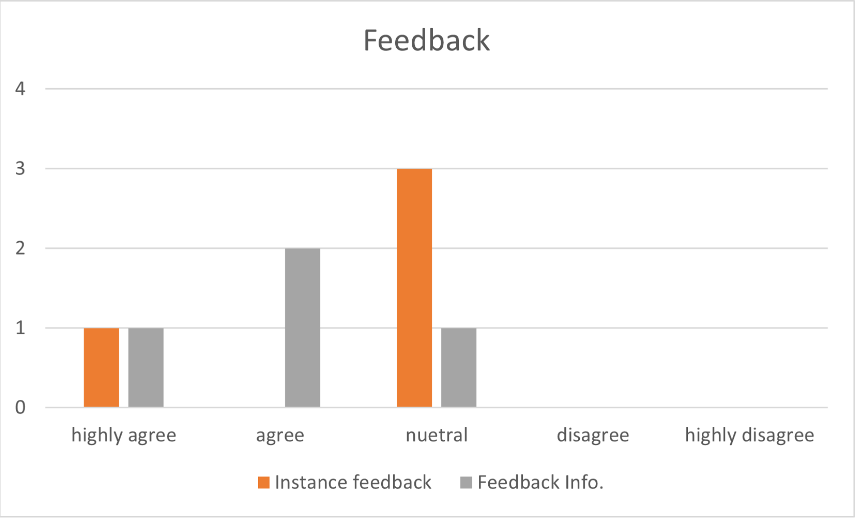


Figure 7.17: Feedback: Professors

The statements below represent the tutorial-related components.

- The game's tutorial was found useful for understanding the game's objectives. ("Tutorial")
- Explaining the scoring scheme before starting the game helped with understanding how to play the game. ("Scoring explanation")
- Using the game's characters helped with understanding the mission's goal. ("Characters")

Responses regarding the tutorial's effect in understanding the game's objectives are shown in figure 7.18

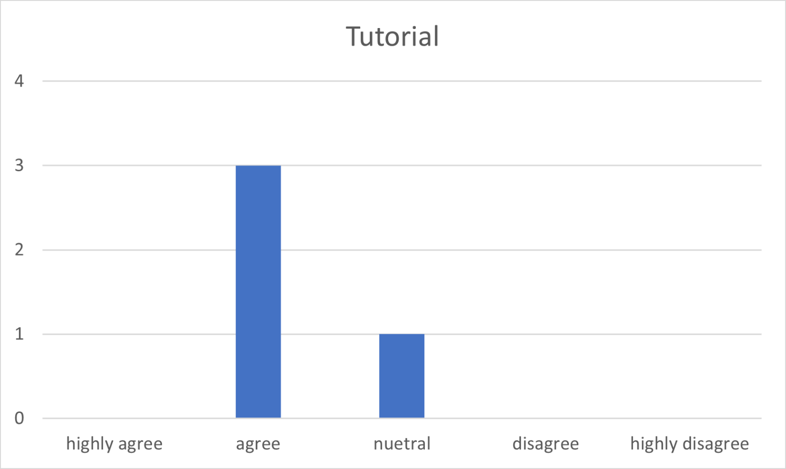


Figure 7.18: Tutorial: Professors

As for the tutorial that was added for explaining the scoring scheme, figure 7.19 shows how professors responded.

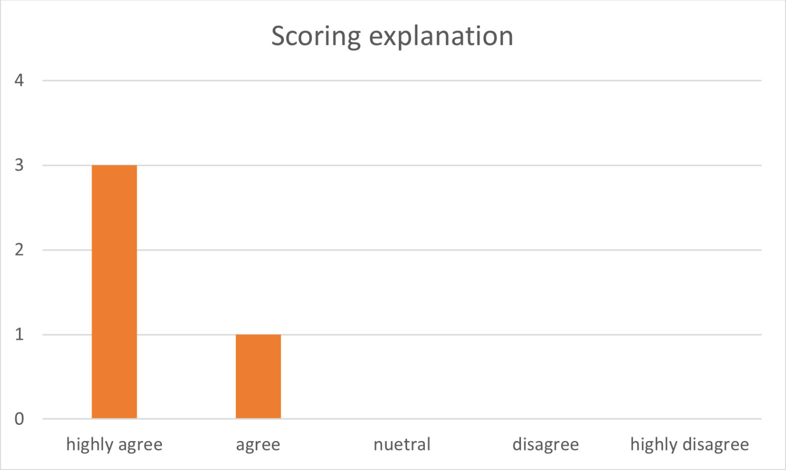


Figure 7.19: Scoring explanation: Professors

7.4.2 Students

Students had a different set of statements and questions than professors, The assessment-related statements are listed below.

- I found the choice “Not Sure” helpful to continue the game. ("Helpfulness of the -Not sure-")
- The 2 points deduction for being falsely confident encouraged me to take a hint. ("2 points deduction")
- The 2 points award for being confident encouraged me to answer without a hint. ("2 points award")
- The scoring technique was fair. ("Scoring fairness")
- How often did you use the hint to visit the ATT&CK framework?

Figure 7.20 shows how much the students found the option -Not sure- helpful. The figure shows how variant were the responses.

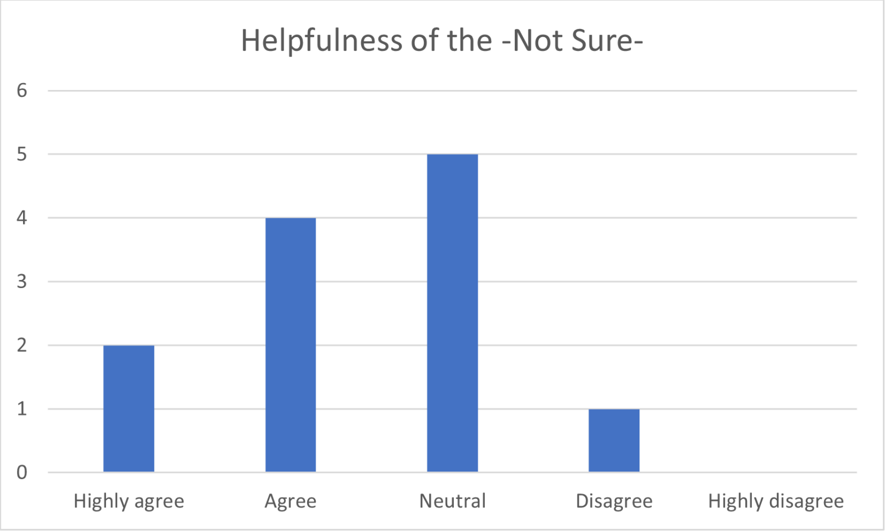


Figure 7.20: Helpfulness of the -Not sure-: Students

Since using and not using the Hint affected the player’s score, the second and third statements were added to measure how this affected the player’s decision in playing. The results are shown in figure 7.21

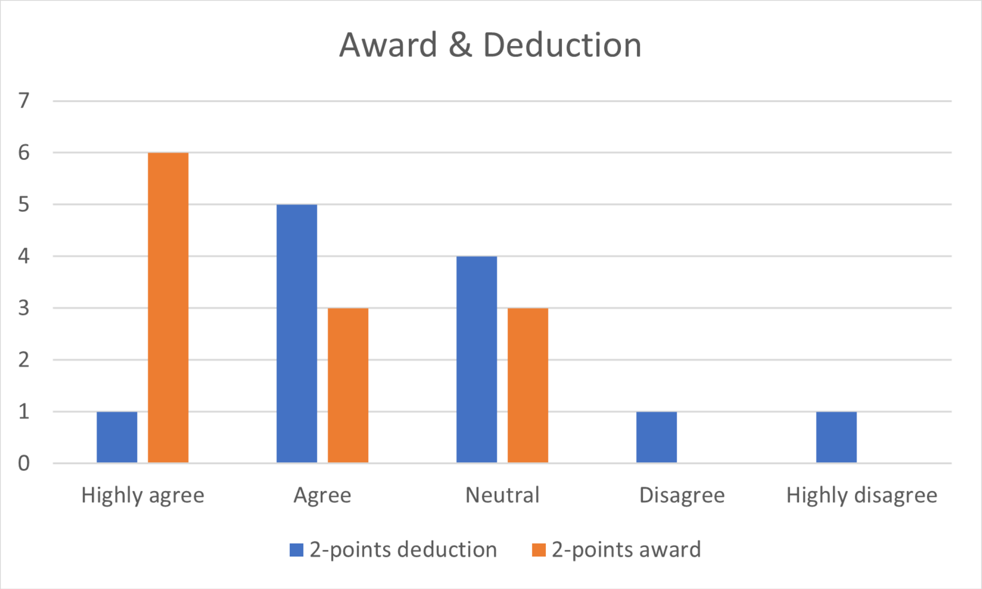


Figure 7.21: Award Deduction: Students

It was important to check whether the players found the scoring scheme fair or not, and figure 7.22 shows their responses.

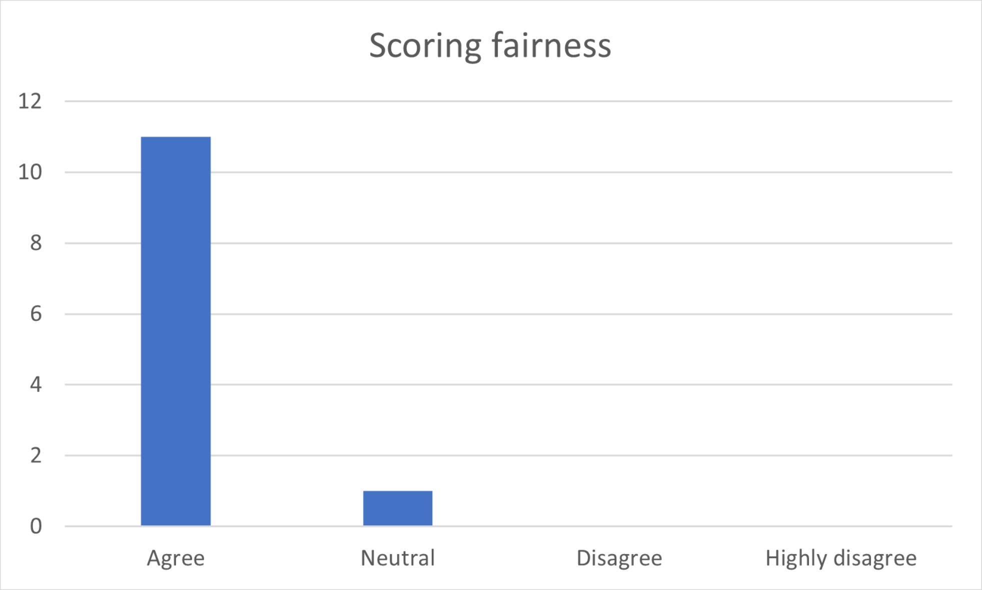


Figure 7.22: Scoring fairness: Students

Last question was given, to check whether the students took advantage of the Hint or not, the results are shown in figure 7.23

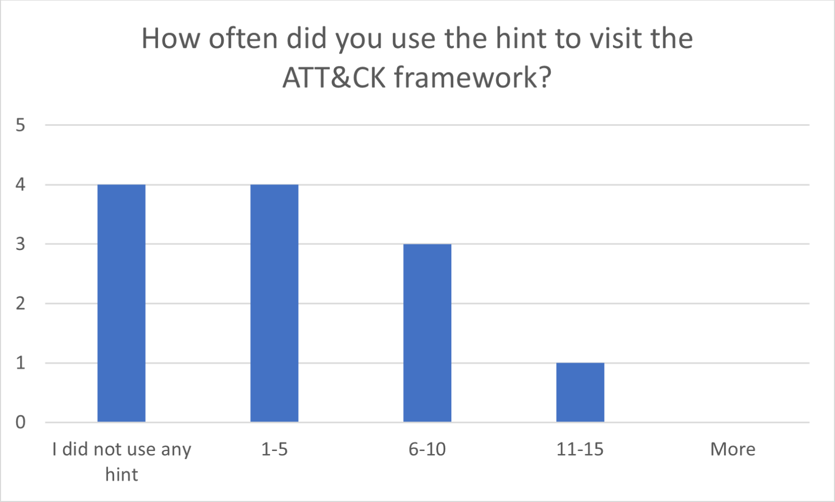


Figure 7.23: Using Hint: Students

The second category for the instructional component is Feedback. The following statements were the ones that covered this area.

- The instance feedback affected my decision in choosing hints for the next missions. ("Effect of feedback on decision")
- The feedback helped me not to be too confident for the next mission. ("Helpfulness of the feedback")
- I found the information given in the feedback useful and informative. ("Feedback info")

The instant feedback did not seem to have a remarkable effect on the students' decision in the next missions, as shown in figure 7.24

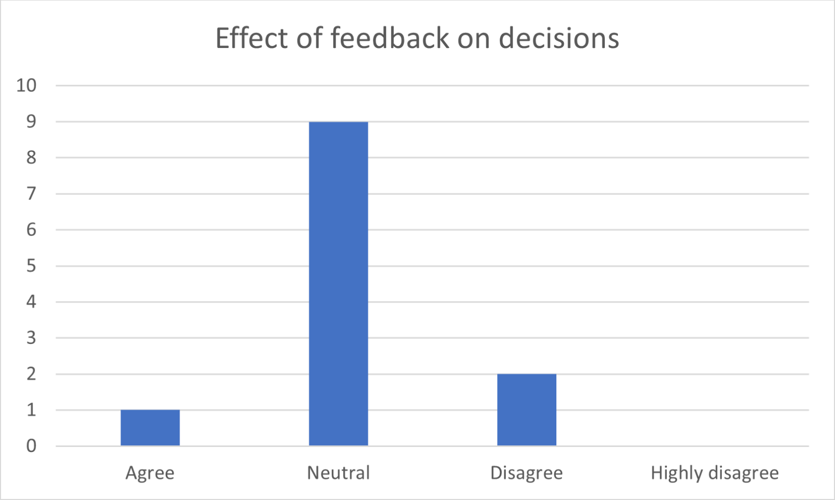


Figure 7.24: Feedback: Students

Since the instance feedback did not have an impact on the student's decision, then it is logical for the second statement to have almost the same response, as shown in figure 7.25.

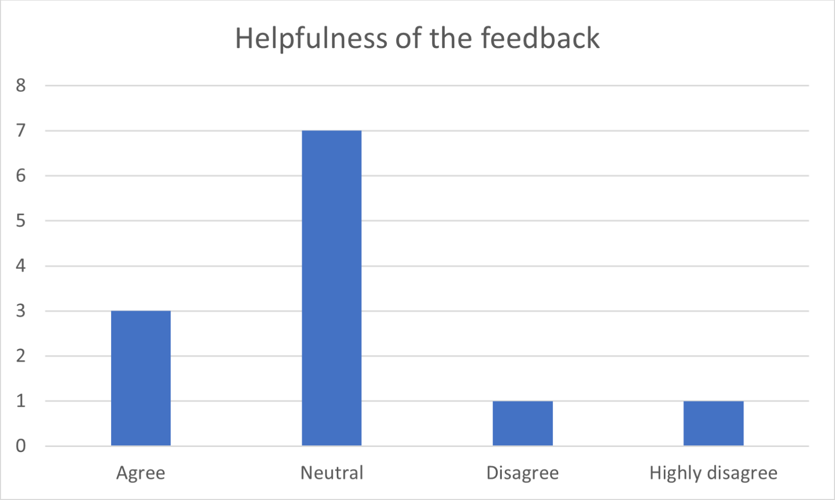


Figure 7.25: Feedback: Students

Regardless of the effect of the feedback on the students' decision, it was needed to check how useful and informative they found information in the feedback. Figure 7.26 shows how did the student respond to this.

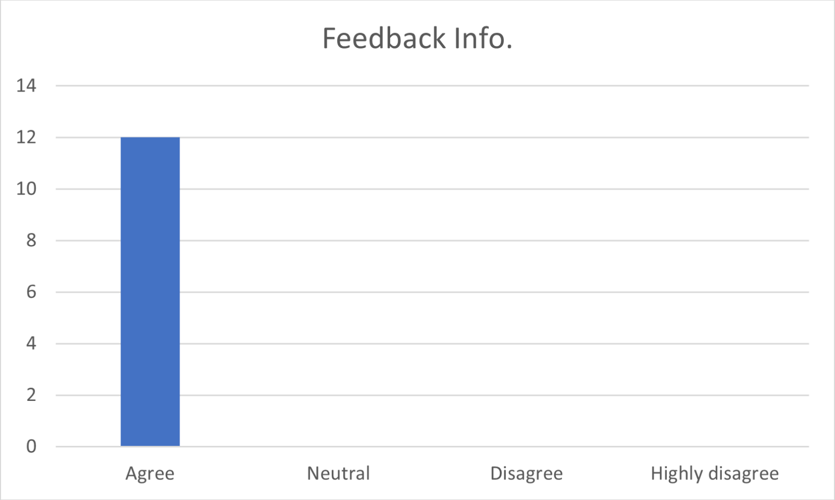


Figure 7.26: Feedback: Students

For the last component in the instructional components, the statements related to the tutorial are listed below:

- I found the tutorial helpful in understanding the game's objectives. ("Tutorial")

- I found the scoring description at the beginning of the game helpful in understanding the confidence factor. ("Scoring description")
- I found the game's characters (Alma & Alti) helpful in understanding the mission's goal. ("Characters")

The first statement checks how useful the students found the tutorial to understand the objectives of the game. Figure 7.27 shows the results.

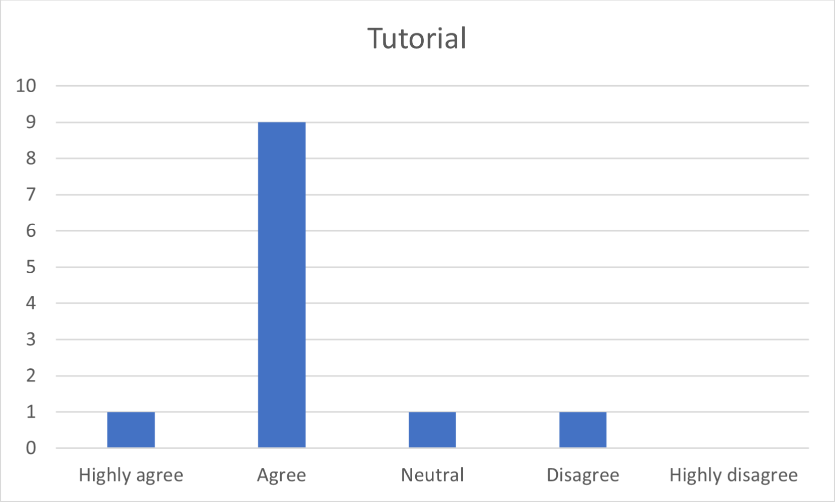


Figure 7.27: Tutorial: Students

The same applies to the second statement, which checks how helpful the students found the scoring description to understand the confidence factor, the results can be seen in figure 7.28

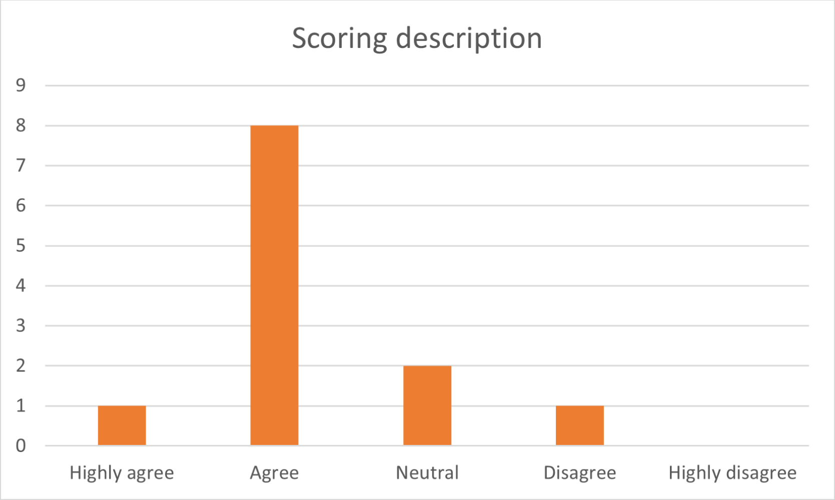


Figure 7.28: Tutorial: Students

The last statement was related to using the characters, and their effect on understanding the goal of each mission. Responses for this statement are shown in figure 7.29.

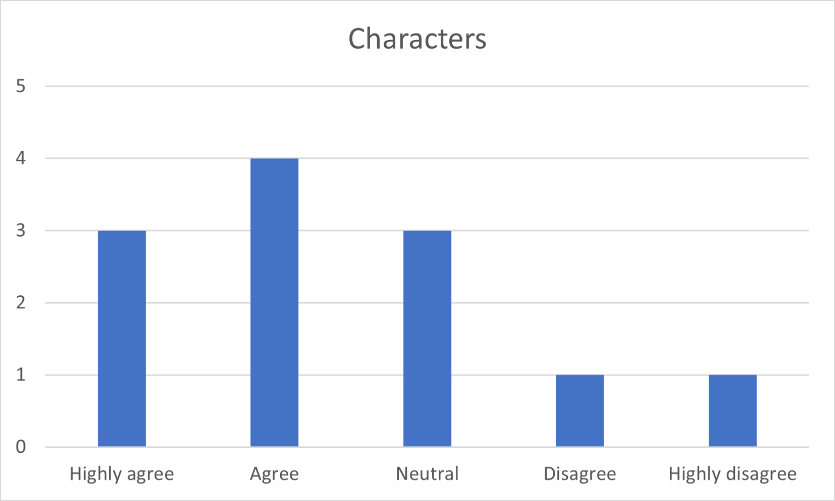


Figure 7.29: Tutorial: Students

7.5 Gaming Components: Professors & Students

The gaming components were evaluated differently between professors and students. The following sections will show how they were divided for both evaluations

7.5.1 Professors

For this evaluation, the gaming components were divided into two categories, Fun, and Usage considerations, and the related statements are listed below.

- The different roles and scenarios made the game fun and motivating. ("Fun & Motivation")
- The user interface was easy to use. ("UI")

For the first statement, which checks whether the professors found that different roles and scenarios can be fun and motivating for students, figure 7.30 shows the results.

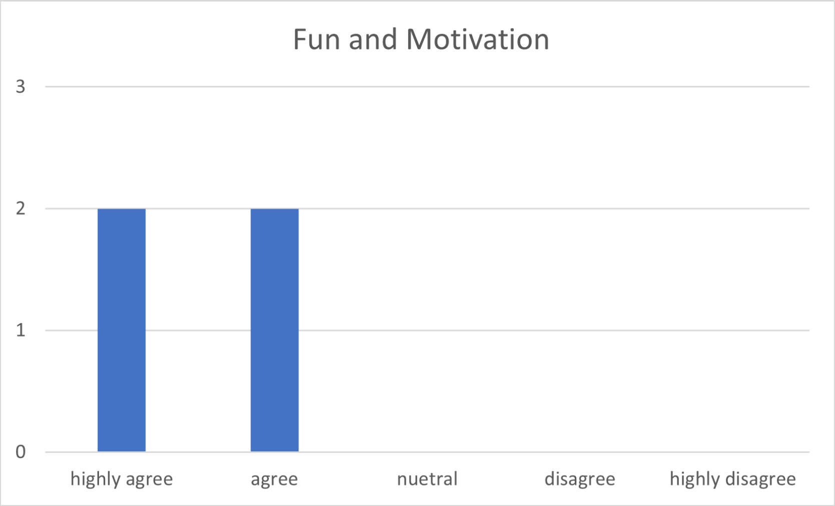


Figure 7.30: Fun & Motivation: Professors

Regarding the UI, in which the only factor that was assessed for professors was how easy it is to use. Figure 7.31 shows the results.

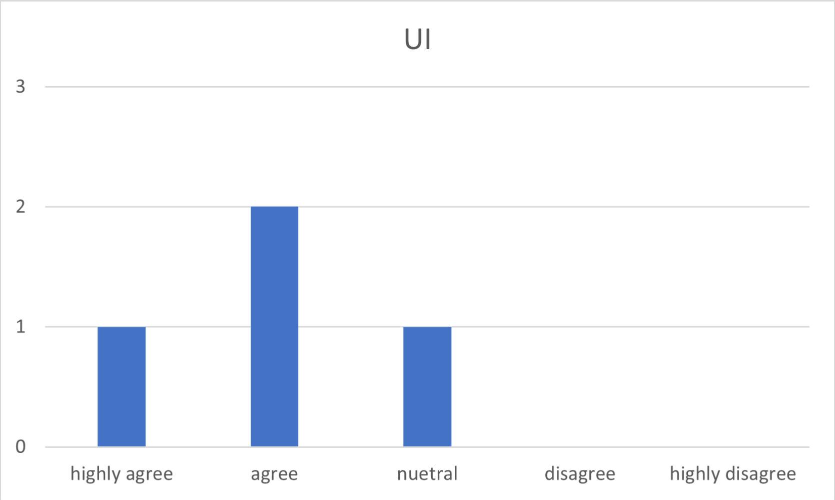


Figure 7.31: UI: Professors

7.5.2 Students

Gaming components were divided into four categories for the students' questionnaire, Fun, Stress, UI, and Gameplay. The following were the questions related to the fun factor of the game

- How would you describe having different scenarios for playing the game? ("Diff. scenarios experience")

- How would you describe having multiple roles for playing the game? ("Multiple roles experience")
- How enjoyable and engaging is it to learn about the ATT&CK framework through the game, compared to traditional methods used before? ("Game vs. class")

The first two questions are asking about the effect of having multiple scenarios and roles in the game on the fun and engagement factors of the game. Figure 7.32 shows how the students felt about these features.

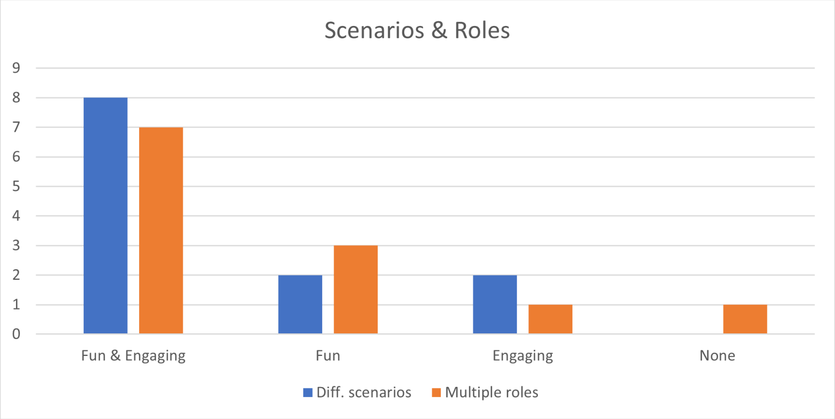


Figure 7.32: Fun: Students

To do the comparison between in-class learning and game-based learning for the ATT&CK framework, the third question was added. The results are shown in figure 7.33.

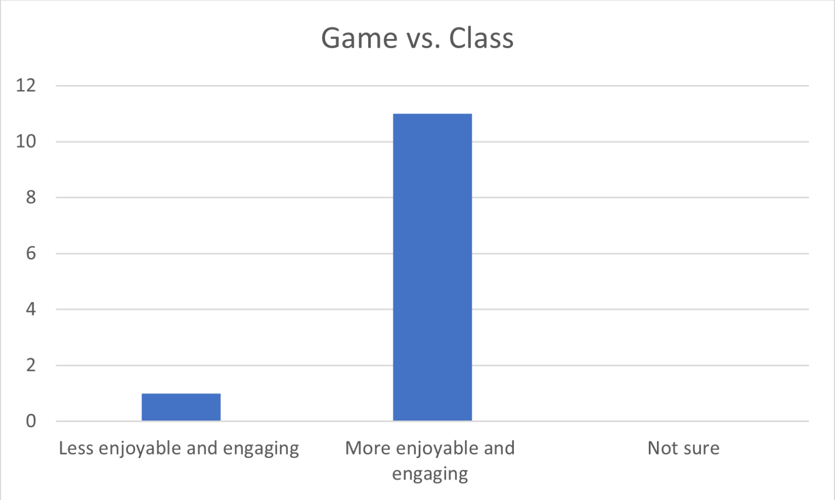


Figure 7.33: Fun: Students

The stress factor was evaluated via the following questions/statements.

- I found the ATT&CK website overwhelming. ("ATT&CK experience")
- How would you describe your feeling when you chose "Not confident"? ("Stress level not conf")
- How would you describe your feeling when you chose "Very confident"? ("Stress level conf")

To see how was the students' experience working with the ATT&CK framework, the author guessed that it would be overwhelming, and collected the students' responses. Figure 7.34 shows the results.

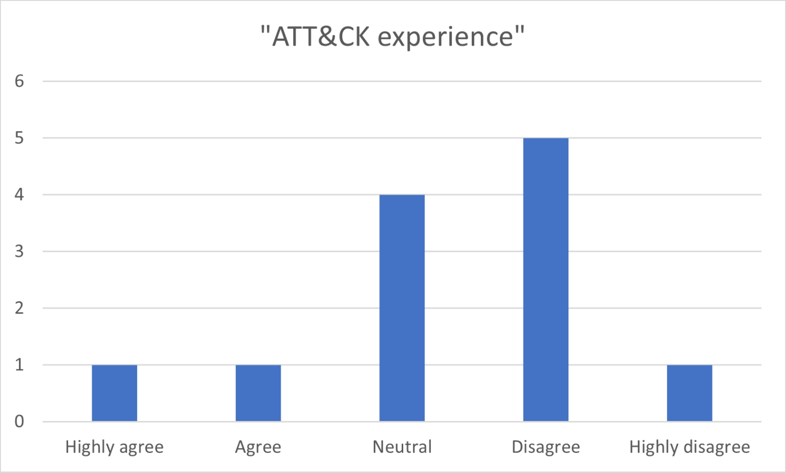


Figure 7.34: Stress: Students

Regarding the second and third questions, the focus was on testing whether the scoring scheme has any effect on the students' stress levels while playing. The answers are shown in figure 7.35.

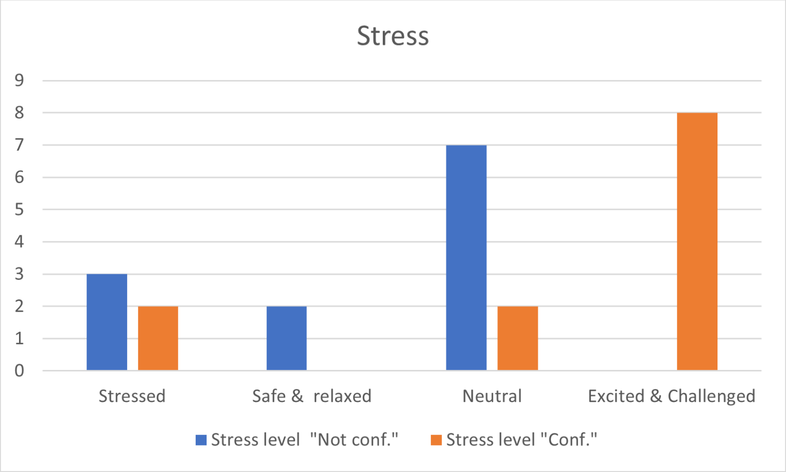


Figure 7.35: Stress: Students

For the UI and Gameplay as the final categories for the gaming components, the following questions were used.

- How would you describe the user interface? "UI"
- Did you try playing with both roles?
- How many missions did you finish?

To describe the UI, the students were given the options shown in figure 7.36 to choose from, and their answers were as shown in the figure.

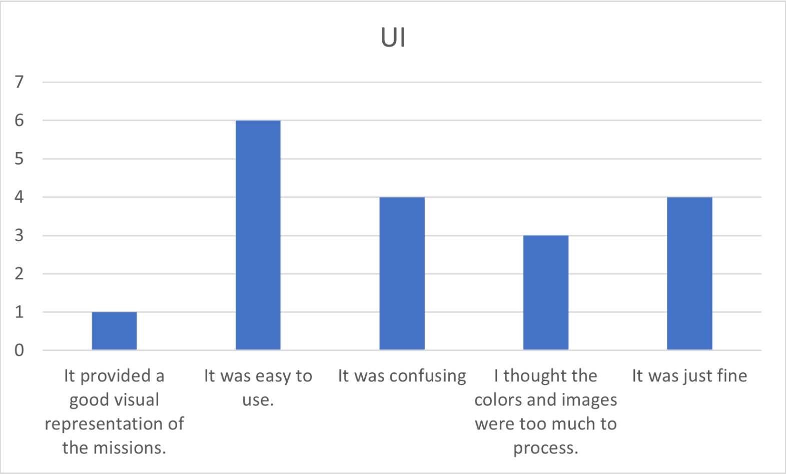


Figure 7.36: UI : Students

Asking about how many roles and missions were played by the students, can show if there were attracted to the game or not. Figures 7.37 and 7.38 show the results for these questions.

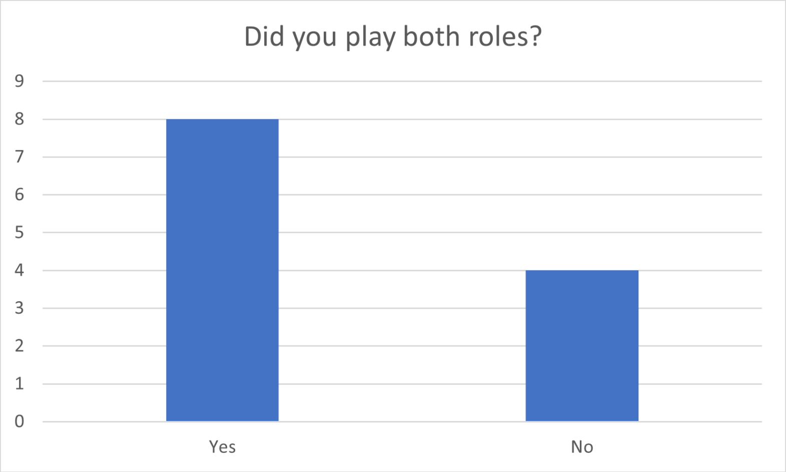


Figure 7.37: Roles played : Students

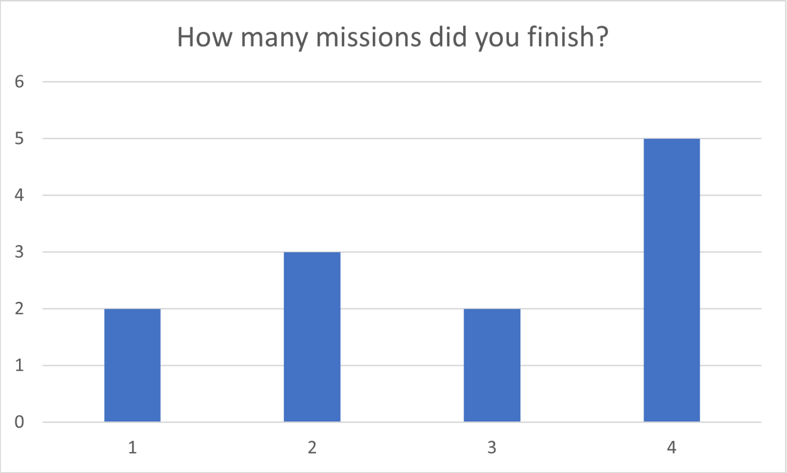


Figure 7.38: Missions played : Students

7.6 Optional questions

In both questionnaires, the participants were given a few optional open-ended questions, where they can express themselves better and elaborate on their opinions.

7.6.1 Professors

Additional optional questions were added to this evaluation, asking about which level (as the year of study) of cyber security bachelor students they think the game suits best, and what type of students/players they think the game suits the best, The given choices were the same as those given to the students in the Pre-game questionnaire, but with the naming of each type, as follows:

1. The Achiever: all about points and status.
2. The Explorer: wants to see new things and discover new secrets.
3. The Socializer: experiences fun in games through interaction with other players.
4. The Killer: wants to see other people lose.

Finally, the following optional open-ending questions were given to the participants to elaborate on their opinions:

- Which aspect/s in the game promotes or prevents active learning?
- What can be changed to make the game more useful?
- What can be improved/changed?

The participants unanimously agreed that the game would suit best the Explorer player/student, who wants to see new things and discover new secrets. As for the level of study, the answers varied between the first, second, and third years, with the majority choosing the second year as shown in figure 7.39.

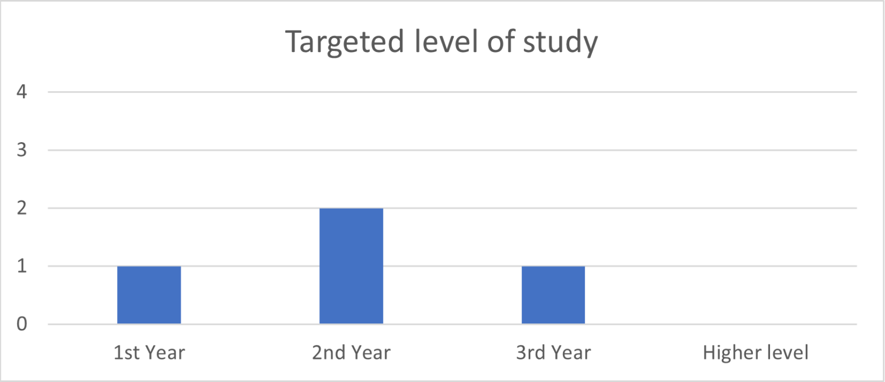


Figure 7.39: Level of study

Only one of the participants answered the optional open-ended questions as follows:

1. Which aspect/s in the game promotes or prevents active learning?
   The game being scenario-based promotes the players toward active participation.
2. What can be changed to make it more useful?
   Making the game more dynamic and open, by changing the scenario path based on the player's choices in the game.

The feedback received from the professor outside the questionnaire form can be summarized in the following points:

- **Positive**:
  1. The game is quite engaging and the role-playing elements are well-chosen.
  2. The game teaches the strategies for both, blue and red teams in a good way.
  3. The game is easy to use, and intuitive
- **What can be improved**:
  1. The user interface is primitive and lacks animation and iconography.
  2. Limited mobile-readiness.
  3. Element of stress like time could be used.
  4. Some metrics can be added as a confidence reflection, instead of it being self-reported.

7.6.2 Students

In this questionnaire, in addition to the quantitative evaluation questions, the students were given a few optional questions to give qualitative feedback and elaborate on their opinions. Below, the questions and the students' answers are listed.

1. **Which aspect/s in the game promote/s or prevent/s active learning?**
   This question had a variety of answers, some mentioned that the aspects that promoted active learning were visiting the ATT&CK website to find the answers, and some said that they need to either memorize or educate themselves via visiting the website in order to answer by clicking on the correct answer, some mentioned that it would be even more effective if an option was offered where they can write their own answers not just click on pre-defined answers. Some also said that one of these aspects is instant feedback, where they were told why their answer was correct and elaborated that it would be easier if feedback with the correct answer was given in case the answer was incorrect. One last comment was that the hint option and the fact that they did not lose points when asking for help, encouraged his/her decision in seeking help and learn more.

2. **What do you think can be improved in the user interface?**
   The collected feedback for this question mainly focused on the quality of the images and the colors of the interface, many said that the images should be cleaner and that the background colors should be more neutral. Some pointed out some bugs in the interface that were not noticed by the developer, some un-clickable boxes that should be clickable, and a button redirects to the wrong page of the game. The last comment pointed out the need for more clarification for some buttons, instead of just putting Hint on the hint button, there should be "Click here for a hint".

3. **What do you think can be improved in the game to increase both, the fun factor and engaging factor?**
   There was not much feedback for this, one mentioned that offering different types of questions other than just multiple choice questions, could improve the game, another wasn't impressed by the feedback for the incorrect answers, saying that the feedback should be straightforward and without sugar coating the feedback. The last feedback mentioned that the game is fun and engaging.

After collecting all of the previous results from both professors and students, the results will be discussed in the following section.

Chapter 8

Discussion

In an attempt to introduce MITRE ATT&CK simply and entertainingly for cyber security students, a web-based game was designed and developed using the COFELET framework. MITRE ATT&CK framework was very helpful in presenting information for the content of the game, whether it is an adversary group, malware, campaign, tactics, techniques, or mitigation, but it lacked information about what should not be used in case of these attacks. This kind of information would have helped to reduce the time and effort of collecting such knowledge, but this issue was solved with the help of a cybersecurity expert.
As for the implementation, the learning curve of Django was steep and fast, and the implementation was the most enjoyable phase of the project.
The evaluation phase was successful, the professors and the students were cooperative, and good responses were collected from both sides, but more responses, especially from the professors' side, would have added more value to the results. The process of this thesis overall added a great knowledge to the author, in the educational serious games field, and the web development area, in addition to some very interesting collateral knowledge in the cyber security field. Below, the game with its different components will be discussed. This part shows that dividing the game's components into three activities does not mean that the components only belong to the category they were mentioned in, many components can overlap between more than one category. For instance, having multiple scenarios, can be considered as a learning component, where the game considered adapting to more than one subject, and as a gaming component, to add the fun and engagement factors for the game. Another example is the scoring technique, where it had an effect in the three activities, as a learning component, by adapting to the needs and knowledge of level for each player, also, as an instructional component, by performing assessment, and finally, as a gaming component, that adds excitement to the game. This chapter is dedicated to discussing the different objectives for the game starting from the learning, then the instructional, and finally the gaming objectives depending on the results of the evaluation of these aspects, and ends by discussing the implications of using the COFELET framework for this thesis, and the limitations of this thesis.

8.1 Learning objectives

This study aimed to investigate the effectiveness of serious games in introducing the ATT&CK framework compared to traditional teaching methods. The fact that all twelve students had prior knowledge of the framework, made it possible to do the comparison. The comparison was done based on the fun and engagement factors, in addition to the acquired knowledge after playing the game. Eleven out of the twelve students replied that the game was more enjoyable and engaging than the way they were introduced to the framework, and eight out of the twelve replied that they acquired a medium level of knowledge about the framework after playing while eleven answered in the Pre-game questionnaire that their level of knowledge was simple. This shows that the game was efficient and successful in both factors of the comparison. The same applies to the active learning promotion, where all professors and students except one, either agreed or highly agreed that the game delivered this, and replied with much feedback to justify their opinion. Additionally, all professors and 10 out of the twelve students agreed that the game offered good training for the students, where scenarios covered different fields in the ATT&CK framework, with the Hint option that can encourage the students to browse the framework to find the answers, which leads to them being more familiar with it. For that, the majority of the professors agreed that the game would be a successful secondary tool to be used in teaching the ATT&CK framework. These results showed that the game delivered its' learning objectives successfully, and its time to discuss whether it delivers the instructional objectives in the nest section.

8.2 Instructional objectives

Since the instructional components are essential to facilitate the learning process, it was important to consider them in the game design, and since the game did not involve an instructor into it, the developer carefully added the instructional components into the game to support the students with the help they could use. That is why a tutorial was added before the game starts, to make sure that the game's objectives and confidence factor are understood, and the vast majority of the participants agreed that it was helpful.

Using the characters in the game did not have the desired instructional effect, but it was found helpful by many students, and professors.

Using formative assessment in the game was applied by using the confidence factor. It was thought that the used scoring technique would decrease the stress level of the students, on which some of the students and the majority of the professors agreed, so they will not be afraid to use the hint and visit the website to look for answers, "which is the main purpose of the game!" While at the same, increasing the excitement of the game, by offering a higher award for those who do not use the hint, which was noticed to be working, when the majority answered that they felt excited and challenged when they chose not to use the Hint. The "Not

Sure" option did not seem to attract the students, but it was helpful for some. This may be due to the nature of the players, where the majority preferred Racing, Competitive, Adventure, and Fighting game genres. This tells that the players did not like to play safe, instead, they liked to be challenged.
As for the feedback, the idea was to offer instant feedback to the player, believing that giving feedback at the end of the game would result in the player losing track of the correct/incorrect answers. The instant feedback is intended to give information about each question individually, to give the player the chance to focus on one question at a time, and get as much knowledge from the feedback as possible, also to affect the player's decision for the next questions, knowing that the player was falsely confident, can make him/her more careful, and knowing that he/she was correct can result in more confident answers in the next questions. The information in the feedback was found useful and informative by all students and by the majority of the professors, but the majority of participants were neutral when asked about the effect of it on the decision. The author believes that the students did not respond to this feature for the same reason they did not respond to the "Not Sure" feature and that the professors were not given a sufficient explanation for this feature, since only one statement was offered to them regarding this point.

8.3 Gaming objectives

The game was designed to be a user interface for a scenario-based game that has different roles and multiple scenarios for each role. This was decided to add fun and engaging factors in the game, so it offers the students a different environment for learning than the traditional one. While some students described having different roles and multiple scenarios as fun, and others as engaging, the majority described this as both fun and engaging. At the same time, the professors agreed that different roles and scenarios made the game fun and motivating. This shows that the game successfully fulfilled its' fun requirements. But when it comes to the UI, it was found that it had many limitations. Although many described it as easy to use, the colors and images were found to be confusing and too much to process, and overall it needed more cleaning and adjusting. Clearly, more focus should have been given to the design of the UI to present all the previous components in a better, more attractive way.

8.4 Using COFELET

Using COFELET was very helpful in designing and evaluating the game. The idea applied from the activity theory for dividing the game's components into its' three components, facilitated the developer's work in discovering what are the important components that should be taken into consideration when developing and evaluating an educational serious game. Since the author is an applied computer science student and had no cyber security knowledge or experience, COFELET was found highly efficient by introducing some of the important cyber security theories and frameworks, this helped in deciding on what basis the game can be built. COFELET supported dividing the scenarios into smaller tasks, which was thought to make it easier to focus on learning about each one individually. Most students agreed that this in fact helped them to focus on each one individually. At the same time, the adaption of CKC by COFELET aided the creation of the scenarios, which was thought to help the players with not just learning about each question individually, but as a part of a whole process, where each question is just a part of it. The evaluation results showed that the game successfully offered that, where nine out of the twelve students agreed that they were better able to understand the attack as a whole. As adaptability is an important feature in a COFELET game, the developer made sure to apply it in the game where it had its' effect, not only by increasing the fun and engaging factors by the roles and scenarios, as mentioned earlier, but also by adapting to the player's preferences and needs by the scoring technique and confidence factor, where the students who prefer to be challenged can discard the Hint, and those who like to play safe, and don't have enough knowledge for the game can use it. In the Pre-game questionnaire, the students described themselves with many different types of players, and it was shown by the Post-game questionnaire that the majority played both roles and more than one scenario, and since it was up to them to choose which roles to play, or how many scenarios to finish, this shows that the game can be played and enjoyed by many types of players, and is not limited to a specific player's type.

8.5 Limitation

The evaluation phase showed that the game has some limitations that affected the gaming experience for the players. The main limitation of the game was the user interface, to which most of the negative feedback belonged. Also, the static nature of the game, where the game's flow was fixed, and, and not dynamic with the player's decision in the game. and finally, the single question type offered to the game, where only multiple choice questions were offered.

The limitation that was faced by the author, is the limited response for the evaluation, which the testing groups, especially from the professors' side were found relatively small.

Chapter 9

Conclusion

This thesis has discussed the efficiency of serious games in introducing MITRE ATT&CK to cybersecurity students, by developing a web-based serious game based on the COFELET framework, in an attempt to overcome some of the challenges that face cybersecurity education. Evaluation data were collected from students and professors, through a Post-game questionnaire for professors, and Pre-Post-game questionnaires for students, covering the three main serious games activities produces by the activity theory. From the work that has been done in this thesis, the following research questions were answered as follows:

- How effective is using the COFELET framework in designing a cyber security serious game?
  From the developer's perspective, using the COFELET framework was effective, by offering the important components and features to be considered in a cyber security serious game. As for the game, the results showed that applying COFELET's methodologies in creating the game had benefits in increasing the learning and instructional aspects of the game, where the players had a better understanding of the whole CKC process, and at the same time, focusing on the individual parts of the CKC, while they were guided through the game by the added instructional components.
- How effective is using serious games to introduce the MITRE ATT&CK to students?
  The results showed that the students enjoyed learning about ATT&CK through the game, more than the traditional methods, with better understanding and more knowledge about it from the game. Also, the professors would agree to use the game as a secondary tool for education. This answers the second question, where it shows that the game was effective in delivering its' learning and instructional purposes, but it needed more work on the gaming part.

In conclusion, it can be demonstrated that, when knowledge is presented in a new fun, and engaging way like a game, in which field-related methodologies are combined with educational theories, students will gain a better learning experi-

ence with good learning outcomes. This supports the hypothesis, that a COFELET serious game is indeed an effective approach for introducing the MITRE ATT&CK framework to university cyber security students.
The author is aware that strong support for the hypothesis needs more testing that involves both the control group and testing group, with a larger testing sample, but due to the limited resources and time, the support of the hypothesis was based only on the evaluation from the testing groups.

As a future work, and to overcome the limitations found in the game, the author is planning to collaborate with a user experience expert, to get familiar with the design principles and models, in order to create a better user interface. the author is planning to collaborate with professors as well, to add more scenarios, that support the materials in their teaching courses, Although the game's evaluation gave good feedback, a larger testing sample, either from professors or students would have added more value with more accurate results. For that reason, the author is planning to pursue more testing with larger testing samples, and conduct the evaluation involving a control group, for stronger support of the hypothesis.

Bibliography

[1] M. Hendrix, A. Al-Sherbaz and B. Victoria, 'Game based cyber security training: Are serious games suitable for cyber security training?' *International Journal of Serious Games*, vol. 3, no. 1, 2016.

[2] M. N. Katsantonis, I. Mavridis and D. Gritzalis, 'Design and evaluation of cofelet-based approaches for cyber security learning and training,' *Computers & Security*, vol. 105, p. 102 263, 2021.

[3] K. Starcher and D. Proffitt, 'Encouraging students to read: What professors are (and aren't) doing about it.,' *International Journal of Teaching and Learning in Higher Education*, vol. 23, no. 3, pp. 396–407, 2011.

[4] T. Anastasiadis, G. Lampropoulos and K. Siakas, 'Digital game-based learning and serious games in education,' *International Journal of Advances in Scientific Research and Engineering*, vol. 4, no. 12, pp. 139–144, 2018.

[5] C. Jordan, M. Knapp, D. Mitchell, M. Claypool and K. Fisler, 'Countermeasures: A game for teaching computer security,' in *2011 10th Annual Workshop on Network and Systems Support for Games*, IEEE, 2011, pp. 1–6.

[6] M. Dark and J. Mirkovic, 'Evaluation theory and practice applied to cybersecurity education,' *IEEE Security & Privacy*, vol. 13, no. 2, pp. 75–80, 2015.

[7] https://attack.mitre.org/, Accessed on Dec/14/2022.

[8] S. Sharma, *See the evolution of the mitre attck framework from 2015 to now*, https://d3security.com/blog/see-the-evolution-of-the-mitre-attack-framework-from-2015-to-now/, Accessed on Dec/14/2022, Apr. 2022.

[9] F. Laamarti, M. Eid and A. El Saddik, 'An overview of serious games,' *International Journal of Computer Games Technology*, vol. 2014, 2014.

[10] Y. Zhonggen, 'A meta-analysis of use of serious games in education over a decade,' *International Journal of Computer Games Technology*, vol. 2019, 2019.

[11] M. Katsantonis and I. Mavridis, 'Evaluation of hacklearn cofelet game user experience for cybersecurity education,' *International Journal of Serious Games*, vol. 8, no. 3, pp. 3–24, 2021.

[12] M. Qian and K. R. Clark, 'Game-based learning and 21st century skills: A review of recent research,' *Computers in human behavior*, vol. 63, pp. 50–58, 2016.

[13] N. M. Katsantonis, I. Kotini, P. Fouliras and I. Mavridis, 'Conceptual framework for developing cyber security serious games,' in *2019 IEEE Global Engineering Education Conference (EDUCON)*, IEEE, 2019, pp. 872–881.

[14] K. Thakur, M. Qiu, K. Gai and M. L. Ali, 'An investigation on cyber security threats and security models,' in *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing*, IEEE, 2015, pp. 307–311.

[15] W. Xiong, E. Legrand, O. Åberg and R. Lagerström, 'Cyber security threat modeling based on the mitre enterprise att&ck matrix,' *Software and Systems Modeling*, vol. 21, no. 1, pp. 157–177, 2022.

[16] A. Georgiadou, S. Mouzakitis and D. Askounis, 'Assessing mitre att&ck risk using a cyber-security culture framework,' *Sensors*, vol. 21, no. 9, p. 3267, 2021.

[17] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington and C. B. Thomas, 'Mitre att&ck: Design and philosophy,'

[18] MITRE, *Phishing*, https://attack.mitre.org/techniques/T1566/, Accessed on Dec/14/2022.

[19] MITRE, *External remote services*, https://attack.mitre.org/techniques/T1133/, Accessed on Dec/14/2022.

[20] A. De Gloria, F. Bellotti and R. Berta, 'Serious games for education and training,' *International Journal of Serious Games*, vol. 1, no. 1, 2014.

[21] V. Wattanasoontorn, I. Boada, R. Garcıa and M. Sbert, 'Serious games for health,' *Entertainment Computing*, vol. 4, no. 4, pp. 231–247, 2013.

[22] P. D. da Silva Simões and C. G. I. Ferreira, 'Military war games edutainment,' in *2011 IEEE 1st International Conference on Serious Games and Applications for Health (SeGAH)*, IEEE, 2011, pp. 1–7.

[23] K. S. Hale and K. M. Stanney, *Handbook of virtual environments: Design, implementation, and applications*. CRC Press, 2014.

[24] A. Nikolova and V. Georgiev, 'Using serious games in e-learning for kids,' in *INTED2021 Proceedings. 15th International Technology, Education and Development Conference*, 2021, pp. 621–625.

[25] D. H. Jonassen and L. Rohrer-Murphy, 'Activity theory as a framework for designing constructivist learning environments,' *Educational technology research and development*, vol. 47, no. 1, pp. 61–79, 1999.

[26] MITRE, *Mitre capec*, https://capec.mitre.org/, Accessed on Dec/14/2022.

[27] B. SOARE, *The cyber kill chain (ckc) explained*, https://heimdalsecurity.com/blog/cyber-kill-chain-model/, Accessed on Dec/14/2022, Jun. 2022.

[28] R. Petersen, D. Santos, K. Wetzel, M. Smith, G. Witte *et al.*, 'Workforce framework for cybersecurity (nice framework),' 2020.

[29] A.-A. Darrow, 'Adaptations in the classroom: Accommodations and modifications, part 2,' *General Music Today*, vol. 21, no. 3, pp. 32–34, 2008.

[30] M. Vandewaetere, F. Cornillie, G. Clarebout and P. Desmet, 'Adaptivity in educational games: Including player and gameplay characteristics.,' *International Journal of Higher Education*, vol. 2, no. 2, pp. 106–114, 2013.

[31] M. B. Carvalho, F. Bellotti, R. Berta, A. De Gloria, C. I. Sedano, J. B. Hauge, J. Hu and M. Rauterberg, 'An activity theory-based model for serious games analysis and conceptual design,' *Computers & education*, vol. 87, pp. 166–181, 2015.

[32] S. Hart, A. Margheri, F. Paci and V. Sassone, 'Riskio: A serious game for cyber security awareness and education,' *Computers & Security*, vol. 95, p. 101 827, 2020.

[33] M. M. Yamin, B. Katt and M. Nowostawski, 'Serious games as a tool to model attack and defense scenarios for cyber-security exercises,' *Computers & Security*, vol. 110, p. 102 450, 2021.

[34] M. Katsantonis and I. Mavridis, 'Ontology-based modelling for cyber security e-learning and training,' in *International Conference on Web-Based Learning*, Springer, 2019, pp. 15–27.

[35] M. Thompson and C. Irvine, 'Active learning with the {cyberciege} video game,' in *4th Workshop on Cyber Security Experimentation and Test (CSET 11)*, 2011.

[36] H. Gore, R. K. Singh, A. Singh, A. P. Singh, M. Shabaz, B. K. Singh and V. Jagota, 'Django: Web development simple & fast,' *Annals of the Romanian Society for Cell Biology*, vol. 25, no. 6, pp. 4576–4585, 2021.

[37] D. D. Dixson and F. C. Worrell, 'Formative and summative assessment in the classroom,' *Theory into practice*, vol. 55, no. 2, pp. 153–159, 2016.

[38] G. Wiggins, *Educative Assessment. Designing Assessments To Inform and Improve Student Performance.* ERIC, 1998.

[39] S. McCallum, 'Game design for computer science education,' *Gjøvik University College*, vol. 18, 2010.

[40] T. Capermint, *Unity 3d vs html5 – which is the best for game development?* https://www.capermint.com/blog/unity-3d-vs-html5-game-development/, Accessed on Dec/14/2022.

[41] J. BRAINS, *Jetbrains developer's survey*, https://www.jetbrains.com/lp/devecosystem-2021/python/, Accessed on Dec/14/2022, 2021.

[42] Y. Nader, *What is django? advantages and disadvantages*, https://hackr.io/blog/what-is-django-advantages-and-disadvantages-of-using-django, Accessed on Dec/14/2022, Mar. 2022.

[43] O. KERR, 'Investigating the most understandable programming language for beginners,'

[44] MITRE, *Apt3 group*, https://attack.mitre.org/groups/G0022/, Accessed on Dec/14/2022.

[45] MITRE, *Sandworm group*, https://attack.mitre.org/groups/G0034/, Accessed on Dec/14/2022.

[46] MITRE, *Stealth mango malware*, https://attack.mitre.org/software/S0328/, Accessed on Dec/14/2022.

[47] MITRE, *Funnydream campaign*, https://attack.mitre.org/campaigns/C0007/, Accessed on Dec/14/2022.

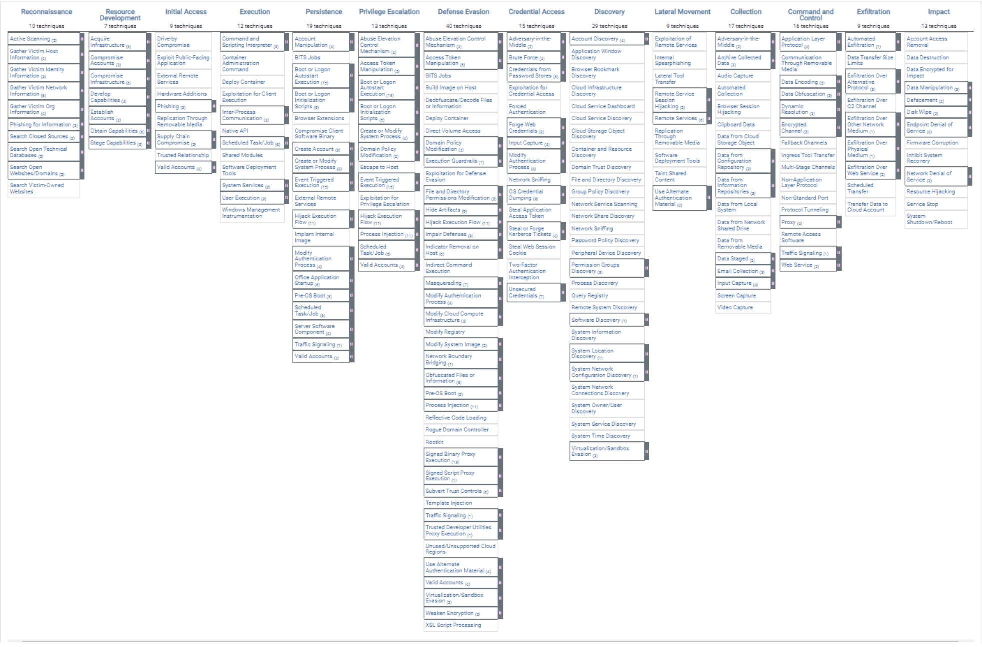
[48] '5-point likert scale,' in *Handbook of Disease Burdens and Quality of Life Measures*, V. R. Preedy and R. R. Watson, Eds. New York, NY: Springer New York, 2010, pp. 4288–4288, ISBN: 978-0-387-78665-0. DOI: `10.1007/978-0-387-78665-0_6363`. [Online]. Available: `https://doi.org/10.1007/978-0-387-78665-0_6363`.

[49] J. Tuunanen and J. Hamari, 'Meta-synthesis of player typologies,' in *Proceedings of Nordic Digra 2012 Conference: Games in Culture and Society, Tampere, Finland*, 2012.

[50] MITRE, *Mitre att@ck enterprise matrix*, `https://attack.mitre.org/versions/v10/matrices/enterprise/`, note = Accessed on Dec/14/2022.

Appendix A

Enterprise Matrix



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	40 techniques
Active Scanning (3)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (15)	Boot or Logon Autostart Execution (15)	BITS Jobs
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (6)	Create Account (3)	Escape to Host	Direct Volume Access
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Domain Policy Modification (2)
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Execution Guardrails (1)
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (11)	Exploitation for Defense Evasion
			User Execution (3)	Hijack Execution Flow (11)	Process Injection (11)	File and Directory Permissions Modification (2)
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (6)	Hide Artifacts (9)
				Modify Authentication Process (4)	Valid Accounts (4)	Hijack Execution Flow (11)
				Office Application Startup (6)		Impair Defenses (9)
				Pre-OS Boot (5)		Indicator Removal on Host (6)
				Scheduled Task/Job (6)		Indirect Command Execution
				Server Software Component (4)		Masquerading (7)
				Traffic Signaling (1)		Modify Authentication Process (4)
				Valid Accounts (4)		Modify Cloud Compute Infrastructure (4)
						Modify Registry
						Modify System Image (2)
						Network Boundary Bridging (1)
						Obfuscated Files or Information (6)
						Pre-OS Boot (5)
						Process Injection (11)
						Reflective Code Loading
						Rogue Domain Controller
						Rootkit
						Signed Binary Proxy Execution (13)
						Signed Script Proxy Execution (1)
						Subvert Trust Controls (6)
						Template Injection
						Traffic Signaling (1)
						Trusted Developer Utilities Proxy Execution (1)
						Unused/Unsupported Cloud Regions
						Use Alternate Authentication Material (4)
						Valid Accounts (4)
						Virtualization/Sandbox Evasion (3)
						Weaken Encryption (2)
						XSL Script Processing

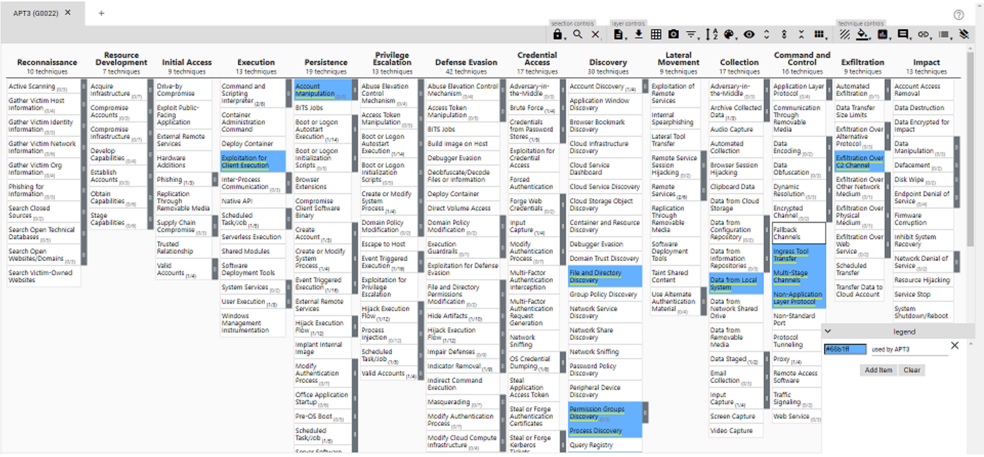
Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
15 techniques	29 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Modify Authentication Process (4)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Network Sniffing	Domain Trust Discovery	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
OS Credential Dumping (8)	File and Directory Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
Steal Application Access Token	Group Policy Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
Steal or Forge Kerberos Tickets (4)	Network Service Scanning		Data from Removable Media	Protocol Tunneling		Service Stop
Steal Web Session Cookie	Network Share Discovery		Data Staged (2)	Proxy (4)		System Shutdown/Reboot
Two-Factor Authentication Interception	Network Sniffing		Email Collection (3)	Remote Access Software		
Unsecured Credentials (7)	Password Policy Discovery		Input Capture (4)	Traffic Signaling (1)		
	Peripheral Device Discovery		Screen Capture	Web Service (3)		
	Permission Groups Discovery (3)		Video Capture			
	Process Discovery					
	Query Registry					
	Remote System Discovery					
	Software Discovery (1)					
	System Information Discovery					
	System Location Discovery (1)					
	System Network Configuration Discovery (1)					
	System Network Connections Discovery					
	System Owner/User Discovery					
	System Service Discovery					
	System Time Discovery					
	Virtualization/Sandbox Evasion (3)					

Figure A.1: MITRE ATT&CK Enterprise Matrix
[50]

For better vision, follow this link: `https://attack.mitre.org/matrices/enterprise/`

Appendix B

ATT&CK navigator for APT3



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/3)	Acquire Infrastructure (0/7)	Drive-by Compromise	Command and Scripting Interpreter (2/8)	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)	Account Discovery (1/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (1/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (1/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (1/14)	Boot or Logon Autostart Execution (1/14)	BITS Jobs	Credentials from Password Stores (1/5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/3)	Phishing (1/3)	Inter-Process Communication (0/3)	Browser Extensions	Create or Modify System Process (1/4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (2/6)	Browser Session Hijacking	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Stage Capabilities (0/6)	Supply Chain Compromise (0/3)	Scheduled Task/Job (1/5)	Create Account (1/3)	Escape to Host	Deploy Container	Input Capture (1/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (1/4)	Event Triggered Execution (1/16)	Direct Volume Access	Modify Authentication Process (0/7)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (0/3)		Valid Accounts (1/4)	Shared Modules	Event Triggered Execution (1/16)	Exploitation for Privilege Escalation	Domain Policy Modification (0/2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Hijack Execution Flow (1/12)	Execution Guardrails (0/1)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (0/2)
			System Services (0/2)	Hijack Execution Flow (1/12)	Process Injection (0/12)	Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			User Execution (1/3)	Implant Internal Image	Scheduled Task/Job (1/5)	File and Directory Permissions Modification (0/2)	OS Credential Dumping (1/8)	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
			Windows Management Instrumentation	Modify Authentication Process (0/7)	Valid Accounts (1/4)	Hide Artifacts (1/10)	Steal Application Access Token	Network Service Discovery		Data Staged (1/2)	Proxy (1/4)		System Shutdown/Reboot
				Office Application Startup (0/6)		Hijack Execution Flow (1/12)	Steal or Forge Authentication Certificates	Network Share Discovery		Email Collection (0/3)	Remote Access Software		
				Pre-OS Boot (0/5)		Impair Defenses (0/9)	Steal or Forge Kerberos Tickets	Network Sniffing		Input Capture (1/4)	Traffic Signaling (0/2)		
				Scheduled Task/Job (1/5)		Indicator Removal (1/9)		Password Policy Discovery		Screen Capture	Web Service (0/3)		
				Server Software		Indirect Command Execution		Peripheral Device Discovery		Video Capture			
						Masquerading (0/7)		Permission Groups Discovery (0/3)					
						Modify Authentication Process (0/7)		Process Discovery					
						Modify Cloud Compute Infrastructure (0/4)		Query Registry					

#66b1ff used by APT3

Figure B.1: ATT&CK navigator for APT3

For better vision, follow this link: `https://macsgame.herokuapp.com/navigator/`

Appendix C

Pre game questionnaire for students

Report from ‘Pre-Game’

Collected results per. 26. November 2022 13:42

- Delivered replies: **12**
- Commenced replies: **0**
- Number of sent invitations: **0**

With text answers

Have you heard about MITRE ATT&CK framework before? *

Answer	Number of	Percentage	
Yes	12	**100%**	
No	0	**0%**	

If Yes
Were you taught the MITRE ATT&CK framework in one of your courses? *

Answer	Number of	Percentage	
Yes	9	**75%**	
No	3	**25%**	

How can you describe your experience in learning the ATT&CK framework in a class?

Answer	Number of	Percentage	
Inefficient and unsatisfactory	0	**0%**	
I don't know	6	**50%**	
Efficient and satisfactory	6	**50%**	

How would you describe your Knowledge of the ATT&CK framework? *

Answer	Number of	Percentage	
None	0	**0%**	
Simple	11	**91.7%**	
Medium	1	**8.3%**	
Very good	0	**0%**	
Expert	0	**0%**	

At which level are you in your study? *

Answer	Number of	Percentage	
1st Year	0	**0%**	
2nd year	12	**100%**	
3rd Year	0	**0%**	
Higher level	0	**0%**	

Do you play video games?

Answer	Number of	Percentage	
Yes	9	**75%**	
No	3	**25%**	

If yes:
What type of video game player do you consider yourself?

You can choose more than one.

Answer	Number of	Percentage	
It is all about points and status for me	5	41.7%	
I like to see new things and discover new secrets	8	66.7%	
I experience fun in games through interaction with other players	7	58.3%	
I like to see other people lose	4	33.3%	

What type (Genre) of video games do you prefer to play?

You can choose more than one.

Answer	Number of	Percentage	
Strategy Games	10	83.3%	
Role-Playing Games	6	50%	
Educational game	1	8.3%	
Other	6	50%	

What other game Genre do you prefer to play?

- FPS - games
- Racing, FPS, competitive
- FPS-games
- Adventure, competitive, racing, FPS, fighting, JRPG, puzzle, ETC
- Grand Strategy
- FPS (Fist Person Shooter), MMORPG (WoW) and Open World
- MOBA, MMO... and whatever Minecraft is

See recent changes in Nettskjema

Appendix D

Post-game questionnaire for students

Report from ‘ATT&CK To Defend student Feedback’

Collected results per. 26. November 2022 13:39

- Delivered replies: **12**
- Commenced replies: **0**
- Number of sent invitations: **0**

With text answers

Post-Game Questionnaire

1- The game promotes active learning. *

Active learning: engaging students as active participants in their learning during class time instead of being passive participants taking notes and watching lectures

Answer	Number of	Percentage	
Highly disagree	0	**0%**	
Disagree	0	**0%**	
Neutral	1	**8.3%**	
Agree	6	**50%**	
Highly agree	5	**41.7%**	

2- Which aspect/s in the game promote/s or prevent/s active learning?

Optional

- You have to check the Mitre&Attack website for questions you are not sure about and actually understand how to use the website.
- Both the answering and information-checking aspects of the game
- By being represented with a question and then having to figure out the correct answer, either by an educated guess or to actually visit the MITRE site, promotes active learning.
- Helps in memorizing techniques
- Promotes active learning through clickable links and s button with require you to have some knowleadge about the subject or to learn about it. It would be more effective to have mix of clickable and writeable awnser, since writing the write awnser requires more knowledge.
- Promote: When the player has answered correctly there as always given an explanation on why that is correct, which is good! Prevent: When the player has answered incorrectly the correct answer should be displayed, instead of giving the player the option to read more about it. This approach gives the correct answer to the player without them having to "go the extra mile" and click on the button to read more about it. Players are lazy:)
- I think there also should be a "info" option to give the user a better understanding of the different options. But was a good game.
- This would be brilliant if there was a lecture or something similar beforehand that covered the corriculum.
- It is nice that there is an option to get a hint where you can read up on the problem. And that wanting a hint isnt a "punishment" for not knowing, but encourage you to learn more!

3- The game provided me with good cyber security “knowledge and skills” practice. *

Meaning: The game helped you to practice your cyber security skills, such as mitigating attacks, knowing the steps of an attack, and performing an attack, resulting in improving these skills.

Answer	Number of	Percentage	
Highly disagree	0	**0%**	
Disagree	0	**0%**	
Neutral	2	**16.7%**	
Agree	7	**58.3%**	
Highly agree	3	**25%**	

4- I found the choice “Not Sure” helpful to continue the game. *

Answer	Number of	Percentage	
Highly disagree	0	**0%**	
Disagree	1	**8.3%**	
Neutral	5	**41.7%**	
Agree	4	**33.3%**	

Answer	Number of	Percentage	
Highly agree	2	16.7%	

5- Redirecting to the ATT&CK webpage helped me with finding the correct answer. *

Answer	Number of	Percentage	
Highly disagree	0	0%	
Disagree	0	0%	
Neutral	2	16.7%	
Agree	4	33.3%	
Highly agree	6	50%	

6- Redirecting to the ATT&CK webpage helped me with getting familiar with the ATT&CK framework *

Answer	Number of	Percentage	
Highly disagree	0	0%	
Disagree	0	0%	
Neutral	3	25%	
Agree	5	41.7%	
Highly agree	4	33.3%	

7- The 2 points award for being confident encouraged me to answer without a hint. *

Answer	Number of	Percentage	
Highly disagree	0	0%	
Disagree	0	0%	
Neutral	3	25%	
Agree	3	25%	
Highly agree	6	50%	

8- The 2 points deduction for being falsely confident encouraged me to take a hint. *

Answer	Number of	Percentage	
Highly disagree	1	8.3%	
Disagree	1	8.3%	
Neutral	4	33.3%	
Agree	5	41.7%	
Highly agree	1	8.3%	

9- The instance feedback affected my decision in choosing hints for the next missions. *

Answer	Number of	Percentage	
Highly Disagree	0	0%	
Disagree	2	16.7%	
Neutral	9	75%	
Agree	1	8.3%	
Highly agree	0	0%	

10- I found the information given in the feedback useful and informative. *

Answer	Number of	Percentage	
Highly disagree	0	0%	
Disagree	0	0%	

Answer	Number of	Percentage
I don't know	0	0%
Agree	12	100%
Highly agree	0	0%

11- I found the tutorial helpful in understanding the game’s objectives. *

Answer	Number of	Percentage
Highly disagree	0	0%
Disagree	1	8.3%
Neutral	1	8.3%
Agree	9	75%
Highly agree	1	8.3%

12- I found the scoring description at the beginning of the game helpful in understanding the confidence factor. *

Answer	Number of	Percentage
Highly disagree	0	0%
Disagree	1	8.3%
Neutral	2	16.7%
Agree	8	66.7%
Highly agree	1	8.3%

13- I found the game’s characters (Alma & Alti) helpful in understanding the mission’s goal. *

Answer	Number of	Percentage
Highly disagree	1	8.3%
Disagree	1	8.3%
Neutral	3	25%
Agree	4	33.3%
Highly agree	3	25%

14- How would you describe your feeling when you chose "Very confident"? *

Answer	Number of	Percentage
stressed	2	16.7%
exciting and challenging.	8	66.7%
Neutral	2	16.7%

15- How would you describe your feeling when you chose "Not confident"? *

Answer	Number of	Percentage
stressed	3	25%
Safe and relax	2	16.7%
Neutral	7	58.3%

16- The feedback helped me not to be too confident for the next missions. *

Answer	Number of	Percentage
Highly disagree	1	8.3%
Disagree	1	8.3%
Neutral	7	58.3%

Answer	Number of	Percentage	
Agree	3	**25%**	
Highly agree	0	**0%**	

17- The scoring technique was fair. *

Answer	Number of	Percentage	
Highly disagree	0	**0%**	
Disagree	0	**0%**	
Neutral	1	**8.3%**	
Agree	11	**91.7%**	
Highly agree	0	**0%**	

18- I found the ATT&CK website overwhilming. *

Answer	Number of	Percentage	
Highly disagree	1	**8.3%**	
Disagree	5	**41.7%**	
Neutral	4	**33.3%**	
Agree	1	**8.3%**	
Highly agree	1	**8.3%**	

19- How would you describe having multiple roles for playing the game *

Answer	Number of	Percentage	
Fun & Engaging	7	**58.3%**	
Fun	3	**25%**	
Engaging	1	**8.3%**	
None	1	**8.3%**	

20- How would you describe having different scenarios for playing the game *

Answer	Number of	Percentage	
Fun & Engaging	8	**66.7%**	
Fun	2	**16.7%**	
Engaging	2	**16.7%**	
None	0	**0%**	

21- Dividing the missions into several tasks, made it easier for me to focus on learning about each one. *

Answer	Number of	Percentage	
Highly disagree	0	**0%**	
Disagree	0	**0%**	
Neutral	2	**16.7%**	
Agree	5	**41.7%**	
Highly agree	5	**41.7%**	

22. By designing the scenarios to include every stage of an attack, from the first to the final, I was better able to understand the attack as a whole. *

Answer	Number of	Percentage	
Highly disagree	0	**0%**	
Disagree	1	**8.3%**	

Answer	Number of	Percentage
Neutral	2	16.7%
Agree	6	50%
Highly agree	3	25%

23- How would you describe the user interface *

You can choose more than one.

Answer	Number of	Percentage
It provided a good visual representation of the missions.	1	8.3%
It was easy to use.	6	50%
It was confusing	4	33.3%
I thought the colors and images were too much to process.	3	25%
It was just fine	4	33.3%

24- What do you think can be improved in the user interface?

Optional

- It looks a bit old
- Have a more clean interface. The pictures were low resolution and the background colors and foreground characters often blended, making them stand out more than they should. Instead of just saying hint on the hint button, you could have it say e.g "click here for a hint". It wasn't clear to me that I had to click it to get a hint, I thought the hint button didn't work.
- Leaves a lot to be desired
- Cleaner og clearer images. a more neutral background so its not so distrackting. Alot of the boxes locked clickable even though it was not. by using different colors hand hues on the clickable vs non-clickable button would suggest it reacts differently.
- The very first question: i was confused that i could not choose an answer before i had indicated my level of confidence. I am unsure if this was declared in the informational text about the confidence level, but in all honesty, i didn't read it all because it was too long for my short concentration span. The images were of poor quality and the colors of the site was a little bit overwhelming. The placement of different objects of the site was also questionable. I do know that this is not the finished version, and i think the end product will look more professional, considering this game is still being developed:)
- a little bit of css magic would do a lot, but the layout was alright
- My quit button didnt work for the post-questions even though i got the button, but it leaded me back to the wrong page. I dont know if this is a bug.

25- What do you think can be improved in the game to increase both, the fun factor and engaging factor?

Optional

- Have different type of question, not just clickable multiple choice.
- It is fun and engaging!
- When you have wrong, tell me. Dont butter it up by saying "yes it is correct, but not in this case"...like, i was correct? or not?

26- How would you describe the level of knowledge you gained about the ATT&CK framework after playing the game? *

Answer	Number of	Percentage
None	1	8.3%
Low	3	25%
Medium	8	66.7%
High	0	0%

27- How enjoyable and engaging is it to learn about the ATT&CK framework through the game, compared to traditional methods used before? *

Answer	Number of	Percentage
I found it less enjoyable and engaging	1	8.3%
I found it more enjoyable and engaging	11	91.7%
Not sure	0	0%

28- Did you try playing with both roles? *

Answer	Number of	Percentage
Yes	8	66.7%
No	4	33.3%

29- How many missions did you finish? *

Answer	Number of	Percentage	
1	2	**16.7%**	
2	3	**25%**	
3	2	**16.7%**	
4	5	**41.7%**	

30- How often did you use the hint to visit the ATT&CK framework? *

Answer	Number of	Percentage	
I did not use any hint	4	**33.3%**	
1-5	4	**33.3%**	
6-10	3	**25%**	
11-15	1	**8.3%**	
More	0	**0%**	

See recent changes in Nettskjema

Appendix E

Post-game questionnaire for Professors

Report from ‘ATT&CK To Defend feedback’

Collected results per. 26. November 2022 13:42

- Delivered replies: **7**
- Commenced replies: **0**
- Number of sent invitations: **0**

With text answers

1- The game promotes active learning. *

Active learning: engaging students as active participants in their learning during class time instead of being passive participants taking notes and watching lecture

Answer	Number of	Percentage	
Highly disagree	0	**0%**	
Disagree	0	**0%**	
Nutral	0	**0%**	
Agree	3	**75%**	
Highly agree	1	**25%**	

2- Which aspect/s in the game promotes or prevents active learning?

Optional

- The scenario based game is positive towards promoting learners to active participation.

3- The game promotes continuous learning. *

Answer	Number of	Percentage	
Highly disagree	0	**0%**	
Disagree	0	**0%**	
Nutral	1	**25%**	
Agree	3	**75%**	
Highly agree	0	**0%**	

4- The game provides students with good cyber security “knowledge and skills” practice. *

Answer	Number of	Percentage	
Highly disagree	0	**0%**	
Disagree	0	**0%**	
Nutral	0	**0%**	
Agree	4	**100%**	
Highly agree	0	**0%**	

5- The confidence factor would motivate students to use the Hint option and visit the ATT&CK framework *

Answer	Number of	Percentage	
HIghly disagree	0	**0%**	
Disagree	0	**0%**	
Nutral	0	**0%**	
Agree	3	**75%**	
HIghly agree	1	**25%**	

6- The confidence factor increased the game's adaptivity "adapting the options and scoring to the student's level of knowledge" *

Answer	Number of	Percentage	
HIghly disagree	0	0%	
Disagree	0	0%	
Nutral	1	25%	
Agree	2	50%	
HIghly agree	1	25%	

7- The different scenarios increased the game's adaptability "adapted to include scenarios from different domains in ATT&Ck" *

Answer	Number of	Percentage	
Highly disagree	0	0%	
Disagree	0	0%	
Nutral	0	0%	
Agree	3	75%	
Highly agree	1	25%	

8- The game would be a successful secondary tool to be used in teaching the ATT&CK framework *

Answer	Number of	Percentage	
Highly disagree	0	0%	
Disagree	0	0%	
Nutral	1	25%	
Agree	2	50%	
Highly agree	1	25%	

9- The scoring scheme of the game helps to decrease the stress level and result in better learning outcomes. *

(No score deduction when asking for hint)

Answer	Number of	Percentage	
Highly disagree	0	0%	
Disagree	0	0%	
Nutral	1	25%	
Agree	3	75%	
Highly disagree	0	0%	

10- The instance feedback would affect the student's decision in choosing hints for the next missions. *

Answer	Number of	Percentage	
Highly disagree	0	0%	
disagree	0	0%	
Nutral	3	75%	
Agree	0	0%	
Highly agree	1	25%	

11- The information in the feedback was found sufficient and informative. *

Answer	Number of	Percentage	
Highly disagree	0	0%	
Disagree	0	0%	

Answer	Number of	Percentage	
Nutral	1	25%	
Agree	2	50%	
Highly agree	1	25%	

12- The game's tutorial was found useful for understanding the game’s objectives. *

Answer	Number of	Percentage	
Highly disagree	0	0%	
Disagree	0	0%	
Nutral	1	25%	
Agree	3	75%	
Highly agree	0	0%	

13- What can be changed to make it more useful?

Optional

- Making the game more dynamic and open. Means: based on some choices of the learners, the scenario path might change. Making the techniques more detailed and specialized based on a concrete system/confi.

14- Explaining the scoring scheme before starting the game helped with understanding how to play the game.

Answer	Number of	Percentage	
highly disagree	0	0%	
Disagree	0	0%	
Nutral	0	0%	
Agree	1	25%	
Highly agree	3	75%	

15- Using the game’s characters (Alma & Alti) helped with understanding the mission’s goal *

Answer	Number of	Percentage	
Highly disagree	0	0%	
Disagree	0	0%	
Nutral	1	25%	
Agree	3	75%	
Highly agree	0	0%	

16- The different roles and scenarios made the game fun and motivating. *

Answer	Number of	Percentage	
Highly disagree	0	0%	
Disagree	0	0%	
Nutral	0	0%	
Agree	2	50%	
Highly agree	2	50%	

17- The user interface was easy to use *

Answer	Number of	Percentage	
Highly disagree	0	0%	
Disagree	0	0%	
Nutral	1	25%	
Agree	2	50%	

Answer	Number of	Percentage	
Highly agree	1	25%	

18- What can be improved/changed?

Optional

19- What type of students/players do you think the game suits the best?

Optional

Answer	Number of	Percentage	
The Achiever " all about points and status "	0	0%	
The Explorer " wants to see new things and discover new secrets"	4	100%	
The Socializer " experiences fun in games through interaction with other players"	0	0%	
The Killer "wants to see other people lose"	0	0%	

20- Which level of cybber security bachelor students do you think the game suits best?

Optional

Answer	Number of	Percentage	
1st Year	1	25%	
2nd Year	2	50%	
3rd Year	1	25%	
Higher level	0	0%	

See recent changes in Nettskjema