European Commission

Horizon 2020
European Union funding
for Research & Innovation

Cyber Security PPP: Addressing Advanced Cyber Security Threats and Threat Actors

Cyber Security Threats and Threat Actors Training - Assurance Driven Multi- Layer, end-to-end Simulation and Training

D4.2: THREAT-ARREST serious games v1†

Abstract: This deliverable reports on the status of developing and interconnecting serious gaming tools to the THREAT-ARREST training platform. The serious games to be developed will mainly be used to for training against social security threats and attacks and will be aimed at enhancing trainees' ability to resist and mitigate social security attacks in realistic cyber system environments. We provide an overview on the serious games, their integration into the THREAT-ARREST training platform and their current development status.

Contractual Date of Delivery	31/08/2019
Actual Date of Delivery	31/08/2019
Deliverable Security Class	Public
Editor	*Ludger Goeke (SEA)*
Contributors	*Kristian Beckers, Ludger Goeke, Sebastian Pape (SEA)* *George Bravos (ITML)*
Quality Assurance	*George Hatzivasilis (FORTH)* *Georgios Leftheriotis (TUV)*

† *The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786890.*

The *THREAT-ARREST* Consortium

Foundation for Research and Technology – Hellas (FORTH)	Greece
SIMPLAN AG (SIMPLAN)	Germany
Sphynx Technology Solutions (STS)	Switzerland
Universita Degli Studi di Milano (UMIL)	Italy
ATOS Spain S.A. (ATOS)	Spain
IBM Israel – Science and Technology LTD (IBM)	Israel
Social Engineering Academy GMBH (SEA)	Germany
Information Technology for Market Leadership (ITML)	Greece
Bird & Bird LLP (B&B)	United Kingdom
Technische Universitaet Braunschweig (TUBS)	Germany
CZ.NIC, ZSPO (CZNIC)	Czech Republic
DANAOS Shipping Company LTD (DANAOS)	Cyprus
TUV HELLAS TUV NORD (TUV)	Greece
LIGHTSOURCE LAB LTD (LSE)	Ireland
Agenzia Regionale Strategica per la Salute ed il Sociale (ARESS)	Italy

Document Revisions & Quality Assurance

Internal Reviewers

1. *George Hatzivasilis (FORTH)*
2. *Georgios Leftheriotis (TUV)*

Revisions

Version	Date	By	Overview
0.4	26/08/2019	Ludger Goeke	Addressed comments by FORTH and TUV, editorial work
0.3.3	19/08/2019	Ludger Goeke	Addressed the comments by TUV
0.3.2	12/08/2019	George Bravos	Addressed the comments by TUV regarding GDPR
0.3.1	07/08/2019	George Bravos	Addition of figures of wireframes for the user interface of the Training Tool
0.3	05/08/2019	Ludger Goeke	Addressed the comments by FORTH
0.2	28/06/2019	Ludger Goeke	First Draft
0.1.4	25/06/2019	George Bravos	Trainee performance assessment design for Serious Games
0.1.3	20/06/2019	Kristian Beckers	AWARENESS QUEST
0.1.2	12/06/2019	Ludger Goeke	PROTECT, introduction, conclusion
0.1.1	11/06/2019	Sebastian Pape	HATCH, Section 2.1
0.1	27/05/2019	Editor	First Draft

Executive Summary

This document represents the first version of the deliverable "D4.2 – THREAT-ARREST serious games v1". It summarizes the activities that have been performed for the task T4.2 *Serious gaming tools*. The document introduces the concepts for the serious games in the form of the online gaming tools AWARNESS QUEST and PROTECT that are part of the Gamification Tool and the physical card game HATCH. Additionally, it discusses the assessment of trainees. This discussion includes a concept for the assessment of trainees, an overview of the interaction of the Gamification Tool with the Training Tool and first designs for the representation of training results in the user interface of the Training Tool. The deliverable describes also, how the gaming tool PROTECT will be integrated into a training program. The compliance of the THREAT-ARREST project to the General Data Protection Regulation (GDPR) (EUROPEAN PARLIAMENT & COUNCIL OF THE EUROPEAN UNION, 2016) is also considered. In this context, appropriate data privacy policies are specified.

Within Work Package (WP) 4, the deliverable D4.2 focuses on the concepts of the serious games and their conceptual integration into the training programs of THREAT-ARREST. In this version of the deliverable the current status of the implementation of PROTECT is already considered. Further implementation tasks for PROTECT and the implementation of AWARENESS QUEST will be described in the second version of this deliverable in Month 30 of the THREAT-ARREST project.

The integration of the graphical user interfaces (GUI) of the gaming tools into the visualisation of the THREAT-ARREST platform is considered in the deliverable D4.1 (Hildebrandt, Bravos, & Goeke, D4.1: THREAT-ARREST Visualisation Tools v1, 2019). The discussion of the technical interaction of the gaming tools as part of the Gamification Tool with the Training Tool is contained in deliverable D4.3 (Hildebrandt, Bravos, & Goeke, D4.3: Training and Visualisation tools IO mechanisms v1, 2019). This discussion considers the specification of the transmitted data for the initialization of the gaming tools and the query of results of finished games.

The deliverable D3.1 (Frati & Prusa, 2019) describes the definition of instances of gaming tools for training scenarios within Cyber Threat and Training Preparation (CTTP) models.

Table of Contents

List of Abbreviations

API Application Programming Interface

CTTP Cyber Threat and Training Preparation

DHS Department of Homeland Security

DoJ Department of Justice

EUROPOL European Union Agency for Law Enforcement Cooperation

FBI Federal Bureau of Investigation

GDPR General Data Protection Regulation

GUI Graphical User Interface

IDN Internationalized Domain Name

M Month

REST Representational State Transfer

T&C Terms and Conditions agreement

TRL Technology Readiness Level

WP Work Package

List of Tables

List of Figures

1 Introduction

This deliverable considers the gamification part of the THREAT-ARREST project. The gamification comprises serious games for training people in relation to the topic of social engineering. These serious games can be distinguished into the following types:

1. The online games AWARENESS QUEST and PROTECT that are provided within THREAT-ARREST training platform by the Gamification Tool. In the following, AWARENESS QUEST and PROTECT are also referred by the term *gaming tools*.
2. The tabletop game HATCH that is used for a training scenario in which the trainees are present on-site and that is moderated by a trainer.

The further content of this deliverable is composed as follows:

- Section 2 describes the game concepts for the serious games HATCH, AWARENESS QUEST and PROTECT. Regarding PROTECT, its implementation is discussed additionally.
- Section 3 considers the assessment of the performance of trainees that use the gaming tools. In addition to a concept for this assessment, the communication between the Training and Gamification Tool is described.
- Section 4 discusses the compliance of THREAT-ARREST to the GDPR and specifies concrete data privacy policies for the handling of data within the THREAT-ARREST project.
- Section 5 considers a concept for the implementation of trainings scenarios for the gaming tool PROTECT within THREAT-ARREST.
- Section 6 contains the conclusion of this deliverable.

The deliverable shall convey an understanding of the concepts of the different serious games. Additionally, it shall outline, how the gaming tools AWARENESS QUEST and PROTECT will be integrated into the THREAT-ARREST training platform. As another outline, the deliverable shall represent how GDPR will be addressed in the context of the THREAT-ARREST project.

2 THREAT-ARREST Serious Games

SEA has developed three different serious games for certain use cases. The use scenario for HATCH (see subsection 2.1) is a dedicated offline training session with a trainer. Teams play with cards in groups with 3 to 5 persons. The AWARENESS QUEST and PROTECT are online games. The AWARENESS QUEST (see subsection 2.2) is a quiz game that allows single and dual player modes. PROTECT (see subsection 2.3) is a single player game in a patience like manner. Both online games are meant to be played in short sessions as “in between games”. Thus, a trainer is not needed, but the results of the games can be reported for further analysis.

2.1 HATCH

HATCH is a card game which can be used to serve two purposes:

1. Elicitation of requirements (Beckers & Pape, A Serious Game for Eliciting Social Engineering Security Requirements, 2016)
2. Training of awareness against Social Engineering attacks (Beckers, Pape, & Fries, HATCH: Hack And Trick Capricious Humans - A Serious Game on Social Engineering, 2016)

In this project, we focus on the use of HATCH as a serious game for raising the awareness of Social Engineering attacks.

Figure 1: HATCH Gaming Sessions

2.1.1 Short description

The rules of the game are as follows:

1. Each player draws a card from the deck of human behavioural patterns (principles), e.g. the Need and Greed principle. The game is designed based on existing published work (e.g. Stajano and Wilson (2011), cf. (Beckers & Pape, A Serious Game for Eliciting Social Engineering Security Requirements, 2016)).
2. Each player draws three cards from the deck of the social engineering attack techniques (scenarios), e.g. phishing. The game is designed based on existing published work (e.g. Gulati (2003); Peltier (2006), cf. (Beckers & Pape, A Serious Game for Eliciting Social Engineering Security Requirements, 2016)).
3. The players decide if they take the roles of insiders or outsiders to the organization.
4. After a brainstorming phase, each player presents an attack to the group and the others discuss if the attack is feasible.

5. The players get points based on how viable their attack is and if the attack was compliant to the drawn cards. The player with the most points wins the game.
6. As debriefing, the perceived threats are discussed, and the players reflect their attacks. They may be supported by the company's security personal.

Figure 2: HATCH Material

An attack consists of a psychological principle and a social engineering attack scenario. The player's task is it to come up with a convincing story how an attack based on the cards could happen. The other players discuss how likely the described attack may succeed and how well it matches the shown cards. Based on the result of the discussion the other players determine the player's score for the described attack.

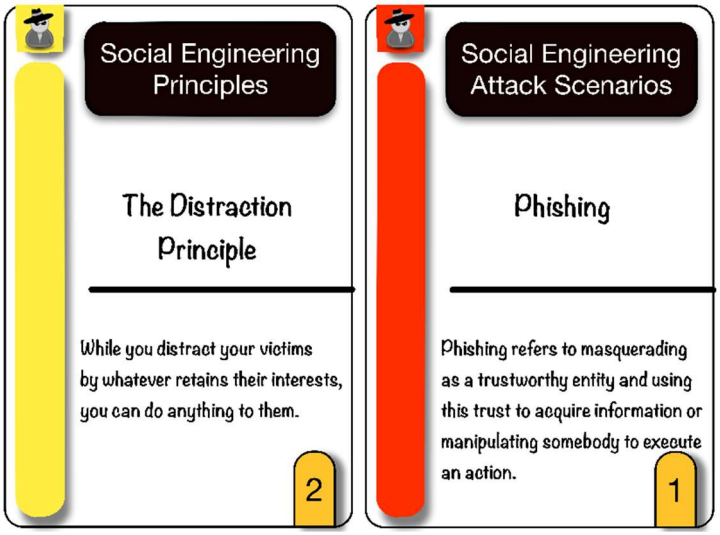


Figure 3: HATCH Cards

In the training/awareness raising version of the game, the attacks take place in a virtual scenario with a board showing the layout of the considered organisation and persona descriptions allowing the players to determine a persona's knowledge, password and if he/she might fall for a certain attack.

2.1.2 New designs

In the THREAT-ARREST project the cards were redesigned. That means, the description of the psychological principles and the social engineering attacks were enhanced and the layout was substantially re-designed. Images of the new design are shown below. We will apply the new design to all type of cards.

Figure 4: New Layout for HATCH Cards

2.1.3 Planned novel game scenarios

So far there exist three different scenarios: A small office of the ACME company, a larger scenario for the SIDATE energy provider with several outposts and a general scenario for the collaboration of a small company with an external consulting company. As sketched above, scenarios include a map of the considered organisation along with a set of persona descriptions.

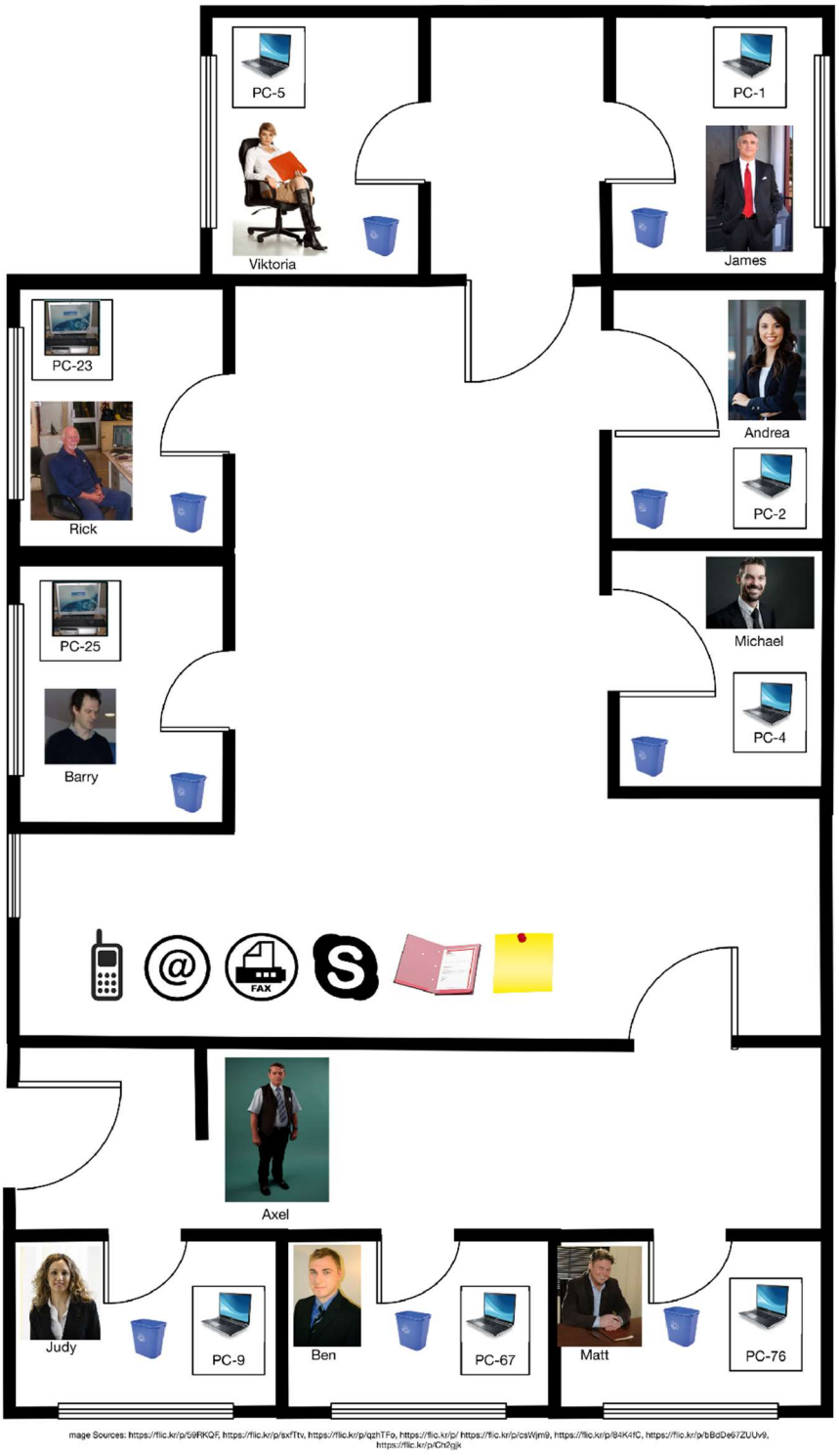


Figure 5: HATCH Game Plan

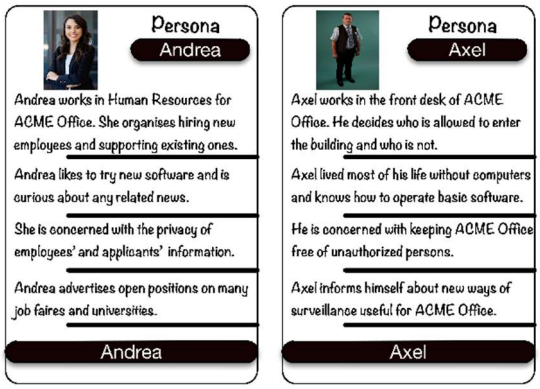


Figure 6: HATCH Persona Cards

During the runtime of the THREAT-ARREST project we will run several workshops with HATCH and develop specific scenarios based on the project pilot scenarios: smart shipping, smart home and electronic health care. These scenarios will be based on expert interviews and designed by the experts from SEA that have done this multiple times.

2.1.4 Summary of Features

Table 1 summarizes the features of HATCH.

Table 1: Features of HATCH

Name	HATCH
Objectives	• Training of awareness against social engineering attacks • Elicitation of security requirements for a company
Game type	Card game
Implementation	Physical tabletop game
Number of players	3 to 5 persons
Customization	HATCH can be adapted to certain scenarios by creating an appropriate game plan and Persona cards.
Role within THREAT-ARREST	Training of awareness against social engineering attacks, whereby each player takes the role of the attacker as well as the attacked in a game of HATCH.

2.2 AWARENESS QUEST

2.2.1 Short description

Security awareness made fun and lightweight is the goal of the AWARNESS QUEST, a simple web-based application that runs in a browser optimized for smart phone screens. This way trainees can do the training whenever they have a few minutes to spare just relying on their phones.

The AWARNESS QUEST contains a set of questions that allows the assessing the security awareness of company employees with regard to concerns such as password policies or letting unauthorized personal enter a company building (Manifavas et al., 2014). This serious game will be enhanced with advanced scenarios of real cyber threats (e.g. (Fysarakis et al., 2014; Hatzivasilis et al., 2019)). We elaborate on how we plan to organize the content management for the AWARNESS QUEST in subsection 2.2.3.

2.2.2 Game Concept

The concept is to allow employees of companies to do quizzes with social engineering scenarios relevant for the domain they are working in. An employee gets a set of questions with different levels of challenges and timing constrains. After each quiz, an employee gets a list of scores and also specific attacks that he/she lacks knowledge in. The game will continuously be enriched with new questions about social engineering threats or cybersecurity attacks that use social engineering in some shape or form (e.g. (Fyarakis et al., 2014; Hatzivasilis et al., 2012)). The game is an electronic game because of these permanent updates an implementation as a physical game would not be possible.

The game offers also various modes. We describe these modes in the following:

- Single Quest: A player plays alone with a set of questions.
- Context Quest: A player shares his/her location with the system and the system picks attacks that happened in that particular location.
- Versus Quest: Two player compete in a challenge against each other. The player that answers more correct questions in a timeframe wins.
- Pick Quest: Two players answer questions one after another. If a player answers correctly he/she can choose the next question for the competing player out of three options.
- Draw Quest: Two player answer questions and if one gets a question right, he/she can choose the context of the question for the other player.

The single player game is meant to be have a learning curve with a slow degree of increase in difficulty. This will keep the flow of player at a constant pace. The multiplayer quests assume that the players are familiar with each other and pick attacks that the player are lease familiar with. Therefore, players will be advices to play the single player extensively first, before moving to the multiplayer competition.

2.2.3 Integration of real Attacks into the Game

The game will rely on the same technical specifications as PROTECT. The presentation will happen on a WEB GUI that will be optimized for smart phones and desktop computers. The persistent data storage will be a REST service in a cloud environment.

The attacks in the game will be based on various online sources. We provide the following Table 2 of example attacks, which will be extended during the next months in the project.

Table 2: Sources for social engineering attack scenarios

Webpage/Article/Document	Description
Real World Examples	The webpage (Social Engineer Inc, 2019) provides descriptions of real-world examples for social engineering.
23 Social Engineering Attacks You Need To Shut Down	The online article (Peterson, 2016) provides a short introduction into the theme of social engineering. After that, it explains 23 social engineering attacks. For several attacks the appropriate countermeasures and defence behaviours are discussed.

Webpage/Article/Document	Description
The 7 Best Social Engineering Attacks Ever	The online article (Peters, 2015) considers seven social engineering attacks. The different attacks are explained by referencing actual incidents based on the executions of the attacks. After the description of the attacks, recommendations according to the awareness against social engineering are given.
Chrome, Firefox, and Opera users beware: This isn't the apple.com you want	The online article (Goodin, 2017) describes the exemplary provision of an internationalized domain name (IDN) homograph attack. Such an attack exploits weaknesses of *Punycode*[1] that specifies the transformation of Unicode to a subset of ASCII characters in the context of the representation of international domain names. In the described attack a domain name has been registered that shall feign the domain name "apple.com"[2]. This is achieved by using only Cyrillic characters in the fake domain name[3]. For a user it is quite difficult to identify that the fake domain name in the web browser consists of Cyrillic characters.
How Hacktivists Have Targeted Major Media Outlets	The online article (Lemos, 2013) considers attacks of the Syrian Electronic Army against major news outlets. The objective of these attacks has been the distortion of online media content. A large amount of the attacks has been started by using phishing emails.
Sicherheits-Report: Unternehmen setzen selbst simple Schutzmechanismen nicht um (translation of the author: Security report: Companies do not even implement simple protection mechanisms)	The online article (Ries, 2016) emphasizes the threats emanating from phishing emails.
Als Chef getarnt fordern Internet-Kriminelle Geld von Firmen (translation of the author: Disguised as the head, internet criminals demand money from companies)	The online article (Schaible, 2016) describes an actual provision of a social engineering attack scenario that uses impersonation. In the context of the considered attack, the attacker impersonates himself/herself as the head of the targeted company and demands the employees of the company via email to perform money transfers.
Deutsche Industrie zieht Cyberkriminelle an (translation of the author: German industry attracts cyber criminals)	The online article (dpa, 2016) states that 69 percent of the German industry companies have been victims of information security attacks. In this connection, a large percentage of attacks have been initiated by current or former employees. Additionally, the most common types of attacks that have been executed are listed.
Cybersecurity Governance: an experiment with Brazilian banks' employees on Facebook	The paper (Terlizzi, Cunha, & Fernando , 2016) describes the execution of an experiment that examines whether employees of banks are more prepared to avoid social engineering attacks on Facebook® than typical users of the platform.

[1] https://www.rfc-editor.org/rfc/rfc3492.txt
[2] https://www.apple.com/
[3] https://www.apple.com/

Webpage/Article/Document	Description
Hacker Publishes Personal Info of 20,000 FBI Agents	The online article (Franceschi-Bicchierai, 2016) describes the robbery of personal information of 20000 agents of the Federal Bureau of Investigation[4] (FBI) and 9000 officers of the Department of Homeland Security[5] (DHS). For the attack, the attacker used compromised credentials to get access to the confidential data. He got these credentials by applying social engineering against an employee of the Department of Justice[6] (DoJ).
Public Awareness and Prevention Guides	On the website (Europol, 2019), the European Union Agency for Law Enforcement Cooperation[7] (EUROPOL) provides public awareness and prevention guides regarding crimes, threats and frauds in the context of the usage of information technology, internet activities and social media. These guides reference among others social engineering attacks like fraud scam and vishing.
Allianz für Cyber-Sicherheit (Alliance for Cyber Security)	On the webpage (BSI, Infromationspool, 2019), the Allianz für Cyber-Sicherheit[8] (Alliance for Cyber Security) provides among others information according to social engineering attacks and corresponding countermeasures (see (BSI, Awareness-Poster - Psychotricks und Phishing-Maschen, 2019) and (Hesse, 2015)).
Falsche Polizei am Telefon (translation of the author: Wrong police at the telephone)	The post (Trickbetrug, 2019) describes a social engineering attack scenario in which fraudsters impersonate themselves as police officers that call their victims by telephone. The fraudsters offer them to store their jewelry and cash safely by the police to avoid its loss due to burglaries in the neighborhood. For this, they should hand over their jewelry and cash to a colleague that would come by later.

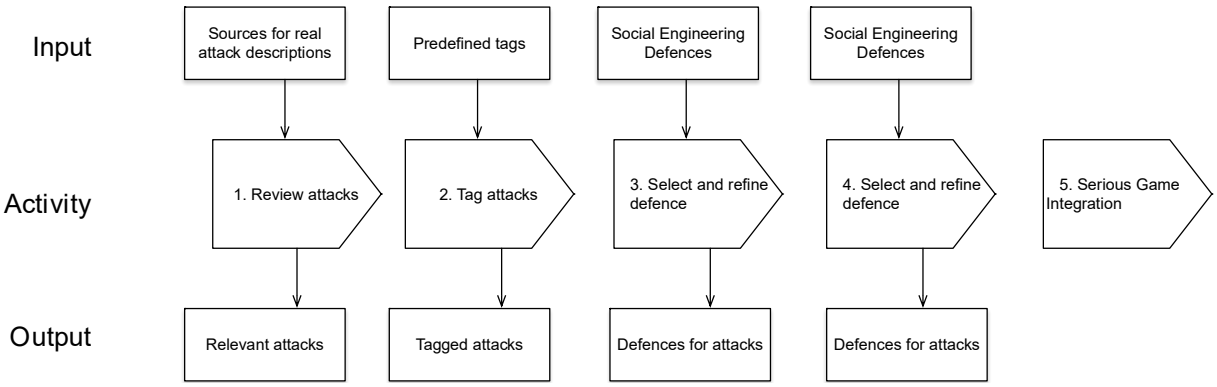


Figure 7: AWARENESS QUEST Attack Source Analysis

We describe the process we will follow to identify and prepare social engineering attacks and defences in Figure 7. We will in regular intervals query established sources for attacks similar to the ones listed beforehand. Afterwards, we will tag the stories with labels such as shipping domain or baiting attack. Next, we will select an appropriate defence and refine it for this particular attack. Finally, based on the details of the attack and defences, we will create a number of questions for the AWARNESS QUEST. This process ensures that all attacks in

[4] https://www.fbi.gov/
[5] https://www.dhs.gov/
[6] https://www.justice.gov/
[7] https://www.europol.europa.eu/
[8] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html

AWARNESS QUEST do refer to real reports of social engineering attacks from credible sources.

2.2.4 Summary of Features

The features of AWARENESS QUEST are summarized in Table 3.

Table 3: Features of AWARENESS QUEST

Name	AWARENESS QUEST
Objectives	Training of awareness against social engineering attacks
Game type	Quiz
Implementation	Online game
Number of players	• One player in single player mode • Two players in different competition modes (see subsection 2.2.2)
Customization	Expandability of the set of questions and corresponding answers of the quiz based on information of real-world social engineering attacks that is elicited by a specific content management process (see Figure 7).
Role within THREAT-ARREST	Training of awareness against social engineering attacks by a quiz game that allows in addition to the single player mode the playing of two players against each other in different competition modes.

2.3 PROTECT

This section considers the serious online game PROTECT that implements a training for the subject of social engineering. A short description of the game is provided in subsection 2.3.1.

The game concepts of PROTECT base on the work of Aladawy et al. (Aladawy, Beckers, & Pape, 2018). Within this work, the specified concepts have been examined by performing a case study. For this case study, a prototype tool has been developed. The subsection 2.3.2 discusses the complete new implementation of the game concepts of (Aladawy, Beckers, & Pape, 2018) in the form of PROTECT. It also describes partial improvements of these concepts that have been made for the implementation of PROTECT.

Subsection 2.3.3 considers the game concepts and mechanisms of PROTECT in detail.

2.3.1 Short description

PROTECT is a serious game for sensitizing people for social engineering. The main goal of this serious game is to “inoculate” people against social engineering attacks. This inoculation is achieved by confronting people repeatedly with social engineering scenarios in order to trigger an appropriate response.

PROTECT is designed to achieve the following goals:

1. increasing awareness for social engineering,
2. training resistance to persuasion and
3. addressing the general population.

PROTECT realizes a serious game in the form of a card game. It is implemented as an online game for single players that is played in a web browser.

The primary game concept of PROTECT is the confrontation of a player with possible social engineering attacks. For an attack, a player shall select the appropriate defense mechanism that ensures a secure outcome of the attack. Both, social engineering attacks and defense mechanisms are represented by corresponding types of cards. The game concepts and game mechanisms of PROTECT are discussed in detail in the subsection 2.3.3.

2.3.2 Novel game implementation in the form of PROTECT

PROTECT is based on the design goals and game concepts of a serious game based on the work of Aladawy et al. (Aladawy, Beckers, & Pape, 2018). This work also contains a case study including an empirical evaluation of the described serious game. For conducting the case study, a prototype of the serious game, named PERSUADED, has been implemented.

PROTECT is a completely new implementation of the design goals and game concepts of (Aladawy, Beckers, & Pape, 2018) and the PERSUADED prototype. This new implementation takes findings from the case study into account. Based on this study, also some game concepts of (Aladawy, Beckers, & Pape, 2018) have been adapted for PROTECT. In this context, PROTECT implements the following improvements:

1. An additional algorithm for the appearance of Attack cards on top of the card deck has been implemented within PROTECT. This algorithm enables beginners an easier start for playing the game.
2. Joker cards, which can be played as a defense for any Attack card, have been added.

The changed game concepts are explained in more detail in the subsection 2.3.3.

PROTECT also provides a completely new designed user interface (see Figure 8 and Figure 9). Compared to PERSUADED, the user interface of PROTECT (see Figure 9) is much more ergonomic and the game flow as well as the resulting user interaction are more self-explanatory. Additionally, the PROTECT user interface is a more realistic simulation of a real-life card game. Therefore, it creates a more friendly game atmosphere that results in more gaming fun.

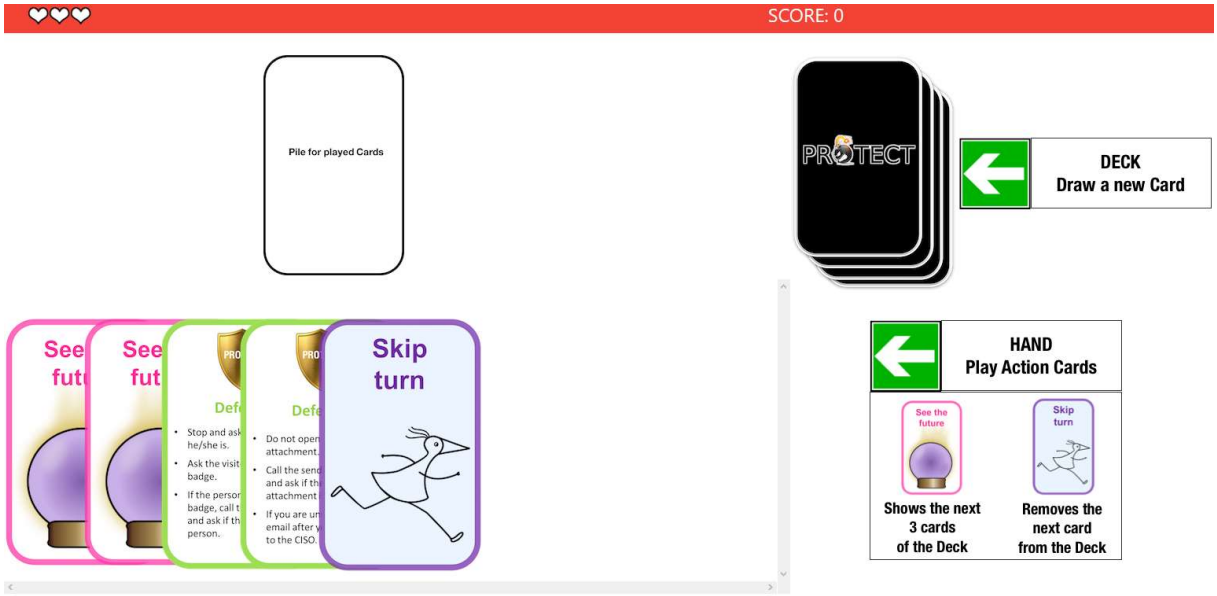


Figure 8: Graphical User Interface of PERSUADED

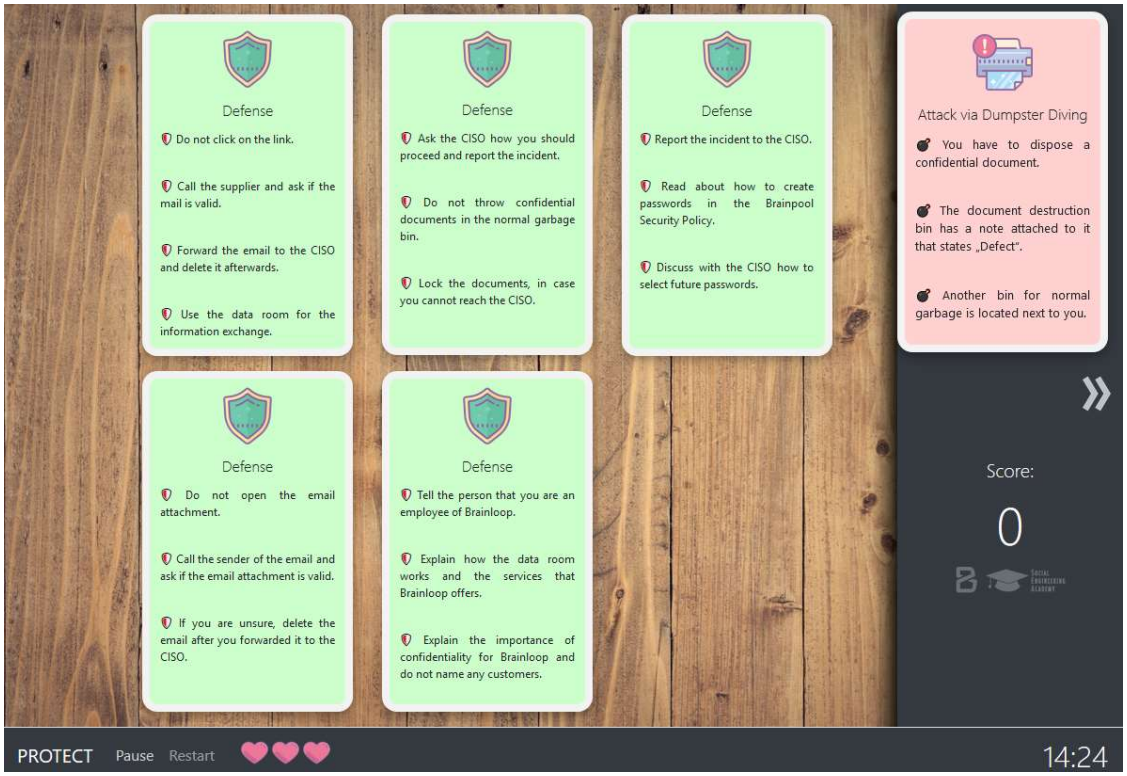


Figure 9: Graphical User Interface of PROTECT

Another major improvement of PROTECT is the implementation of the cards. Within the PERSUADED prototype, every card is implemented by a single image that has to be created

with help of special tools. In PROTECT the content of the cards of a deck are defined in a JSON format. Every card is defined by a single JSON file. The graphical representation of a drawn card is generated on the fly during a game, based on the content of the corresponding JSON file. The definition of cards based on JSON files enables an easier and faster creation of new cards. Because JSON files can be created with any text editor, there is no need for special tools. The definition of cards in JSON is especially important in the context of the THREAT-ARREST project. This is because the creation of new card decks corresponding to the different pilot scenarios within the project is extremely simplified.

Another new feature of PROTECT is the ability to configure certain parameters for the instantiation of the game. These parameters include among others the:

- game time,
- unique identifier of the player,
- player name, and
- identifier of the card deck to be played

The configuration feature is very crucial within the THREAT-ARREST project, because it enables certain instantiations of PROTECT for corresponding training scenarios. Additionally, it allows the definition of difficulty levels for a game of PROTECT with a certain card deck. This definition of difficulty levels is described in more detail in Section 5.

In contrast to the PERSUADED prototype, the final implementation of PROTECT shall have a degree of maturity that allows a commercial provision of the tool.

Table 4 compares the features of PERSUDED and PROTECT.

Table 4: Comparison of features of PERSUADED and PROTECT

Features	PERSUADED	PROTECT
Technology Readiness Level	TRL 4	TRL7 (at the end of the THREAT-ARREST project)
Suitable GUI for mobile devices	no	yes
Configuration of game parameters	no	yes
Definition of difficulty levels	no	yes
Representation of cards	digital images	based on JSON files
Provision of standard card deck	yes	yes
Selection of different card decks	no	yes
Attack cards	yes	yes
Defense cards	yes	yes
“See the future” cards	yes	yes
“Skip turn” cards	yes	yes
Joker cards	no	yes
Different algorithms for appearance of attack cards	no	yes

2.3.3 Game concepts and mechanisms of PROTECT

This section discusses the game concepts and game mechanisms of the serious game PROTECT.

Regarding its game concept, PROTECT is designed as single player game with easy rules and a low complexity. Based on that, PROTECT implements a card game that realizes a patience and solitaire game approach. This game approach enables a player to play the game at any time independently from other persons. Because the deck of cards is shuffled before a game starts, each game is different from the previous game(s) (cf. (Aladawy, Beckers, & Pape, 2018), Chap. 3, p. 5). This fact shall motivate players to play the game repetitively. Because of the low complexity, the initial barrier for playing the game is quite low and the focus is on the actual content of teaching.

In the following the game mechanisms of PROTECT are discussed. While playing PROTECT, the player is confronted with social engineering threats. Here, the player takes the role of the attack receiver/defender. The task of the player is the selection of the appropriate defense mechanism for the attacks. A defense mechanism is a pattern of behaviour that prevents a successful conduct of the corresponding attack (cf. (Aladawy, Beckers, & Pape, 2018), Chap. 1, p. 2).

PROTECT is implemented as an online game, because, online games reduce the preparation effort for a game to a minimum, compared to tabletop games. Furthermore, online games can be played much better on the way. Together with a short playing time, PROTECT can be easily integrated into the players' life.

In the following, the different types of cards within PROTECT are discussed. A social engineering attack is represented by a certain type of cards named *Attack cards*. These cards display attack scenarios in textual form. Defense mechanisms are represented by so called *Defense cards*. These cards display the appropriate behavioural patterns for the defense also in textual form. For each Attack card exists exactly one corresponding Defense card.

In addition to Attack and Defense cards, PROTECT provides the following special cards:

1. *"See the Future" cards* allow the player to take a look on the next three cards on the top of card deck.
2. *"Skip turn" cards* allow the player to skip the top card of the deck and put this card to the bottom of the deck. It is only allowed to play a "Skip turn" card if the top card of the deck is still hidden (cf. (Aladawy, Beckers, & Pape, 2018), chap. 1, p. 4).
3. *Joker cards* are wildcards that can be selected by the player as a defense mechanism for every Attack card.

The Joker cards represent an extension of PERSUADED. By playing Joker cards, players can achieve a good score even if they do not know the appropriate defenses for some attacks. This shall keep up the motivation of the players high, to play the game repeatedly. Within instantiations of PROTECT with a more advanced difficulty level, the number of Joker cards in the card deck is reduced more and more.

The Figure 10 shows the start view of PROTECT. All cards are included in a random order in the card deck that is positioned in the top right corner. The game score as well as the game time are displayed in the bottom right corner. The remaining lives of the player are represented by the pink heart symbols. A running game can be interrupted by the player by pressing the Pause button.

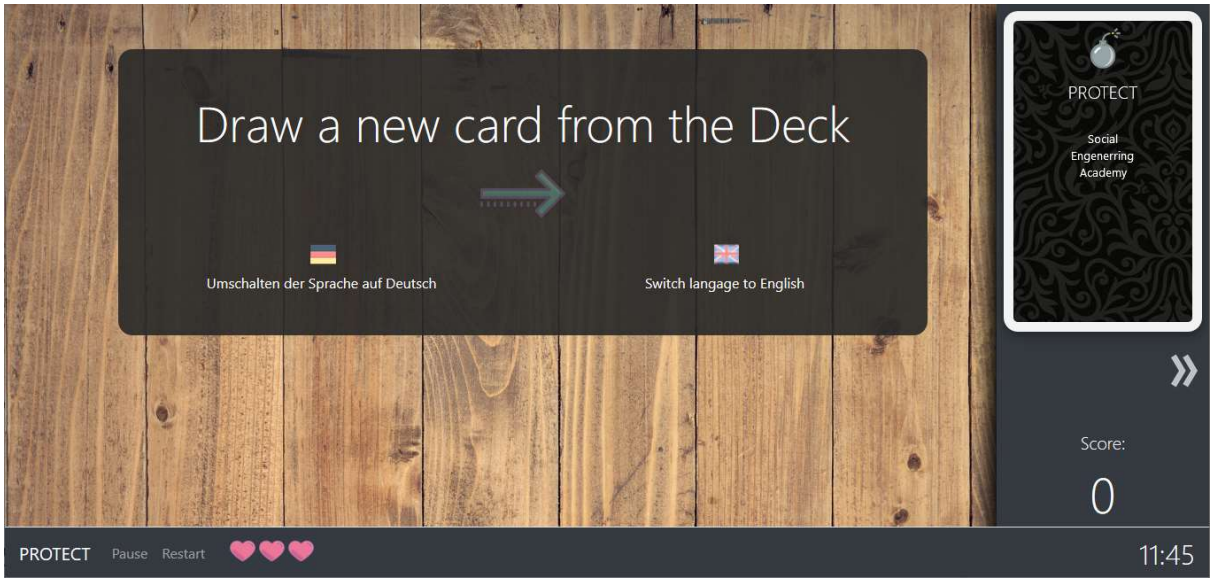


Figure 10: Start view of PROTECT

A game starts when the player draws the first card from the top of deck. When the card deck is empty, the game is won. The game is lost when:

1. the game time is up before finishing the deck or
2. a player has lost all his/her lives.

Before every turn in the game, the top card of the deck is always hidden. At the beginning of a turn, a player can perform one of the following actions:

1. Draw the top card on the deck.
2. Playing a “See the future” card or “Skip turn” card if such a card is on the player’s hand.

Any drawn card that is **not** an Attack card, is put to the hand of the player. After that, the turn is over. All cards on the player’s hand are placed on the table that is included in the graphical user interface (see Figure 11).

If the drawn top card represents an Attack card (see Figure 12), the player has to select the appropriate Defense card. The selection of the correct Defense card is confirmed by certain dialog (see Figure 13) and the score is increased. Both, the drawn Attack card and the selected Defense card are removed from the game.

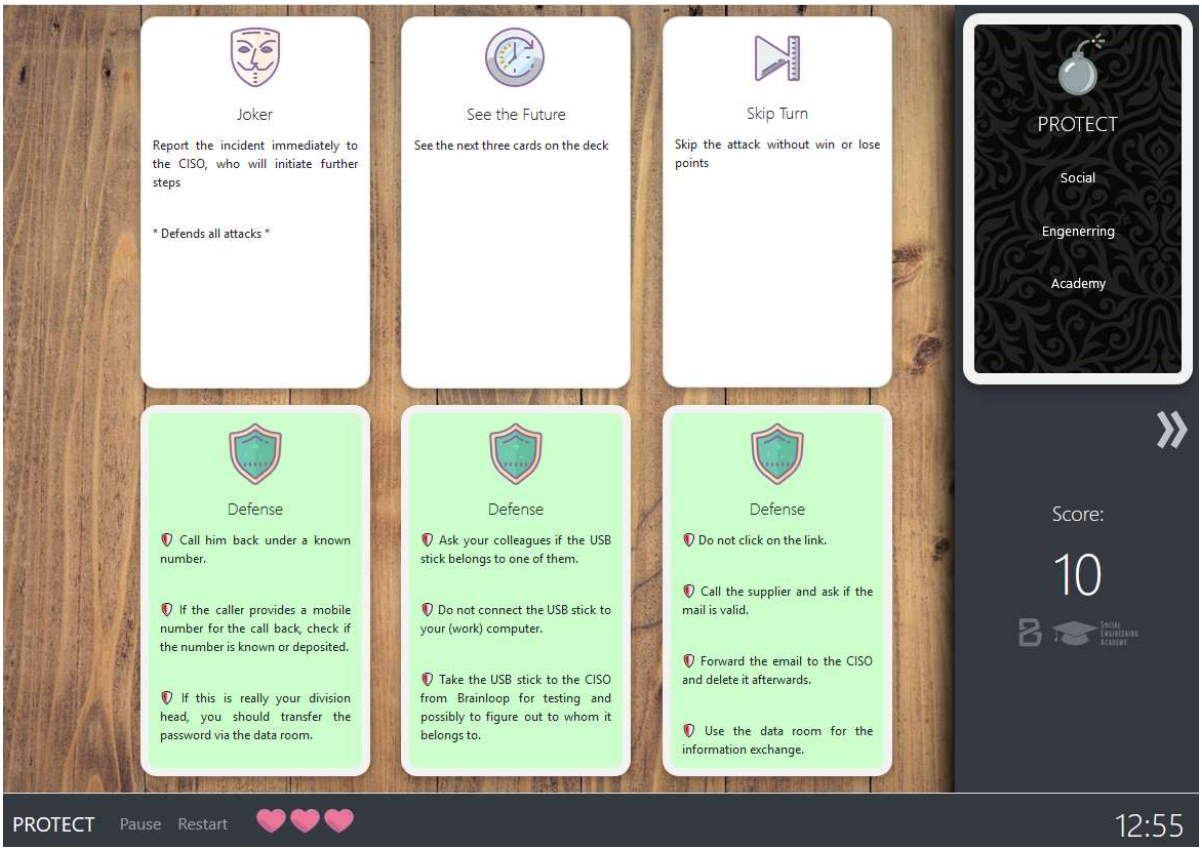


Figure 11: Cards on Hand of the Player

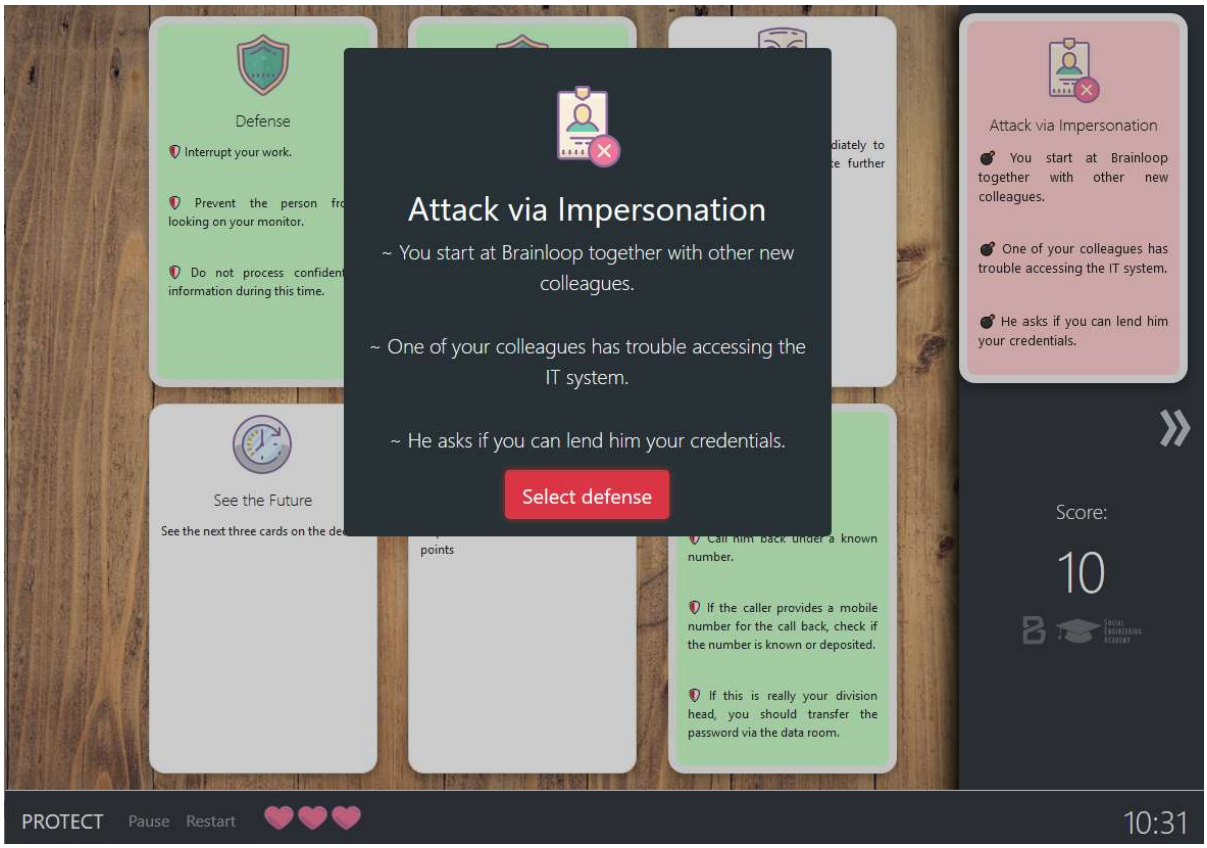


Figure 12: Drawing of an Attack Card

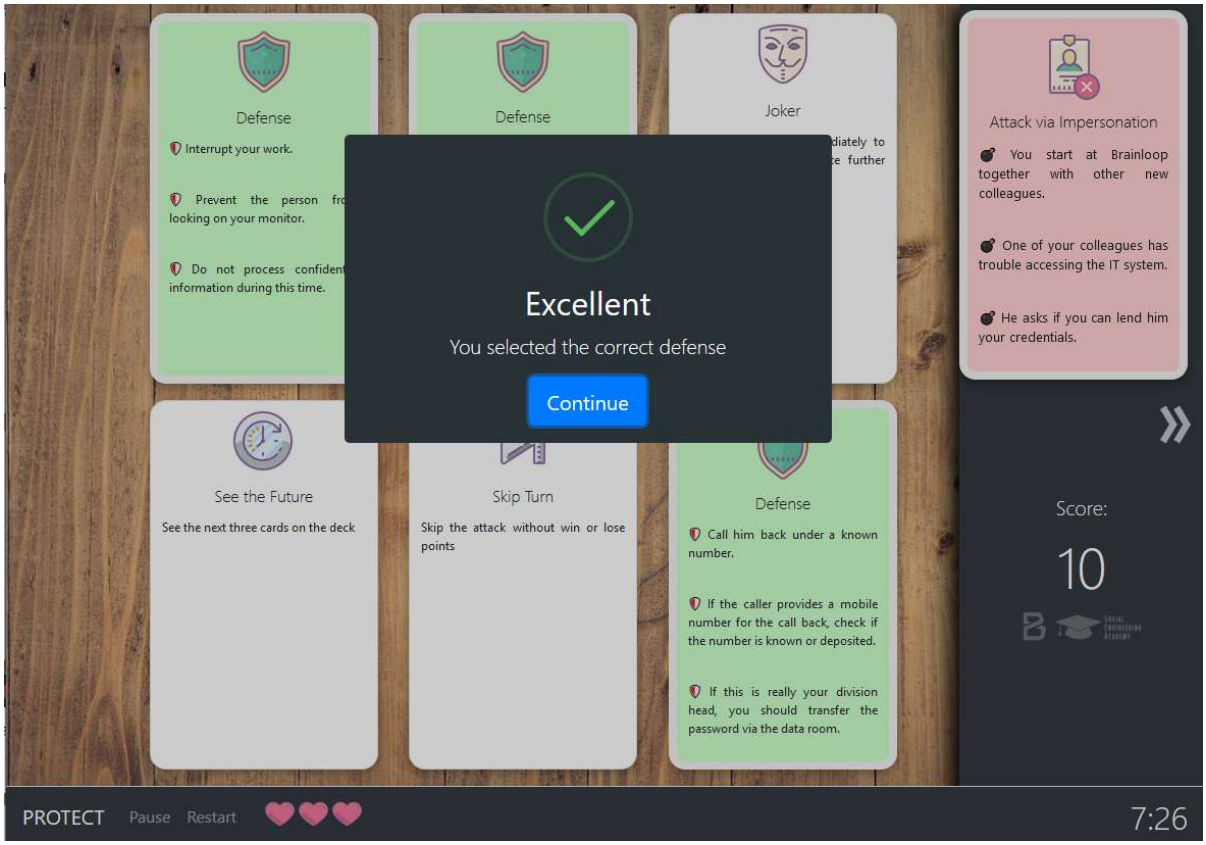


Figure 13: Selection of the correct Defense Card

If an incorrect Defense card has been chosen, an appropriate dialog is shown (see Figure 14) and the text of the correct defense is displayed to the player (see Figure 15). Additionally, the player loses one life and the score is decreased. The drawn Attack card is removed from the card deck. The selected Defense card stays on the hand of the player. If the player has no Defense card on the hand, he/she loses one life.

If the player does not know the correct defense for an attack or has no Defense card on the hand, he/she can also play a Joker card, if possible, to repeal the attack. In this case the score is also increased. The player is not allowed to play a “Skip turn” card after the top card on the deck has been drawn.

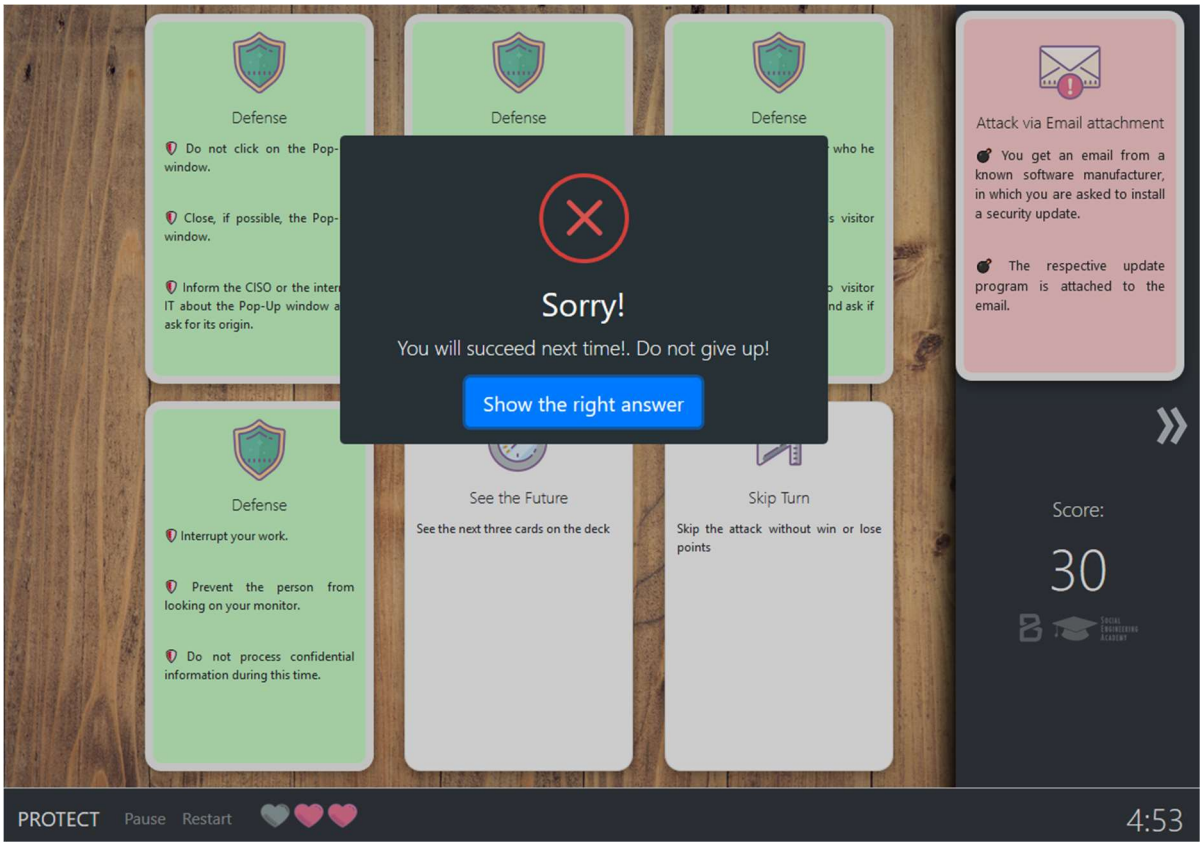


Figure 14: Selection of an incorrect Defense Card

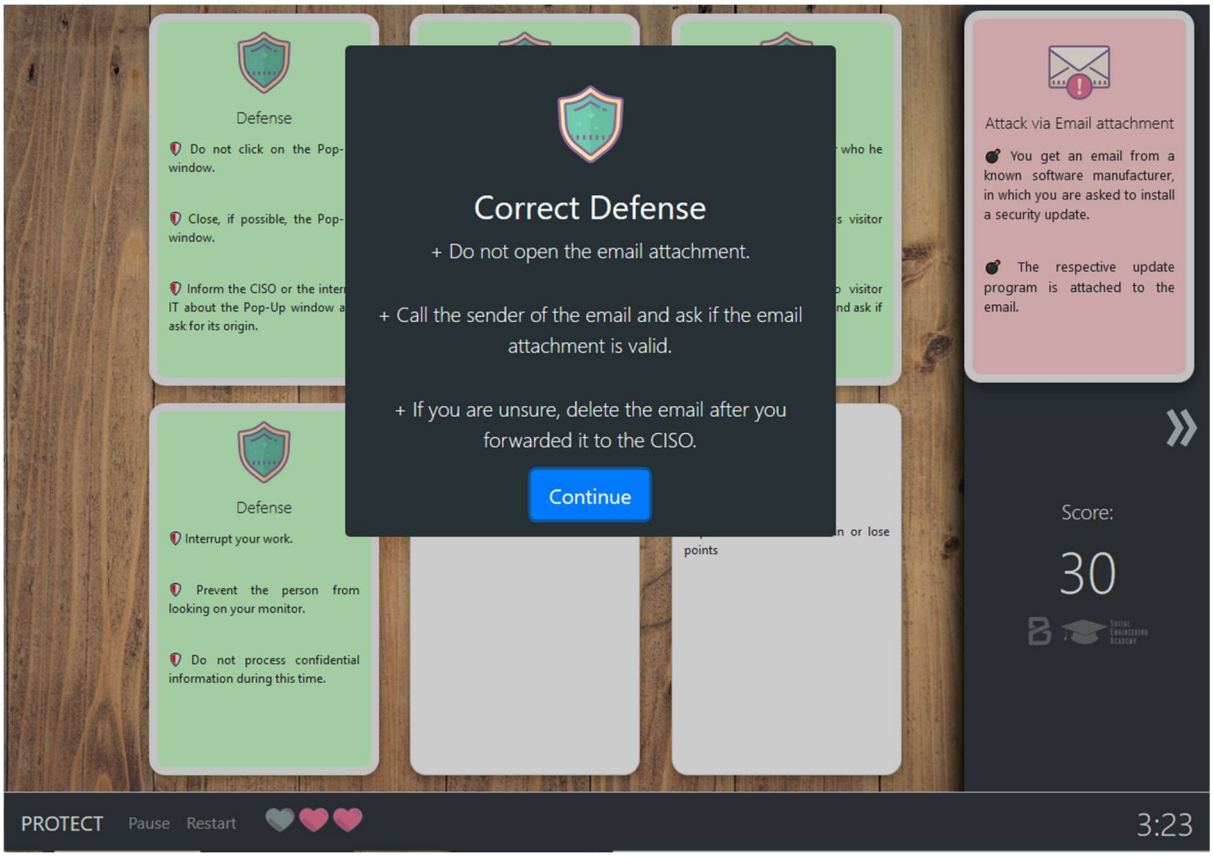


Figure 15: Display of the correct defense after an incorrect Defense Card has been selected

As it can be seen in Figure 14, all Defense cards contain the same icon in the form of a shield. In contrast to that, the Attack cards for the different types of social engineering attacks include a respective icon. This is to avoid that correct matches of Attack and Defense cards could be implied by the icons of the cards.

As already mentioned in Section 2.3.2, PROTECT provides an additional algorithm for the appearance of Attack cards on top of the card deck, compared to PERSUADED. The concepts in (Aladawy, Beckers, & Pape, 2018) do not define any restrictions for the appearance of Attack cards on the top of the card deck. Because of that, it can happen that the player draws an Attack card for which no appropriate Defense card is included on his/her hand. In this case, the player is forced to play an incorrect Defense card and loses a life. This fact shall encourage the player to use “See the future” and “Skip turn” cards in the following way.

The player can play a “See the future” card (see Figure 16) to see the next three cards on the deck. If these cards include any Attack cards, he/she can check if the appropriate Defense cards are:

- on his/her hand or
- contained in the future cards itself at the right position.

If the future cards should contain any Attack cards for which no corresponding Defense cards are available, the player can remember the order of these Attack cards and play a “Skip turn” card to skip such an Attack card when it is on the top of the deck. In this way, he/she can prevent the loss of a life. The provision of this game strategy increases the learning effect because the player studies the content of any Attack cards included in the future cards more carefully. This also applies for the content of the current Defense cards on his/her hand. Furthermore, he/she matches Attack cards partly against defense mechanisms that are not represented by Defense cards on the player’s hand.

The provision of the strategy, as mentioned before, requires an increased understanding of the game from the player. Additionally, it has a random factor because of the random order of the cards in the deck.

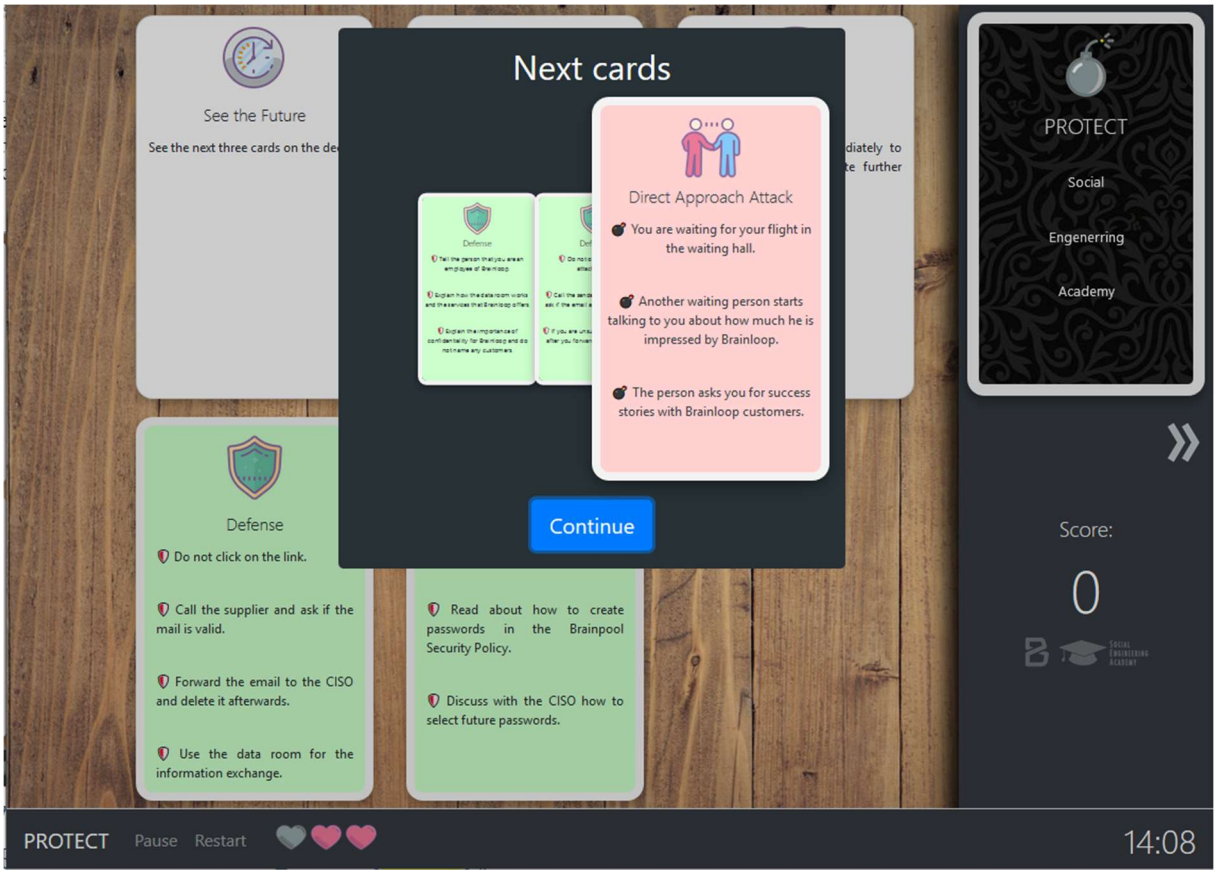


Figure 16: Display of the next three cards on the top of the deck after playing a "See the future" card

In the study for PERSUADED, the players have rated the original algorithm for the appearance of Attack cards, mentioned above, as negative. This result has been taken into account for the game concept and implementation of PROTECT. Thus, PROTECT provides, additionally to the original algorithm, a further concept for the appearance of Attack cards. The implementation of this concept ensures only Attack cards for which an appropriate Defense card is currently on the hand of the player can be drawn. In this scenario the player can use the "See the future" cards and "Skip turn" cards to skip Attack cards for which he/she is not able to identify the appropriate Defense card on the hand.

Because the new algorithm for the appearance of Attack cards makes the playing of PROTECT easier, it shall be used for players at the beginner level. Accordingly, the original algorithm shall be used for more advanced players. During an instantiation of PROTECT it can be configured which concept shall be used.

2.3.4 Summary of the features

Table 5 summarizes the features of PROTECT.

Table 5: Features of PROTECT

Name	PROTECT
Objectives	Training of awareness against social engineering attacks
Game type	Patience card game
Implementation	Online game
Number of players	Single player
Customization	Attack and Defense cards can be adjusted and/or created for different scenarios.
Role in THREAT-ARREST	Training of awareness against social engineering attacks. These attacks will address also the THREAT-ARREST pilot scenarios (e. g. smart shipping)

3 Trainee performance assessment design for Serious Games

3.1 Trainee Assessment Concept

The trainee performance assessment will be visualised in the THREAT-ARREST dashboard, based on specific requirements aggregated from the THREAT-ARREST end-users. The visualisation of this information comprises two main different fields: the screens for the trainees and the screens for the trainers; these screens will be available for the users initiating the Gamification Tool, but also for the scenarios based on emulation and simulation environments.

In more detail, each trainee will have access to its personal account profile information and its status in terms of the training scenarios (available and completed) and relevant scores of the games he/she has completed. In the preliminary versions of the games, scores will be updated and made available only after the end of each game and not during the games' duration. In the updated versions, assessment will be also made available real-time, within each game's duration.

In addition to that, several types of information will be available for the trainers in each organization with respect to the assessment of the trainees. Each trainer will be able to get an overview of all trainees in the organization (or his/her department); in the health pilots the trainer will be also able to get information about the score of the trainees per rank, while in the maritime pilots per department and vessel. On top of that, the trainers will also have detailed information about the trainees' performance and status per game and per trainee.

3.2 Integration with Serious Games

In order for the trainee and the trainer to obtain access to the respective profiles (and assessment outcomes), a detailed analysis has been carried out with respect to the sequence of the actions/messages to be exchanged between the various components of the THREAT-ARREST platform, including the Gamification Tool. The outcome of this analysis has been depicted in a detailed sequence diagram (see Figure 17), according to which the THREAT-ARREST dashboard, as the main component of the THREAT-ARREST Training Tool, will be responsible for initiating the Gamification Tool for each training session and consequently aggregating all the information regarding the profiles and the assessment of the players/trainees.

In more details, and according to the diagram, the first step in the communication process is related to the acquiring all necessary information from the CTTP modeler. Following that, the Training Tool initializes the gamification environment. After that, the Visualisation Tool is also initialized, and last the Assessment Tool is initialized in order to provide real-time information to the trainees and the trainers. More details about the sequence of communications can be found in D4.3 ((Hildebrandt, Bravos, & Goeke, D4.3: Training and Visualisation tools IO mechanisms v1, 2019), subsection 3.1).

With respect to the above sequence of communications, the initialisation of the Gamification Tool is performed by a dedicated REST API. In order to carry out the initialisation, a CTTP model (or relevant part of it) is used as an input, along with information about each training session; this information includes, among others, the session ID, the user ID and the role ID. More details about the REST API used for the Gamification Tool can be found in D4.3 ((Hildebrandt, Bravos, & Goeke, D4.3: Training and Visualisation tools IO mechanisms v1, 2019), subsection 5.1).

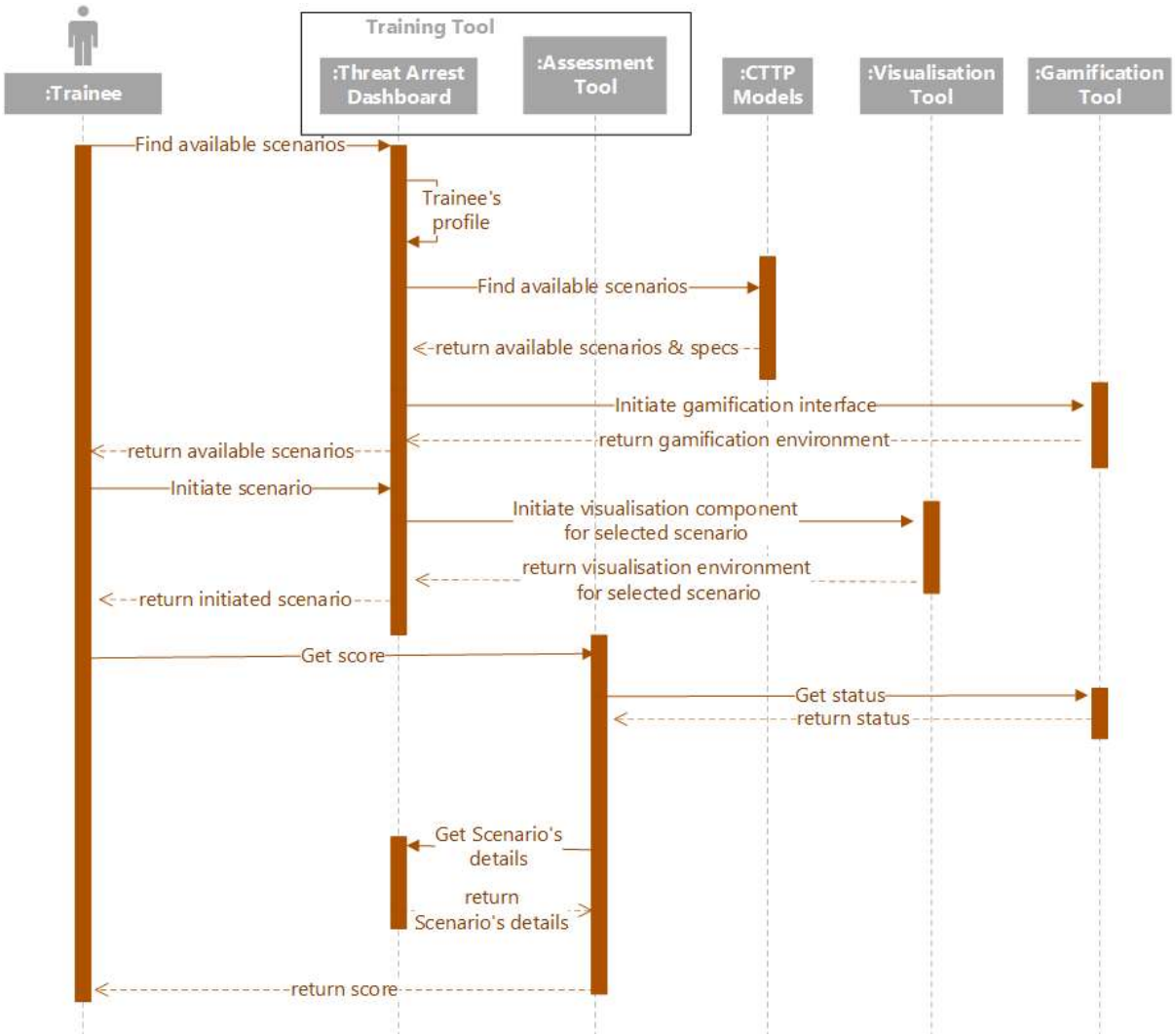


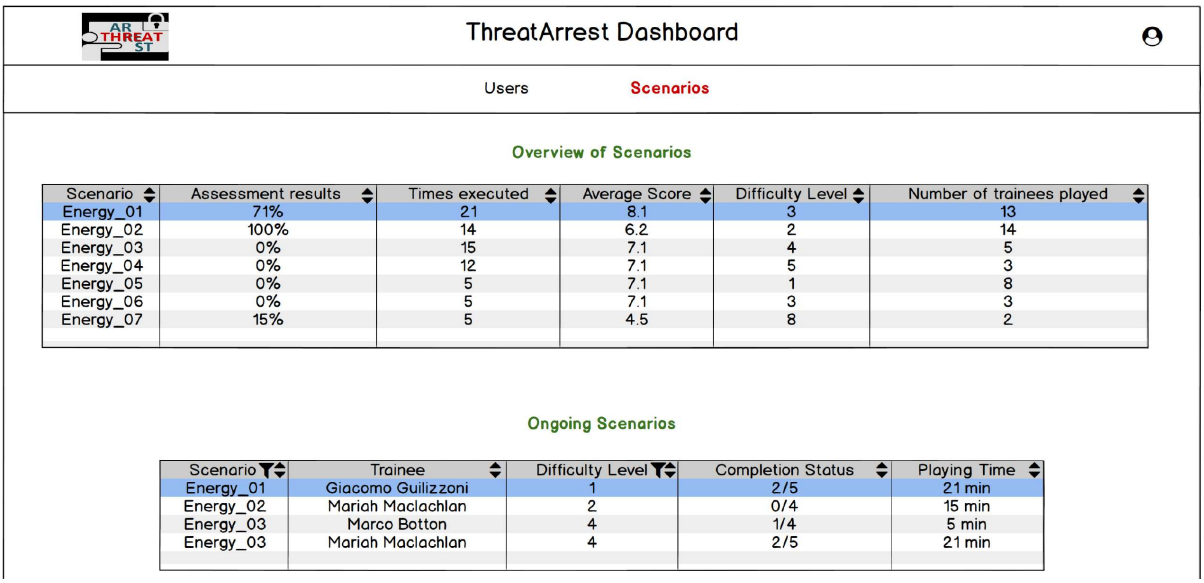
Figure 17: THREAT-ARREST sequence Diagram towards trainees' assessment

3.3 Wireframes of Training Tool and Dashboard with respect to Gamification Tool

The assessment of the serious games will be visualised through the THREAT-ARREST dashboard. Each game will be presented as a separate scenario; the trainer/administrator will be able to have an overview of all scenarios as depicted in Figure 18.

In terms of assessment, the trainer will have access to both an aggregated overview of all trainees (see Figure 19) and of more details for each trainee (see Figure 20).

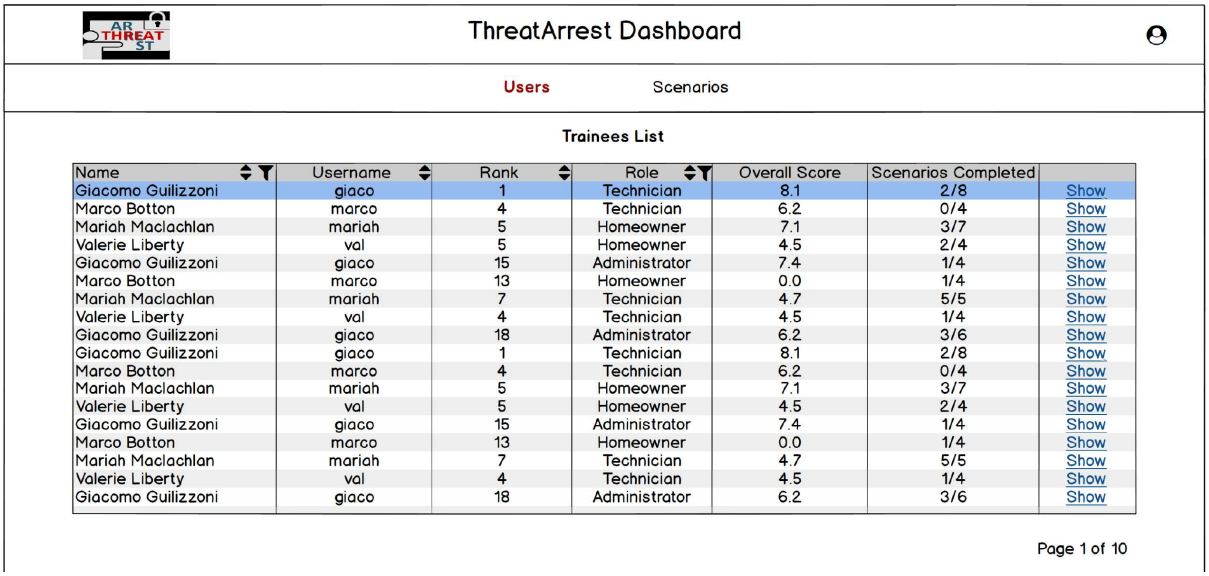
Finally, each trainee will have an overview of his/her status through his/her personal dashboard (see Figure 21). More details about the functionalities of the dashboard are presented in D4.1 (Hildebrandt, Bravos, & Goeke, D4.1: THREAT-ARREST Visualisation Tools v1, 2019).



Scenario	Assessment results	Times executed	Average Score	Difficulty Level	Number of trainees played
Energy_01	71%	21	8.1	3	13
Energy_02	100%	14	6.2	2	14
Energy_03	0%	15	7.1	4	5
Energy_04	0%	12	7.1	5	3
Energy_05	0%	5	7.1	1	8
Energy_06	0%	5	7.1	3	3
Energy_07	15%	5	4.5	8	2

Scenario	Trainee	Difficulty Level	Completion Status	Playing Time
Energy_01	Giacomo Guilizzoni	1	2/5	21 min
Energy_02	Mariah Maclachlan	2	0/4	15 min
Energy_03	Marco Botton	4	1/4	5 min
Energy_03	Mariah Maclachlan	4	2/5	21 min

Figure 18: Visualisation of available scenarios in THREAT-ARREST dashboard



Name	Username	Rank	Role	Overall Score	Scenarios Completed	
Giacomo Guilizzoni	giaco	1	Technician	8.1	2/8	Show
Marco Botton	marco	4	Technician	6.2	0/4	Show
Mariah Maclachlan	mariah	5	Homeowner	7.1	3/7	Show
Valerie Liberty	val	5	Homeowner	4.5	2/4	Show
Giacomo Guilizzoni	giaco	15	Administrator	7.4	1/4	Show
Marco Botton	marco	13	Homeowner	0.0	1/4	Show
Mariah Maclachlan	mariah	7	Technician	4.7	5/5	Show
Valerie Liberty	val	4	Technician	4.5	1/4	Show
Giacomo Guilizzoni	giaco	18	Administrator	6.2	3/6	Show
Giacomo Guilizzoni	giaco	1	Technician	8.1	2/8	Show
Marco Botton	marco	4	Technician	6.2	0/4	Show
Mariah Maclachlan	mariah	5	Homeowner	7.1	3/7	Show
Valerie Liberty	val	5	Homeowner	4.5	2/4	Show
Giacomo Guilizzoni	giaco	15	Administrator	7.4	1/4	Show
Marco Botton	marco	13	Homeowner	0.0	1/4	Show
Mariah Maclachlan	mariah	7	Technician	4.7	5/5	Show
Valerie Liberty	val	4	Technician	4.5	1/4	Show
Giacomo Guilizzoni	giaco	18	Administrator	6.2	3/6	Show

Figure 19: Visualisation of trainees' assessment in THREAT-ARREST dashboard

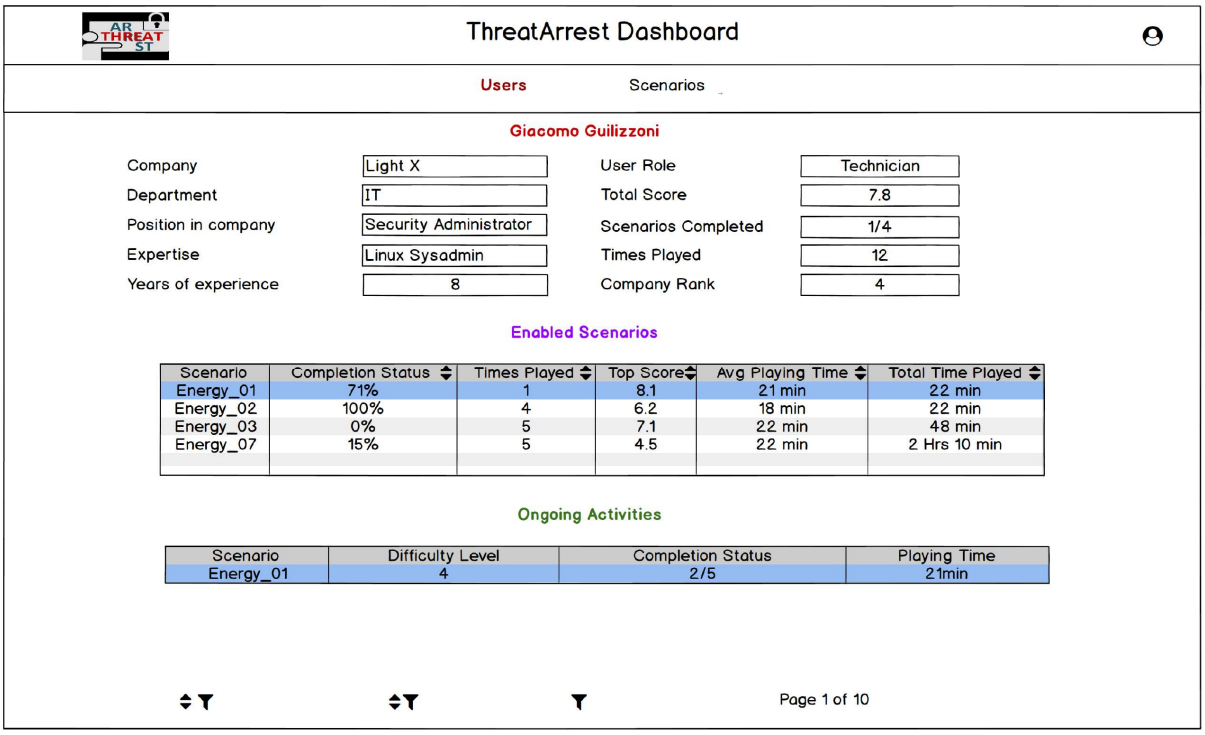


Figure 20: Visualisation of individual trainee's assessment status in THREAT-ARREST dashboard for trainers

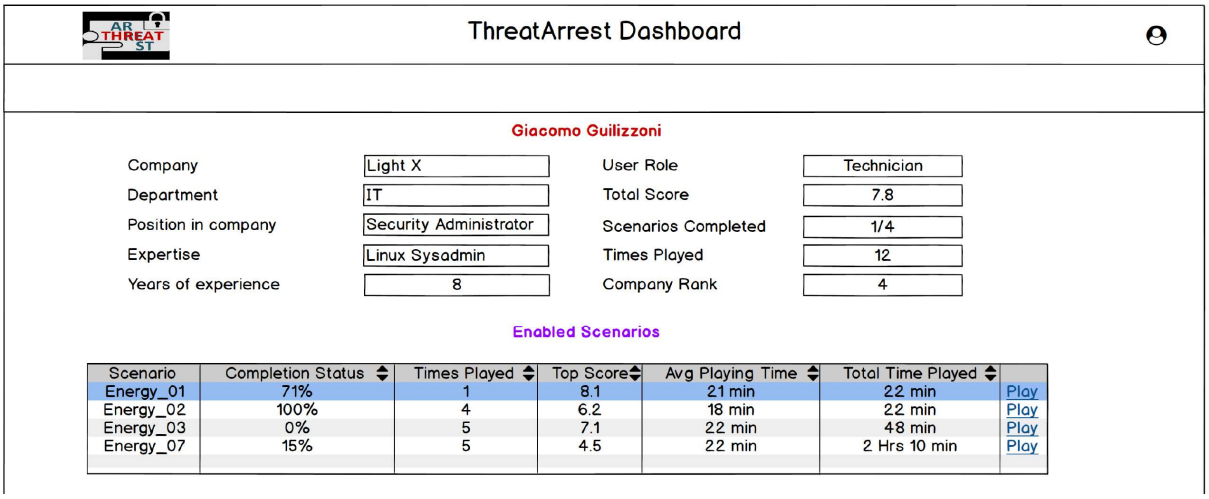


Figure 21: Visualisation of individual trainee's assessment status in THREAT-ARREST dashboard for each trainee

4 Compliance with GDPR

The main principles and rights according to Regulation 2016/679/EU: General (personal) Data Protection Regulation[9] (GDPR) (EUROPEAN PARLIAMENT & COUNCIL OF THE EUROPEAN UNION, 2016) that apply to THREAT-ARREST:

- Right to the protection of personal data
- Principle of free flow of personal data between Member States
- Principle of the general interest and public security
- Principle of transparency - fair and transparent processing
- Lawfulness/Legitimacy of Processing
- Data Minimization
- Privacy-by-Design
- Data Subjects' rights

According to these principles, systems and technologies should be designed in a way that ensures that data protection is limited to: (a) what is necessary for the purpose for which the data are collected; and (b) only those who need to access the personal data can do so. To that end, the following section provides an overview of the approach and the technologies used in the THREAT-ARREST project to ensure the alignment with these policies and regulations.

4.1 Data Privacy Policies in THREAT-ARREST

Taking into consideration the GDPR regulation, the following data privacy policies are defined in THREAT-ARREST that are described in the subsections 4.1.1, 4.1.2 and 4.1.3.

4.1.1 Privacy Notice and Terms and Conditions

The THREAT-ARREST platform ensures that all users (both trainees and trainers) become aware of the terms and conditions and the privacy policy.

Regarding the privacy policy, it requires that the following should be disclosed:

- What personal information is collected through the Training Tool
- What's the purpose of collecting this information
- How the collected information is used by business and/or by any third parties, and for how long it is retained
- How the user can access, review and make changes or ask for deletion of his/her information

Regarding the Terms and Conditions agreement (T&C), also known as a Terms of Service or Terms of Use agreement, it is the legal agreement that sets forth the rules, requirements, and standards of using a website or a mobile/desktop application etc.

For THREAT-ARREST, the privacy policy will be visible in the training platform for both trainees and trainers. The Data privacy policy in detail can be found in subsection 4.2.

4.1.2 Opting out – Withdraw permissions

Apart from the privacy policy, the THREAT-ARREST application provides the capability to the users to opt out from granting consent for their personal data that was previously given or withdraw any permissions that may have been granted through the application.

[9] https://eur-lex.europa.eu/eli/reg/2016/679/oj

Moreover, the application supports the functionality of account deletion upon user request (right-to-be-forgotten); on top of that, the user is able to decide which data are deleted and what are left (anonymized) for research purposes.

4.1.3 Password security and retention policy

The last measure used in THREAT-ARREST in order to ensure alignment with data privacy policies and regulations, is related to password security and the relevant retention policy.

How passwords are stored, and reset is a critical aspect of GDPR security compliance (e.g. (Hatzivasilis, 2017; Hatzivasilis et al., 2015)). Clients and staff members may unwillingly forget or need to reset passwords for a number of reasons. GDPR security requirements dictate that companies must be able to demonstrate that their password reset processes and procedures are secure. Systems must be in place, for example, to prevent help desk employees who may be involved in resets from directly accessing passwords.

The optimum way to ensure this is through the use of a secure "self-service" password reset system. These systems can make use of two- or multi-factor authentication to check that the person requesting the reset is the legitimate owner of the account. A common method to implement this for online services, that will be also used within the THREAT-ARREST platform, is to transmit an automatically generated reset code to the telephone number associated with the individual account name. If used within a short period of time, this process then opens a temporary window when a password reset may occur using the account name or email address.

On top of that, specific guidelines and restrictions will be provided regarding the complexity of the passwords that the users will have to use. In more detail, passwords would necessarily need to consist of at least 10 digits and be complex with at least 3 different types of characters, with the available types being small letters, capital letters, numbers, and special characters.

Finally, THREAT-ARREST users will need to update their passwords periodically; a notification will be sent to the users after 3 months of having the same password, in order to log in to the application and change it. Specific guidelines will be provided, and the user will not be able to use the same password for a second time.

4.2 The THREAT-ARREST Data Privacy Policy

4.2.1 Types of Data collected - What data does the training platform collect

This application collects socio-demographic data, data related to your position in the company, and data related to the performance in training games and scenarios.

4.2.2 Your personal data – what is it?

Personal data relates to a living individual who can be identified from that data. Identification can be possible from this information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession. The processing of personal data is governed by the GDPR (EUROPEAN PARLIAMENT & COUNCIL OF THE EUROPEAN UNION, 2016). The only personal data that you will be asked for is your name, the location of your residential, work, shopping and leisure activities.

4.2.3 Your results – what is it?

By the term "responses", we refer to the outcomes of the training sessions that you will carry out. The only personal data that you will be asked for is your name, age, gender and position in the company. All the other questions do not require the release of any further personal data, and thus to avoid any confusion, we call them responses.

4.2.4 How do we process your personal data?

All the THREAT-ARREST partners who are based in Europe and IBM (who is based in Israel - covered by the EU/Israel Adequacy decision of 31.1.2011) comply with the obligations under the GDPR (EUROPEAN PARLIAMENT & COUNCIL OF THE EUROPEAN UNION, 2016) by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorized access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data.

4.2.5 Sharing your data/responses

Your personal data and responses will be used/processed only by the THREAT-ARREST partners. The THREAT-ARREST partners will use your personal data and responses only for the purposes of the research project THREAT-ARREST. No personal data will be shared with external parties.

4.2.6 Retaining your data

Your personal data will be retained in the THREAT-ARREST platform for as long as you do not “opt-out”; regardless the opting-out option, your personal data will not be stored for more than 1 year after you have entered it.

4.2.7 Your rights and your personal data

You have the right, at any time, to know whether your personal data has been stored. Additionally, you can consult the data controller to learn about their contents and origin, to verify their accuracy or to ask for them to be supplemented, cancelled, updated or corrected, or for their transformation into anonymous format or to block any data held in violation of the law, as well as to oppose their treatment for any and all legitimate reasons.

5 Implementation of a trainings scenario for PROTECT

This chapter describes in a general way how a trainings scenario can be implemented for the serious gaming tool PROTECT (see subsection 2.3).

A game of PROTECT can be adjusted to a certain training scenario by the configuration of the following data:

- The content of the Attack and Defense cards of the card deck for a game of PROTECT
- The difficulty level of which PROTECT is instantiated.

The THREAT-ARREST training platform enables the model-driven specification of training programs by using CTTP models. The content of a training program corresponds always to the target group of trainees for that it has been specified. A target group could be for example a certain sector of industry, state authorities or a specific company.

Concerning the use of PROTECT in a training program, it is crucial that the set of social engineering attacks that are represented in the card deck cover all the characteristics of the targeted organization. Such characteristics include among others business processes, types of processed/stored information, used communication channels and facilities of an organisation. Because of that, it is necessary to check if the standard card deck of PROTECT is sufficient for a training program. If this is not the case, the card deck has to be adjusted. To this,

- relevant existing Attack and Defense cards are modified by updating the content of the associated JSON files (see subsection 2.3.2) and/or
- new pairs of appropriate Attack and corresponding Defense cards are added by creating the corresponding JSON files.

Within PROTECT, the standard card deck and each specific card deck are associated with an unique identifier. The definition of an appropriate PROTECT training scenario inside the CTTP model can use this identifier to define the card deck with which PROTECT is played. Every card deck can be played on different difficulty levels. A difficulty level for a card deck is mapped to values of certain internal configuration parameters of PROTECT. These configuration parameters are represented in Table 6.

Table 6: Internal configuration parameters of PROTECT

Configuration Parameter	Description
Number of lives	Numbers of lives that a player has during a game of PROTECT.
Number of Joker cards	Number of Joker cards that are contained in the card deck.
Number of “See the future” cards	Number of “See the future” cards that are contained in the card deck.
Number of “Skip turn” cards	Number of “Skip turn” cards that are contained in the card deck.
Increase of score	Number of points that are added to the score when the correct Defense card or a Joker card has been selected for an Attack card.
Decrease of score	Number of points that are removed from the score when an incorrect Defense card has been selected for an Attack card.

Configuration Parameter	Description
Range of score	Specification if the lowest score is zero or if the score can be less than zero.

For every card deck a corresponding set of difficulty levels is defined. Accordingly, the difficulty level for a game of PROTECT with a certain card deck in a training scenario, can be defined in the corresponding CTTP model. The number of difficulty levels for a card deck depends on its playability and is determined by the gaming experts within the THREAT-ARREST project.

Both values for the card deck identifier and the difficulty level are hand over from the Training Tool to the Gamification Tool during the instantiation of a game of PROTECT. For this, PROTECT provides a REST API that is described in detail in D4.3 (Hildebrandt, Bravos, & Goeke, D4.3: Training and Visualisation tools IO mechanisms v1, 2019).

6 Conclusions

In this deliverable we introduced the serious games HATCH, AWARENESS QUEST and PROTECT. For AWARNESS QUEST, its game concepts have been described. Additionally, we introduced an approach for the content management of information for the creation of game scenarios within AWARENESS QUEST. The discussion of PROTECT contained the new implementation and partial improvement of the concepts of (Aladawy, Beckers, & Pape, 2018) by PROTECT. It pointed out, why this new implementation is necessary for the representation of the scenario pilots of THREAT-ARREST with PROTECT. Furthermore, this deliverable has provided a design for the assessment of trainees and the communication between the Training Tool and the Gamification Tool. Finally, we discussed the compliances to the GDPR.

One of the major improvements that results from the new tool implementation in the form of PROTECT is the configurability of this game. The corresponding configuration parameters that are accessible from the outside enable the definition of specific instantiations of PROTECT in the context of corresponding training scenarios that are specified within CTTP models (see (Frati & Prusa, 2019), subsection 3.2.4). These parameters will also allow the instantiation of specific games of PROTECT by the Training Tool via a REST API that will be provided by PROTECT (see (Hildebrandt, Bravos, & Goeke, D4.3: Training and Visualisation tools IO mechanisms v1, 2019), Section 5). The internal configuration parameters will enable the definition of difficulty levels for certain games of PROTECT that will be addressed in training scenarios defined in CTTP models (see (Frati & Prusa, 2019), subsection 3.2.4). Another major improvement is the ability to specify the content of cards by JSON files, instead of representing each card as a digital image. This feature enables a fast and uncomplicated creation of new card decks for PROTECT that are specific to certain training scenarios. It supports the representation of the THREAT-ARREST pilot scenarios by PROTECT.

Because the concept of AWARENESS QUEST includes different types of modes for two players, the motivation of the trainees to play the game will be additionally increased. The related concept for the continuously elicitation of current social engineering attacks will ensure that the learning content of AWRENESS QUEST will be always up-to-date.

The specified data protection policy will ensure that THREAT-ARREST will be compliant to the GDPR.

The future version of this deliverable in the form of the deliverable “D4.9 – THREAT-ARREST serious games v2” (M30) for task T4.2 will include the description of the implementation of AWARNESS QUEST and PROTECT to the designated TRL. The integration of the GUI of AWARNESS QUEST into the visualisation of the THREAT-ARREST platform will be substantiated in deliverable “D4.8 – THREAT-ARREST visualisation tools v2” (M30) for task T4.1. Regarding the deliverable “D4.11 – Training and Visualisation tools IO mechanisms v2” (M30) for task T4.6, a REST API for the instantiation of AWARNESS QUEST and a query of game results will be specified.

7 References

[1] Aladawy, D., Beckers, K., & Pape, S. (2018). *PERSUADED: Fighting Social Engineering Attacks with a Serious Game.* Springer.

[2] Beckers, K., & Pape, S. (2016). *A Serious Game for Eliciting Social Engineering Security Requirements.* IEEE Computer Society.

[3] Beckers, K., Pape, S., & Fries, V. (2016). *HATCH: Hack And Trick Capricious Humans - A Serious Game on Social Engineering.* ACM.

[4] BSI (Ed.). (2019). *Awareness-Poster - Psychotricks und Phishing-Maschen.* Retrieved August 23, 2019, from https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/partner/20190116_Awareness_Poster_SoSafe.pdf?__blob=publicationFile&v=3

[5] BSI (Ed.). (2019). *Infromationspool*. Retrieved August 23, 2019, from Alianz für Cyber-Sicherheit: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/_function/Informationspool_Formular.html?nn=6651414

[6] dpa. (2016, April 25). *Deutsche Industrie zieht Cyberkriminelle an*. (F. A. GmbH, Editor) Retrieved August 21, 2019, from XING: http://www.xing-news.com/reader/news/articles/264892?link_position=digest&newsletter_id=12800&xng_share_origin=email

[7] EUROPEAN PARLIAMENT, & COUNCIL OF THE EUROPEAN UNION. (2016). *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da.*

[8] Europol (Ed.). (2019). *Public Awareness and Prevention Guides*. Retrieved August 23, 2019, from EUROPOL: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides

[9] Franceschi-Bicchierai, L. (2016, February 8). *Hacker Publishes Personal Info of 20,000 FBI Agents*. Retrieved August 23, 2019, from VICE: https://www.vice.com/en_us/article/wnxdxq/hacker-publishes-personal-info-of-20000-fbi-agents

[10] Frati, F., & Prusa, J. (2019). D3.1: CTTP Models and Programmes Specification Language.

[11] Fysarakis, K., et al., 2014. Embedded systems security challenges. Measurable security for Embedded Computing and Communication Systems (MeSeCCS 2014), within the 4th International Conference on Pervasive and Embedded Computing and Communication Systems (PECCS 2014), 7-9 January 2014, Lisbon, Portugal, pp. 1-10.

[12] Goodin, D. (2017, April 20). *Chrome, Firefox, and Opera users beware: This isn't the apple.com you want*. (Condé Nast, Editor) Retrieved August 21, 2019, from arsTECHNICA: https://arstechnica.com/information-technology/2017/04/chrome-firefox-and-opera-users-beware-this-isnt-the-apple-com-you-want/

[13] Hesse, D. (2015). *Keine Geheimnisse mehr. - Methoden des Social Engineering.* Retrieved August 23, 2019, from https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/partner/150420_Partnerbeitrag_Riskworkers.pdf?__blob=publicationFile&v=4

[14] Hatzivasilis, G., et al., 2019. Review of Security and Privacy for the Internet of Medical Things (IoMT). 1st International Workshop on Smart Circular Economy (SmaCE), Santorini Island, Greece, 30 May 2019, IEEE, pp. 1-8.

[15] Hatzivasilis, G., 2017. Password-Hashing Status. Cryptography, MDPI Open Access Journal, vol. 1, issue 2, number 10, 2017.

[16] Hatzivasilis, G., et al., 2015. Password Hashing Competition – Survey and benchmark. Cryptology ePrint Archive, IACR, 2015/265.

[17] Hatzivasilis, G., et al., 2012. Building trust in ad hoc distributed resource-sharing networks using reputation-based systems. 16th Panhellenic Conference on Informatics (PCI 2012), IEEE, 5-7 October 2012, Piraeus, Greece, pp. 416-421.

[18] Hildebrandt, T., Bravos, G., & Goeke, L. (2019). D4.1: THREAT-ARREST Visualisation Tools v1.

[19] Hildebrandt, T., Bravos, G., & Goeke, L. (2019). *D4.3: Training and Visualisation tools IO mechanisms v1.* THREAT-ARREST.

[20] Lemos, R. (2013, August 21). *How Hacktivists Have Targeted Major Media Outlets*. (UBM, Editor) Retrieved August 21, 2019, from DARKReading: https://www.darkreading.com/vulnerabilities---threats/how-hacktivists-have-targeted-major-media-outlets/d/d-id/1140341

[21] Manifavas, C., et al., 2014. DSAPE – Dynamic Security Awareness Program Evaluation. Human Aspects of Information Security, Privacy and Trust (HCI International 2014), 22-27 June, 2014, Creta Maris, Heraklion, Crete, Greece, Springer, LNCS, vol. 8533, pp. 258-269.

[22] Peters, S. (2015, March 17). *The 7 Best Social Engineering Attacks Eve*. (UBM, Editor) Retrieved August 21, 2019, from DARKReading: https://www.darkreading.com/the-7-best-social-engineering-attacks-ever/d/d-id/1319411?_mc=RSS%5FDR%5FEDT&