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

D4.9: THREAT-ARREST serious games v2[†]

Abstract: This deliverable is the result of the second and last iteration of activities with respect to task "T4.2 – Serious gaming tools". It describes the concepts and implementation of the gaming tools AWARENESS QUIZ and PROTECT as well as their integration into THREAT - ARREST training scenarios. Additionally, the physical and multi-player card game HATCH is described. This second version updates the deliverable "D4.2 – THREAT-ARREST serious games v1" from month 12. Compared to D4.2, the main update considers the architecture of the AWARENESS QUIZ components and their implementation. Furthermore, improvements of PROTECT are described. Regarding HATCH, a new gaming scenario and a process for the creation of game scenarios are introduced.

Contractual Date of Delivery	28/02/2021
Actual Date of Delivery	28/02/2021
Deliverable Security Class	Public
Editor	*Ludger Goeke (SEA)*
Contributors	*Ludger Goeke, Sebastian Pape (SEA), George Tsakirakis (ITML)*
Quality Assurance	*George Hatzivasilis (FORTH), Martin Kunc (CZNIC)*

[†] *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. *Martin Kunc (CZNIC)*

Revisions

Version	Date	By	Overview
0.4	23/02/2021	Editor	Final version
0.3	22/02/2021	Editor	Addressed comments from FORTH and CZNIC
0.2	17/02/2021	Ludger Goeke	First Draft
0.1.5	16/02/2021	Ludger Goeke	Update of content for PROTECT
0.1.4	15/02/2021	George Tsakirakis	Update of the content for trainee performance assessment design for serious games
0.1.3	11/02/2021	Sebastian Pape	Adding process for systematic scenario creation for HATCH
0.1.2	03/02/2021	Ludger Goeke	Description of AWARENESS QUIZ implementation
0.1.1	27/01/2021	Ludger Goeke	Adding HATCH shipping scenario
0.1	11/01/2021	Editor	First Draft

Executive Summary

This document represents the second and last iteration of activities regarding the task "T4.2 – Serious gaming tools". It represents an update and extension of the content of the first version "D4.2 – THREAT-ARREST serious games v1" and 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 QUIZ and PROTECT, which are part of the Gamification Tool in the THREAT-ARREST platform, 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 the representation of training results in the user interface of the Training Tool. The deliverable describes also, how the gaming tools AWARENESS QUIZ and PROTECT will be integrated into training scenarios. 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 connection, appropriate data privacy policies are specified.

Within Work Package (WP) 4, the deliverable "D4.9 – THREAT-ARREST serious games v2" focuses on the concepts and implementation of the serious games and their conceptual integration into the training scenarios of THREAT-ARREST. The integration of the graphical user interfaces (GUIs) of the gaming tools into the visualisation of the THREAT-ARREST platform is considered in the deliverable "D4.8 – THREAT-ARREST Visualisation Tools v2" (Hildebrandt, et al., 2021). The discussion of the technical interaction of the gaming tools as part of the Gamification Tool with the Training Tool is contained in deliverable "D4.11 – Training and Visualisation tools IO mechanisms v2" (Koshutanski, et al., 2021). This discussion considers the initialization of the gaming tools and the transmission of results of finished games. The deliverable "D3.1 – CTTP Models and Programmes Specification Language" (Fysarakis, et al., 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 serious gaming part of the THREAT-ARREST project. The serious gaming comprises serious games for training people in relation to the topic of social engineering. These serious games can be distinguished in the online games AWARENESS QUIZ (the name has been changed from AWARENESS QUEST to AWARENESS QUIZ) (Pape et al., 2020) and PROTECT (Goeke et al., 2019) as well as the physical card game HATCH (Beckers & Pape, 2016).

The online games AWARENESS QUIZ and PROTECT are provided within the THREAT-ARREST training platform by the Gamification Tool. In the following, AWARENESS QUIZ and PROTECT are also referred by the term *gaming tools*. The usage of the gaming tools is integrated in the THREAT-ARREST training programmes. A Gaming Tool is invoked by the Training Tool whereby the necessary information for the instantiation of a game is provided by the passed CTTP model. After a game has finished, the game results are communicated to the Training Tool via a message broker.

The serious game HATCH represents a physical card game which 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 QUIZ, and PROTECT. For the gaming tools AWARENESS QUIZ and PROTECT, their implementation and integration into the THREAT-ARREST training scenarios is discussed. Regarding the AWARENESS QUIZ, a process for the creation of quiz content is introduced, including the definition of metadata types for describing the content.
- 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 Tool 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 the integration of the gaming tools AWARENESS QUIZ and PROTECT within THREAT-ARREST training scenarios.
- Section 6 contains the conclusion of this deliverable.

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

Compared to initial deliverable D4.2, the main update is the description of the different components of AWARENESS QUIZ and their implementation. Furthermore, the definition of types of metadata for tagging questions and answers within the AWARENESS QUIZ are provided. Another important update with respect to AWARENESS QUIZ addresses the integration of AWARENESS QUIZ into THREAT-ARREST training scenarios.

Regarding PROTECT, this deliverable describes improvements of its graphical user interface and functionality. For HATCH, a newly realized game scenario and a new process for creating new game scenarios are introduced.

The content for the trainee performance assessment design is adapted to the latest state of the THREAT-ARREST platform and it is referring now to the concrete implementation of the Training Tool.

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 QUIZ (the name of the quiz game has changed from AWARENESS QUEST to AWARENESS QUIZ) and PROTECT are online games. The AWARENESS QUIZ (see subsection 2.2) is a quiz game that allows different single 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, 2016)
2. Training of awareness against Social Engineering attacks (Beckers, et al., 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, 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, 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.

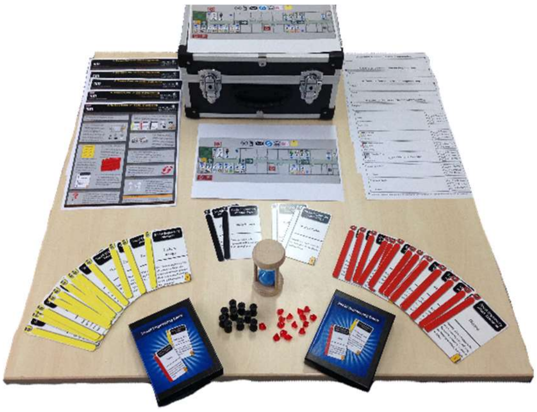
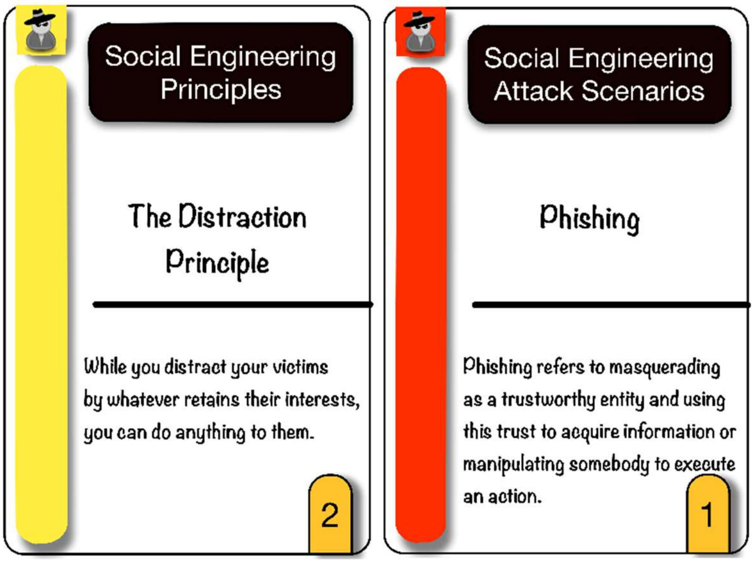


Figure 2: HATCH Material

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.



Social Engineering Principles

The Distraction Principle

While you distract your victims by whatever retains their interests, you can do anything to them.

2

Social Engineering Attack Scenarios

Phishing

Phishing refers to masquerading as a trustworthy entity and using this trust to acquire information or manipulating somebody to execute an action.

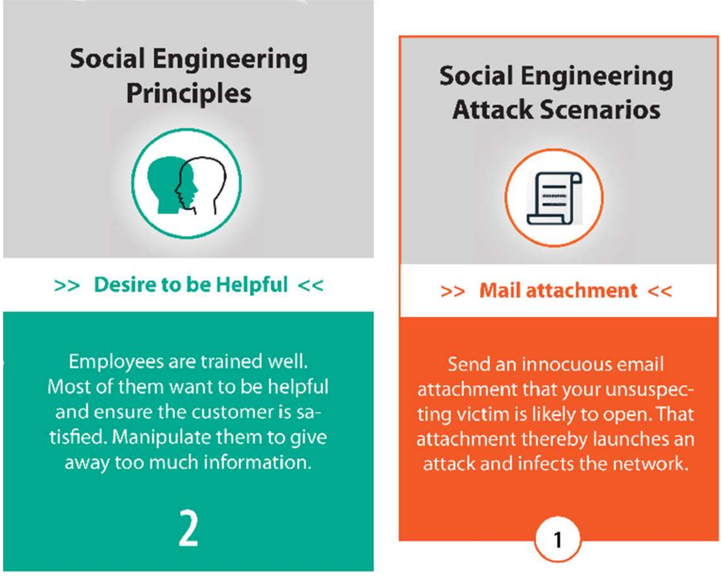
1

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.



Social Engineering Principles
>> Desire to be Helpful <<

Employees are trained well. Most of them want to be helpful and ensure the customer is satisfied. Manipulate them to give away too much information.

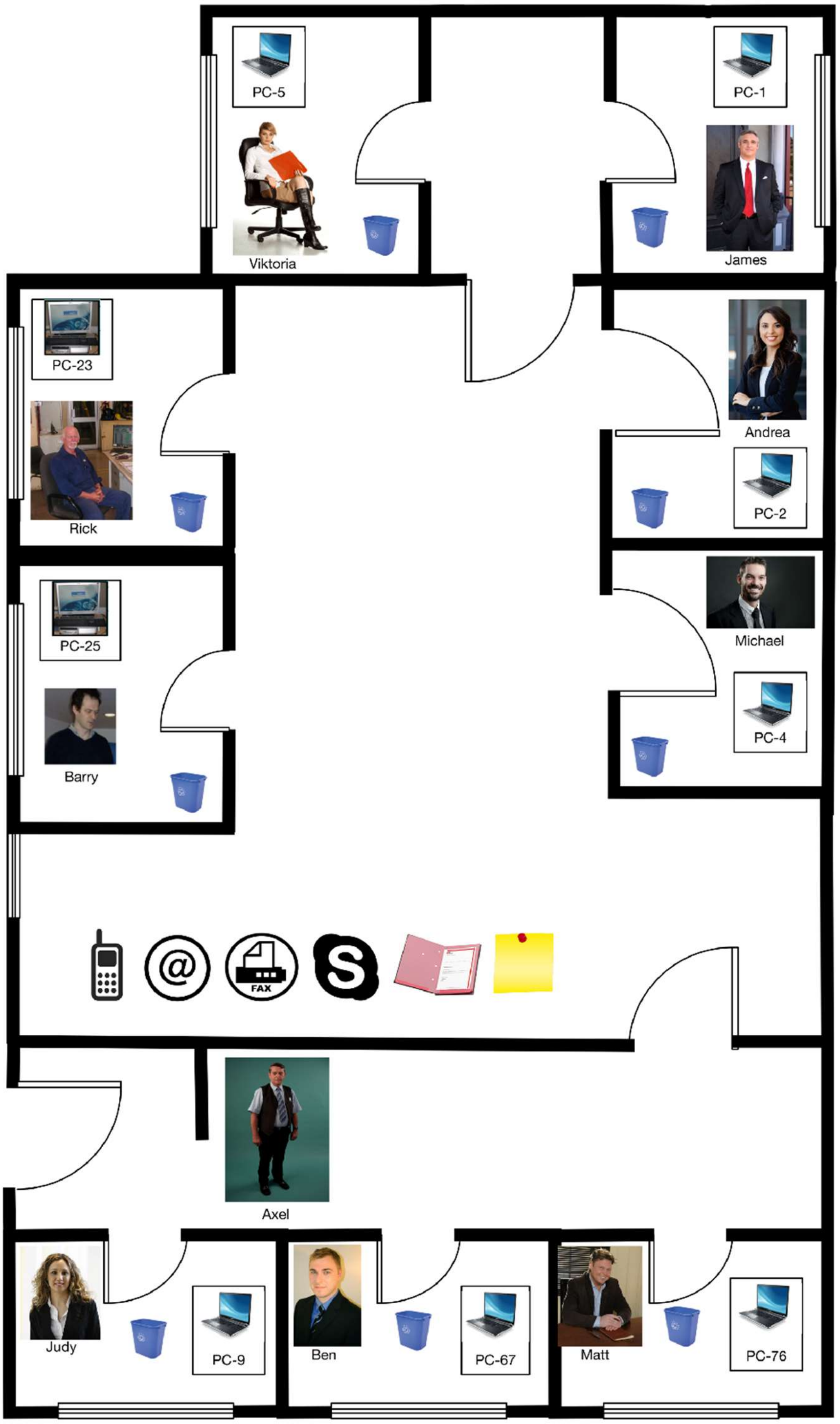
2
Social Engineering Attack Scenarios
>> Mail attachment <<

Send an innocuous email attachment that your unsuspecting victim is likely to open. That attachment thereby launches an attack and infects the network.

Figure 4: New Layout for HATCH Cards

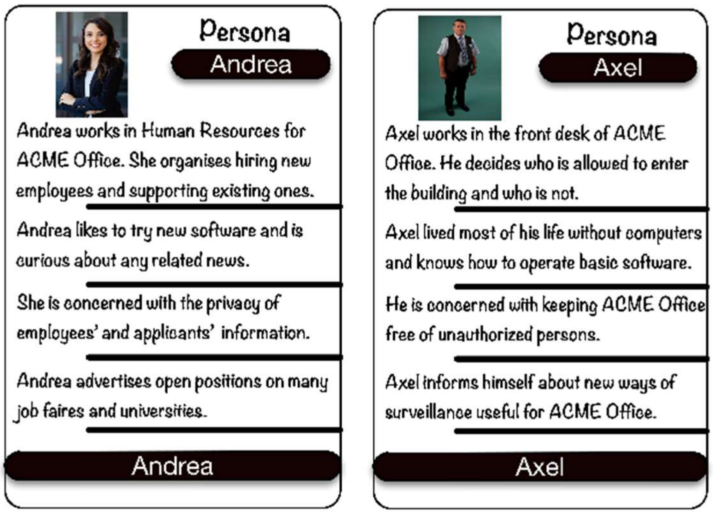
2.1.3 Planned Novel Game Scenarios

So far, there exist three different scenarios (Beckers & Pape, 2016): 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.



mage Sources: https://flic.kr/p/59RKQF, https://flic.kr/p/sxfTtv, https://flic.kr/p/qzhTFo, https://flic.kr/p/ https://flic.kr/p/csWjm9, https://flic.kr/p/84K4fC, https://flic.kr/p/bBdDe67ZUUv9, https://flic.kr/p/Ch2gjk

Figure 5: HATCH Game Plan



Persona
Andrea

Andrea works in Human Resources for ACME Office. She organises hiring new employees and supporting existing ones.

Andrea likes to try new software and is curious about any related news.

She is concerned with the privacy of employees' and applicants' information.

Andrea advertises open positions on many job faires and universities.

Andrea

Persona
Axel

Axel works in the front desk of ACME Office. He decides who is allowed to enter the building and who is not.

Axel lived most of his life without computers and knows how to operate basic software.

He is concerned with keeping ACME Office free of unauthorized persons.

Axel informs himself about new ways of surveillance useful for ACME Office.

Axel

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 Shipping Scenario

In the context of the THREAT-ARREST project, SEA provided several sessions of HATCH at the 6th NIS summer school 2019 on Crete, Greece. Therefore, SEA created a new game scenario which considers, corresponding to the THREAT-ARREST pilot smart shipping, the sector of shipping. This scenario considers the fictional container vessel "Valentina", its crew, and responsible personnel onshore. SEA created a new game plan which represents the vessel and its crucial systems which could be targets for social engineering attacks (see Figure 7). Additionally, SEA conceptualized new persona cards for the crew of the Valentina which represent the captain (see Figure 8), 1st officer, 2nd officer, chief engineer, cook, as well as a deck cadet, a boatswain, and a maintenance worker. The persona cards with respect to the ashore personnel are comprised by an operator (see Figure 9) and a port agent.

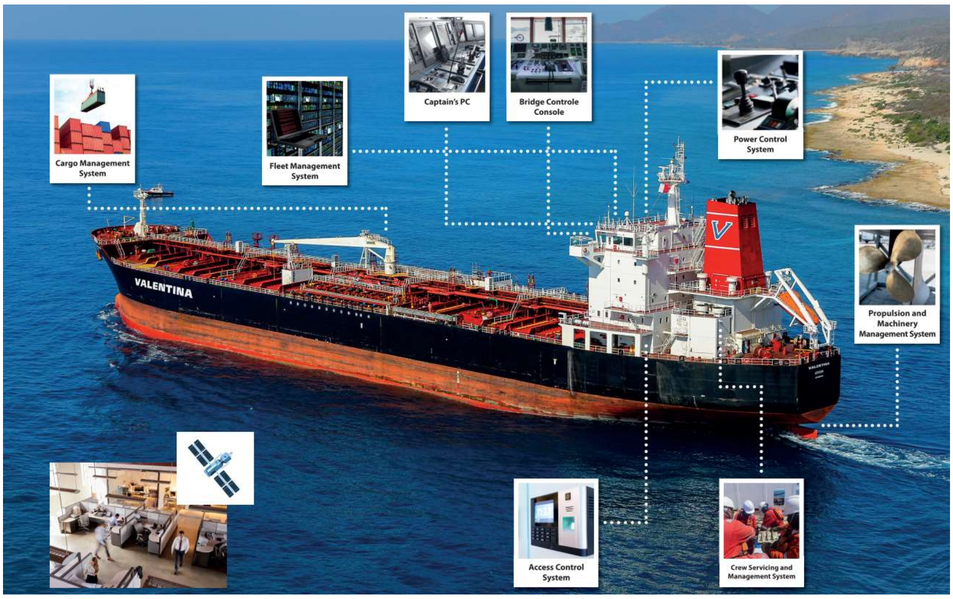
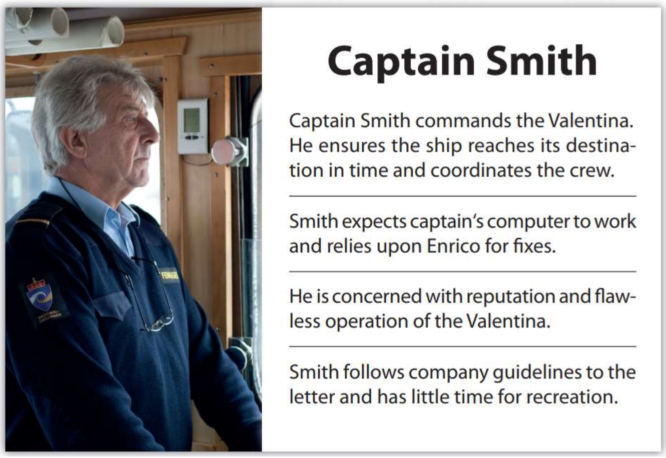


Figure 7: HATCH game plan for shipping scenario



Captain Smith

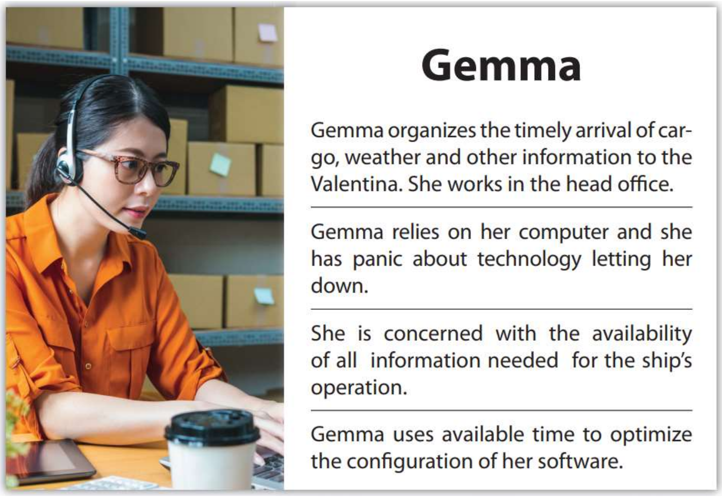
Captain Smith commands the Valentina. He ensures the ship reaches its destination in time and coordinates the crew.

Smith expects captain's computer to work and relies upon Enrico for fixes.

He is concerned with reputation and flawless operation of the Valentina.

Smith follows company guidelines to the letter and has little time for recreation.

Figure 8: Persona card of the crew representing the captain of the Valentina



Gemma

Gemma organizes the timely arrival of cargo, weather and other information to the Valentina. She works in the head office.

Gemma relies on her computer and she has panic about technology letting her down.

She is concerned with the availability of all information needed for the ship's operation.

Gemma uses available time to optimize the configuration of her software.

Figure 9: Persona card of the ashore personnel representing an operator

2.1.5 Systematic Scenario Creation

To allow a systematic way of creating new scenarios, we propose a method to create specific scenarios for HATCH by considering domain-specific properties (Hazilov & Pape, 2020). Our method is based on the work of Faily and Flechais (Faily & Flechais, 2011), who created personas utilizing grounded theory.

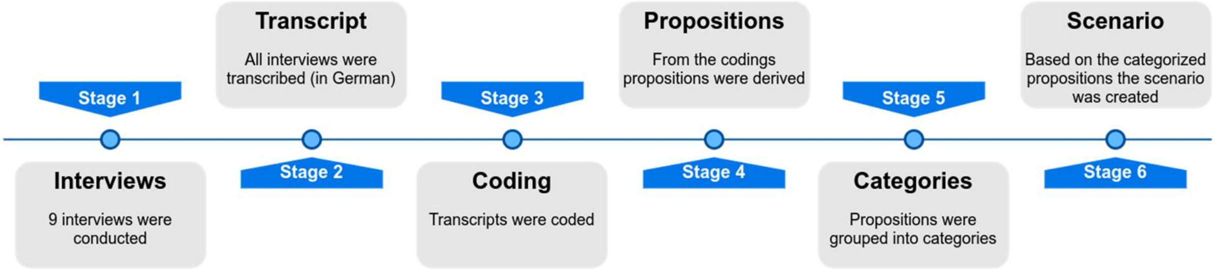

Stage 1
Interviews
9 interviews were conducted
Stage 2
Transcript
All interviews were transcribed (in German)
Stage 3
Coding
Transcripts were coded
Stage 4
Propositions
From the codings propositions were derived
Stage 5
Categories
Propositions were grouped into categories
Stage 6
Scenario
Based on the categorized propositions the scenario was created

Figure 10: Process of creating a new HATCH scenario

Figure 10 shows the process of creating a new scenario. In Stages 1-3, interviews are conducted, transcribed and coded. Following Faily and Flechais' method for developing personas, we developed propositions from codes (Stage 4), such as *'more consultants are hired for project than clients'*, *'with the exception of client's assistants, consultants are generally younger'* and *'generally, the consulting team consists of 4 to 5 people'*. These propositions were summarized, assigned to concepts and categorized (Stage 5). As the last step, appropriate propositions were selected and stated as potential characteristics of a persona to write persona narratives and develop the scenario (Stage 6). For this purpose, all personas-related concepts and propositions were reviewed again, in order to identify most valuable and meaningful insights, and later embodied into future personas. For example, the propositions from the concepts 'roles' and 'age' lead to the decision of having more consulting personas (4) than personas of the client company (3). Furthermore, with the exception of the client's assistant, all consulting personas are younger than personas of the client. In the same manner, propositions were used to develop professional consultants' working environment and surroundings.

2.1.6 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 QUIZ

2.2.1 Short Description

We decided to change the name of the game AWARENESS QUEST (see (Goeke, et al., 2019), subsection 2.2) to AWARENESS QUIZ because this name better describes the characteristics of the game.

Security awareness made fun and lightweight is the goal of the AWARNESS QUIZ, 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 QUIZ contains a set of questions that allows 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. We elaborate on how we plan to organize the content management for the AWARNESS QUIZ 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. 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. The game is an electronic game because of these permanent updates an implementation as a physical game would not be possible.

The objective of the game is to sensitize employees for the threats and negative consequences through social engineering attacks. To this, a question describes a scenario of a real-world attack in an abstract way and asks for the biggest threats in the scenario. The correct answers represent impacts which result from a successful execution of the considered attack. Thus, incorrect answers represent consequences which cannot result from the attack (Pape, et al., 2020).

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

- *Predefined Quiz*: A player plays alone with a predefined quiz. Here, the set of questions deals with certain aspects in order to convey knowledge regarding a specific context. For example, the questions of a quiz could consider attacks which target a particular industry sector. Compared to version 1 of this deliverable (Goeke, et al., 2019), the name of this mode has changed from *Single Quest* to *Predefined Quiz* because this name better represents the characteristics of the quiz mode.
- *Context Quiz*: In this single player quiz, the set of questions for a quiz is compiled on the fly based on information which represents the interests of the player. This quiz mode can be used by players to increase their knowledge with respect to specific attack types or to keep their knowledge regarding new attacks up to date. For example, a quiz could contain only questions about attacks which are executed by using emails or all new attacks which have been executed from a certain date onwards. The name of this mode has changed from *Context Quest* to *Context Quiz* related to the change of the game name to AWARENESS QUIZ. This feature could be also utilized by the Adaptation Tool in order to adapt the training process based on the trainee's demands ("D4.10 – CTTP Programme Adaptor v2").

The single player game is meant to have a learning curve with a slow degree of increase in difficulty. This will keep the flow of players at a constant pace. In the first version of the platform (D4.2), the additional multiplayer modes *Versus Quest*, *Pick Quest* and *Draw Quest* had been conceptualized (see (Goeke, et al., 2019), subsection 2.2.2). During the subsequent design phase, it became apparent that these multiplayer modes are not appropriate in the context of the THREAT-ARREST training programmes. On the one hand, it became visible that the learning objectives are better achieved with the single player quizzes. On the other hand, the organizational effort to plan and schedule the quiz duels for the employees of a company would be inappropriate. Nevertheless, the motivation and a positive competition between the players is also achieved by the single player modes because the employees of a company can compare their results and can discuss the played attack scenarios among each other.

2.2.3 Integration of Real Attacks into the Game

The game will rely on the same technical specifications as PROTECT. The presentation will be offered by a WEB GUI which will be optimized for smart phones and desktop computers. The persistent data storage will be a database which is hosted in the THREAT-ARREST platform. In this context, the database only stores quizzes with the corresponding questions and answers, as well as the definition of metadata types. The user data and scores of players is stored within the Training Tool.

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 (Anon., 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.
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.

[1] https://www.rfc-editor.org/rfc/rfc3492.txt

[2] https://www.apple.com/

[3] https://www.apple.com/

Webpage/Article/Document	Description
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, et al., 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.
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 (Anon., 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 (Anon., 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, 2019) and (Hesse, 2015)).
Falsche Polizei am Telefon (translation of the author: Wrong police at the telephone)	The post (Anon., 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.

These table has been extended internally during the project duration. Especially with respect to sources which address social engineering attacks in the context of the COVID-19 pandemic. The URL to a particular source will be represented for each question in the AWARENESS QUIZ itself.

Figure 11 illustrates the process that we will follow to identify and prepare social engineering attacks. We will in regular intervals query established sources for attacks similar to the ones listed beforehand (see Figure 11, step 1). Afterwards, we will formulate an abstracted question scenario based on the attack source (see Figure 11, step 2). The created question is tagged with metadata which describes the characteristics of the attack (see Figure 11, step 3). For example, the category of an attack could be "baiting" and the targeted industry sector could be the

[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

"shipping domain". The definition of the different types of metadata is described in detail in subsection 2.2.4. Next, if available, corresponding correct answers, which represent an impact of the considered attack, are selected from the pool of predefined answers and are refined if necessary (see Figure 11, step 4). If the answer pool should not contain appropriate answers, new answers are created and tagged with metadata regarding the attack category. The same tasks are performed for the association of incorrect answers, which describe impossible outcomes of the attack (see Figure 11, step 5). Finally, the created question, depending on its topic, can be added to a new quiz or integrated into an existing quiz (see Figure 11, step 6). The described process ensures that all attacks in AWARNESS QUIZ do refer to real reports of social engineering attacks from credible sources.

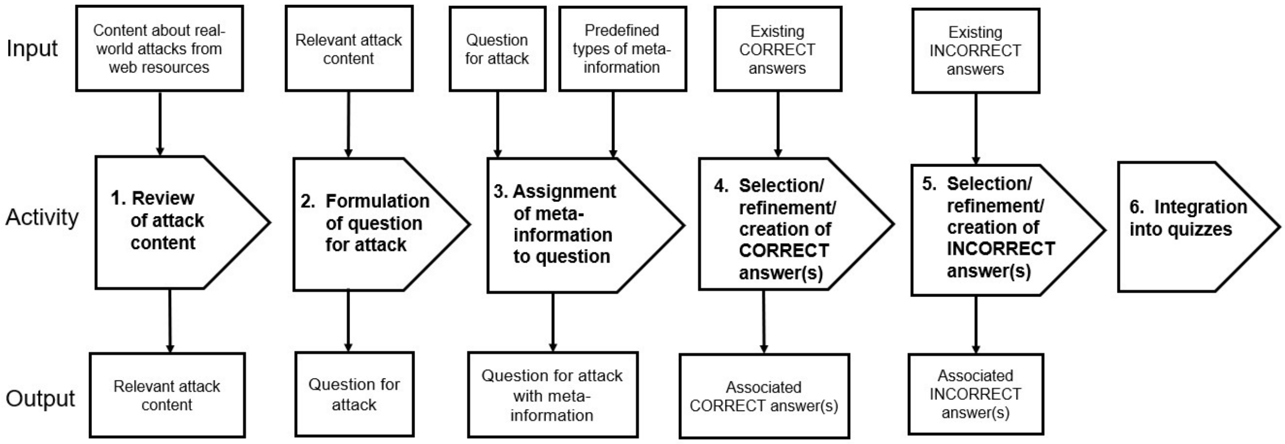

Input
Activity
Output
Content about real-world attacks from web resources
1. Review of attack content
Relevant attack content
Relevant attack content
2. Formulation of question for attack
Question for attack
Question for attack
Predefined types of meta-information
3. Assignment of meta-information to question
Question for attack with meta-information
Existing CORRECT answers
4. Selection/ refinement/ creation of CORRECT answer(s)
Associated CORRECT answer(s)
Existing INCORRECT answers
5. Selection/ refinement/ creation of INCORRECT answer(s)
Associated INCORRECT answer(s)
6. Integration into quizzes

Figure 11: AWARENESS QUIZ Attack Source Analysis (cf. (Pape, et al., 2020), Fig. 4)

2.2.4 Specification of Metadata Types

As already mentioned in the context of the process for attack source analysis (see Figure 11), the questions and answers within the AWARENESS QUIZ are tagged with metadata of predefined types. These metadata can be used for the following use cases:

- Identification of relevant existing questions during the creation of a quiz for a certain topic.
- Identification of suitable existing answers for a newly created question.
- On the fly compilation of a set of existing questions for a Context Quiz (see subsection 2.2.2) based on provide metadata.

A metadata type is defined by the following properties:

- *Name of metadata type:* Specifies the name of a metadata type;
- *Description:* Describes the logical meaning of the metadata type;
- *Multiplicity:* Specifies the number of metadata items which must be assigned to a question or answer at least and can be assigned at most;
- *Value type:* Defines if a metadata value is represented as a string, numeric, or date value;
- *Predefined values:* Specifies predefined values for metadata types whose values are represented as strings;

- *Extensible values:* This Boolean value defines if the set of predefined values:
  - can be extended by new values, which means that there are no restrictions to the used metadata values for the metadata type, or
  - cannot be extended, which means that only the predefined values can be used as potential metadata values for the metadata type.

Table 3 shows the definition of metadata types for questions.

Table 3: Definition of metadata types for tagging questions

Name of metadata type	Description	Multi-plicity	Value type	Predefined values	Exten-sible values
Type of attack execution	Specification if an attack is executed: (i) *directly* on site by an attacker (e.g. an attacker tries to get access to a secured area by pretending to be business partner who has an appointment) (ii) *indirectly* by using a technical medium (e.g. vishing by phone, phishing via email) or (iii) combinations of direct and/or indirect executions	1..2	String	Directly, Indirectly	no
Attack category	Categories by which an attack is typified	1..*	String	Phishing, Spear Phishing, Whaling, Business Email Compromise, Vishing, Shoulder Surfing, Dumpster Diving, etc.	yes
Type of attacker	Types the executer of an attack	1..*	String	Fraudster, Cyber Criminal, Intelligence Service, Hacker, etc.	yes
Feigned identity	Defines the identity of the entity/person which/who is feigned by the attacker during an attack	1..*	String	Bank, Tax Authority, CEO, Cousin	yes
Context of victims	Specifies the context of the victims who are targeted by an attack	1..2	String	Individual, Organisation	no
Min age of victim	Minimum age of targeted victims	0..1	Numeric	not relevant	not relevant
Max age of victim	Maximum age of targeted victims	0..1	Numeric	not relevant	not relevant
Gender of victim	Gender of targeted victims	1..3	String	Female, Male, Transgender	no
Interests of victim	Interests of targeted victims	0..*	String	Cooking, Gaming, Programming, Soccer, Traveling, Pets, Handicrafts, Science Fiction, Literature, etc.	yes
Internet usage of victim	Characteristics regarding the internet usage of designated victims	0..*	String	Occasional, Often, Only for Shopping, etc.	yes

Name of metadata type	Description	Multi-plicity	Value type	Predefined values	Exten-sible values
Sector[9]	Specification of the sector/industry of organisations which are targeted by an attack	0..*	String	Shipping domain, State Institutions, Energy Suppliers, Financial Institutes, etc.	yes
Department[9]	Defines certain departments of an organisation which are affected by an attack	0..*	String	Finance, Human Resources, IT, etc.	yes
Role[9]	Indicates roles of employees of an organisation which are targeted by an attack	0..*	String	Financial Accountant, CEO, Administrator, etc.	yes
Motivation for attack	Specifies the motivation for executing an attack	1..*	String	Espionage, Criminal Intend, Interest in Hacking, etc.	yes
Objective of attack	Defines the objective of an attack	1..*	String	Illegal Financial Transactions, Gaining of sensitive Information Data, Identity Theft, etc.	yes
Exploited psychological pattern	Psychological pattern which is tried to be exploited by an attack	1..*	String	Authority, Good Faith, Laziness, Fear etc.	yes
Used technology	Technology which has been used during the attack	0..*	String	Telephone, Email, etc.	yes
Geographical spreading	The geographical area where the attack has been conducted	1..*	String	Worldwide, Europe, Italy, Crete, Apulia, Madrid, etc.	yes
Start of attack period	Start of the time period in which the attack has been executed	0..1	Date	not relevant	not relevant
Start of attack period	End of the time period in which the attack has been executed	0..1	Date	not relevant	not relevant

[9] CONDITION: This parameter shall only be used when the parameter *Context of victims* contains the value *Organization*

Answers are only tagged by metadata values of the type *Attack category* (see Table 4). This allows a proposal of predefined answers which could fit potentially to a newly created question of a certain attack category.

Table 4: Definition of metadata types for tagging answers

Name of metadata type	Description	Multi-plicity	Values Type	Predefined values	Extensible values
Attack category	Categories by which an attack is typified	1..*	String	Phishing, Spear Phishing, Whaling, Business Email Compromise, Vishing, Shoulder Surfing, Dumpster Diving, etc.	yes

2.2.5 Overview AWARENESS QUIZ Components

This section discusses the different components of the AWARENESS QUIZ. The main components in the form of the *Quiz Game* and the *Quiz Manager* are shown in Figure 12. The component Quiz Game represents the actual quiz which is played by a trainee in the context of a training program. The Quiz Manager allows the game content editor to create, edit, and manage: (i) quizzes, (ii) questions, (iii) answers, and (iv) metadata types. To this, the game content editor logs in to the Trainer GUI of the Training Tool and can from there open the Quiz Manger.

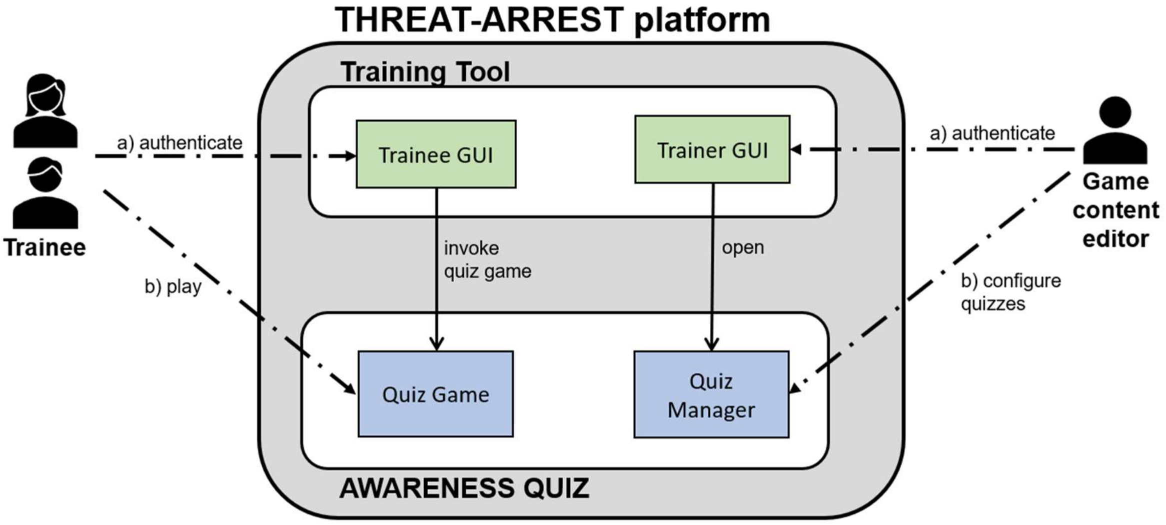


Figure 12: AWARENESS QUIZ components

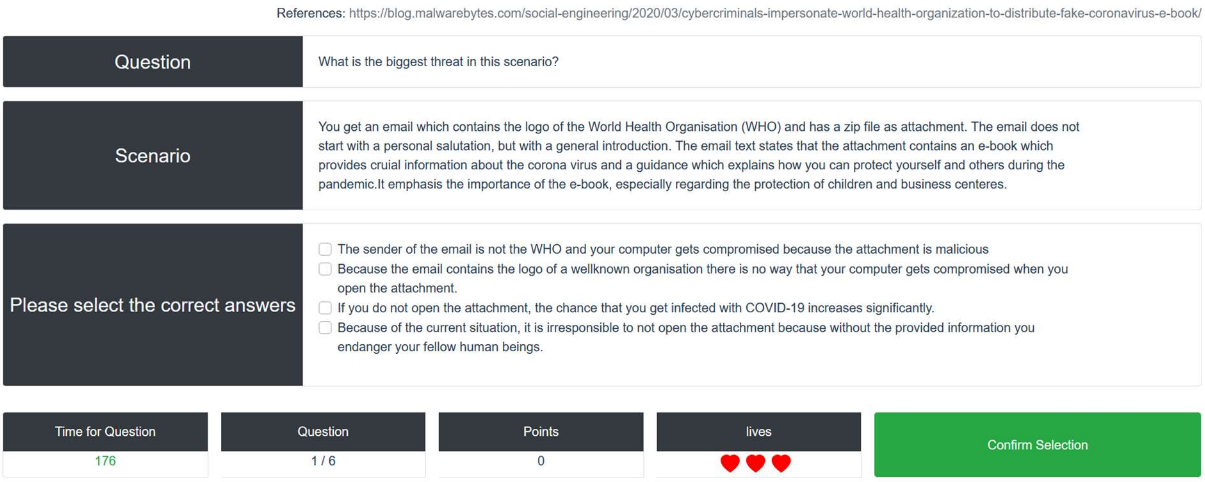
The Quiz Game is described further in subsection 2.2.6. In subsection 2.2.7 the Quiz Manager is discussed in detail.

2.2.6 Quiz Game

This section discusses the concepts and implementation of the *Quiz Game* component which realizes the playing of the actual quizzes within AWARENESS QUIZ. Figure 13 shows the representation of a question during a running quiz in the graphical user interface (GUI) of the *Quiz Game*.

As it has already been mentioned, the questions of a quiz are based on real-world attacks. The displayed question in Figure 13 is based on an email campaign with malicious attachments which was executed at the beginning of the COVID-19 pandemic (Threat Intelligence Team, 2020). In this context, the sent email pretends to origin from the *World Health Organisation*[10] (WHO) and to provide an e-book in the attachment which includes crucial information and guidance with respect to the coronavirus. The email text emphasizes the importance of the information in the e-book, especially regarding the protection of children and business centre (cf. (Threat Intelligence Team, 2020)). When the file of the e-book is opened inside the attached *zip* archive, a malware is downloaded on the computers of the victims.

Within the Quiz Game, this attack scenario is explained in an abstract way (see Figure 13, text field *Scenario*). The reference to the source for the scenario is provided to the player top right in the GUI (see Figure 13). This allows and shall motivate the players to do further own research regarding an attack which leads to a deeper understanding of the attack and its consequences. The actual question asks for the biggest threat(s) in the explained scenario (see Figure 13, text field *Question*). A player has to select the correct answer(s) from the set of provided answers (see Figure 13, *Please select the correct answers* selectable text fields). Here, the correct answer(s) present an impact which can be caused by the attack. Incorrect answers describe impacts which are not possible due to the attack. With regard to the scenario in Figure 13, only the answer "The sender of the email is not the WHO and your computer gets compromised when you open the attachment" is correct.



References: https://blog.malwarebytes.com/social-engineering/2020/03/cybercriminals-impersonate-world-health-organization-to-distribute-fake-coronavirus-e-book/

Question: What is the biggest threat in this scenario?

Scenario: You get an email which contains the logo of the World Health Organisation (WHO) and has a zip file as attachment. The email does not start with a personal salutation, but with a general introduction. The email text states that the attachment contains an e-book which provides cruial information about the corona virus and a guidance which explains how you can protect yourself and others during the pandemic.It emphasis the importance of the e-book, especially regarding the protection of children and business centeres.

Please select the correct answers

- □ The sender of the email is not the WHO and your computer gets compromised because the attachment is malicious
- □ Because the email contains the logo of a wellknown organisation there is no way that your computer gets compromised when you open the attachment.
- □ If you do not open the attachment, the chance that you get infected with COVID-19 increases significantly.
- □ Because of the current situation, it is irresponsible to not open the attachment because without the provided information you endanger your fellow human beings.

Time for Question	Question	Points	lives
176	1 / 6	0	♥♥♥

Figure 13: Representation of a question in the Quiz Game GUI during a quiz

By the creation of a question, its level of difficulty is defined by the value of the *weighting* parameter (see subsection 2.2.7.2). The weighting value can be used when the questions for a context quiz shall have certain levels of difficulty.

During a quiz, a player has to answer the corresponding set of questions by selecting the correct answers for each question. The player has a certain amount of time to answer a question. When a question is answered correctly, the score is increased by a predefined number of points. An

[10] https://www.who.int/

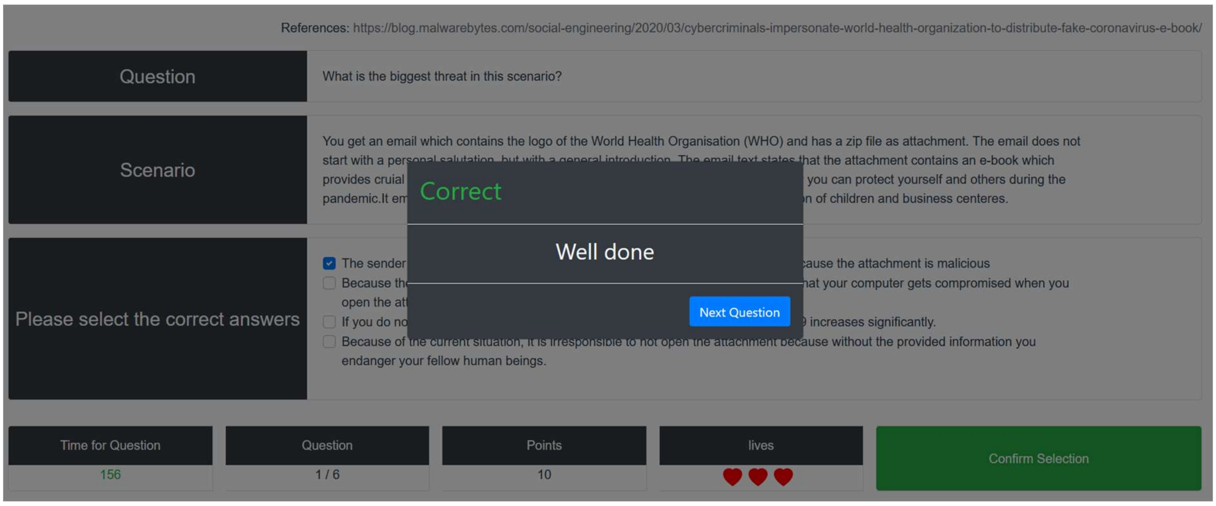
incorrect answer or a non-answering of the question in the given time causes a decrease of the score by a predefined number of points and the loss of a life. A quiz is won when all its questions have been answered. A quiz is lost when a player has lost all his/her lives.

At the bottom of the Quiz Game GUI starting from left, the following information is presented to the player:

- *Time for Question:* Remaining time for answering the current question;
- *Question*: Total number of questions in a quiz and the number of played questions, including the current question;
- *Points*: Current score;
- *Lives*: Number of remaining lives.

The selection of answers for a question is confirmed by clicking the *Confirm Selection*-button which is placed bottom right in the Quiz Game GUI (see Figure 13).

The game flow of a quiz is supported by appropriate dialogs which provide necessary information and instructions to the player. Figure 14 shows the dialog which is displayed after a question has been answered correctly. It informs the player that the question has been answered correctly and that he/she can continue the quiz by pressing the *New Question*-button.



References: https://blog.malwarebytes.com/social-engineering/2020/03/cybercriminals-impersonate-world-health-organization-to-distribute-fake-coronavirus-e-book/

Question: What is the biggest threat in this scenario?

Scenario: You get an email which contains the logo of the World Health Organisation (WHO) and has a zip file as attachment. The email does not start with a personal salutation, but with a general introduction. The email text states that the attachment contains an e-book which provides cruial … you can protect yourself and others during the pandemic.It em… n of children and business centeres.

Please select the correct answers

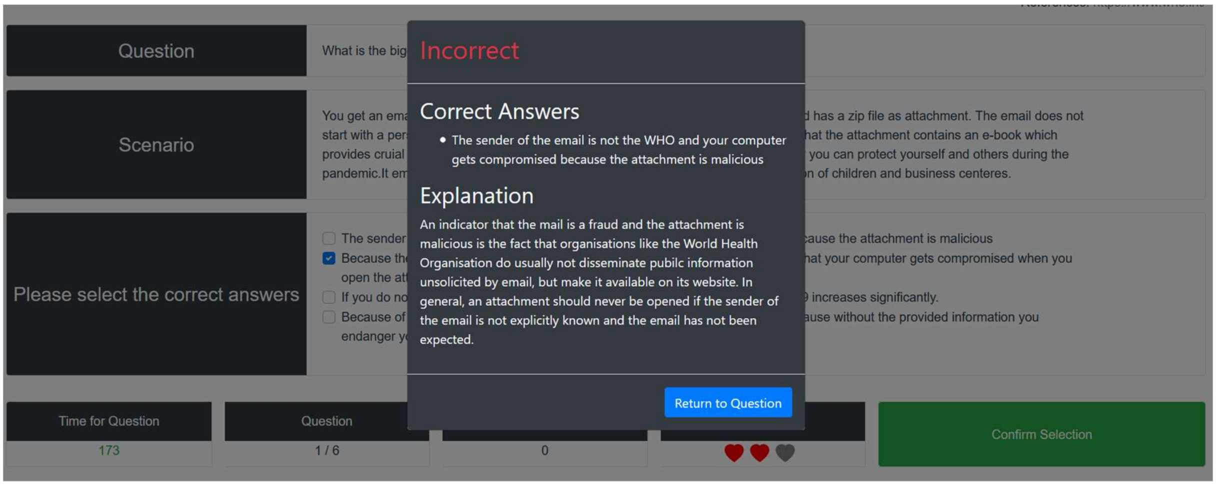
☑ The sender … cause the attachment is malicious
☐ Because th… hat your computer gets compromised when you open the at…
☐ If you do no… 9 increases significantly.
☐ Because of the current situation, it is irresponsible to not open the attachment because without the provided information you endanger your fellow human beings.

Correct

Well done

Figure 14: Dialog after a question has been answered correctly

After a question has been answered incorrectly, the corresponding dialog provides the correct answer(s) and an explanation of the attack scenario (see Figure 15). When the player clicks on the *Return to question*-button the dialog closes and he/she returns to the question (see Figure 16). Thus, the player is given the opportunity to analyse the correct and wrong answers. The quiz continues after the player has clicked the *New Question*-button.



Incorrect

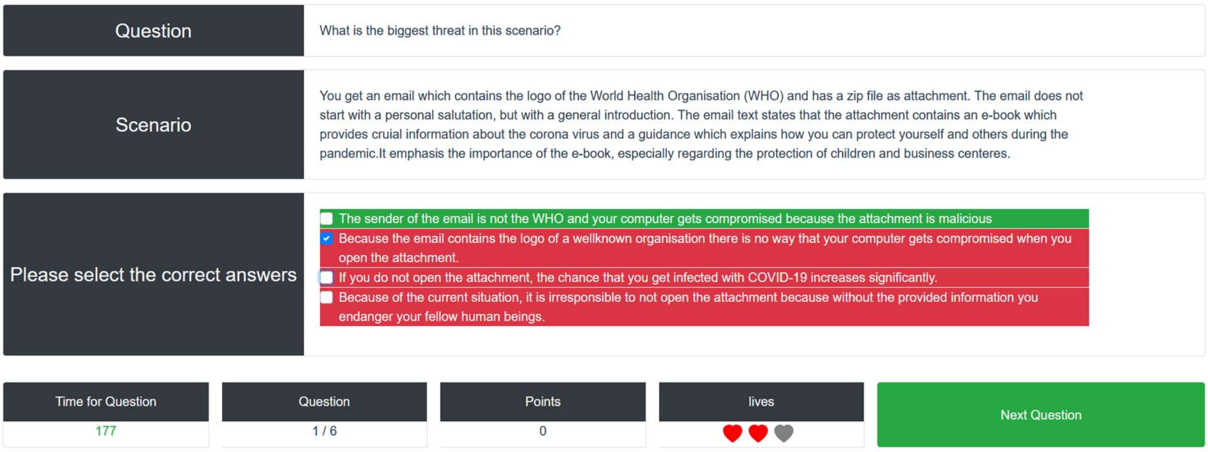
Correct Answers

- The sender of the email is not the WHO and your computer gets compromised because the attachment is malicious

Explanation

An indicator that the mail is a fraud and the attachment is malicious is the fact that organisations like the World Health Organisation do usually not disseminate pubilc information unsolicited by email, but make it available on its website. In general, an attachment should never be opened if the sender of the email is not explicitly known and the email has not been expected.

Figure 15: Dialog after a question has been answered incorrectly



Question	What is the biggest threat in this scenario?
Scenario	You get an email which contains the logo of the World Health Organisation (WHO) and has a zip file as attachment. The email does not start with a personal salutation, but with a general introduction. The email text states that the attachment contains an e-book which provides cruial information about the corona virus and a guidance which explains how you can protect yourself and others during the pandemic.It emphasis the importance of the e-book, especially regarding the protection of children and business centeres.
Please select the correct answers	□ The sender of the email is not the WHO and your computer gets compromised because the attachment is malicious ☑ Because the email contains the logo of a wellknown organisation there is no way that your computer gets compromised when you open the attachment. □ If you do not open the attachment, the chance that you get infected with COVID-19 increases significantly. □ Because of the current situation, it is irresponsible to not open the attachment because without the provided information you endanger your fellow human beings.

Time for Question	Question	Points	lives	Next Question
177	1 / 6	0	♥♥♥	

Figure 16: Repeated display of a question after an incorrect answer

The different parameters regarding the invocation of a quiz game are configurable. These configuration parameters are described in detail in subsection 5.1.

2.2.7 Quiz Manager

The *Quiz Manager* enables the management of:

- quizzes,
- questions,
- answers, and
- metadata types.

These different types of information are stored in a pool, each of which can be edited by a corresponding editor (see Figure 17).

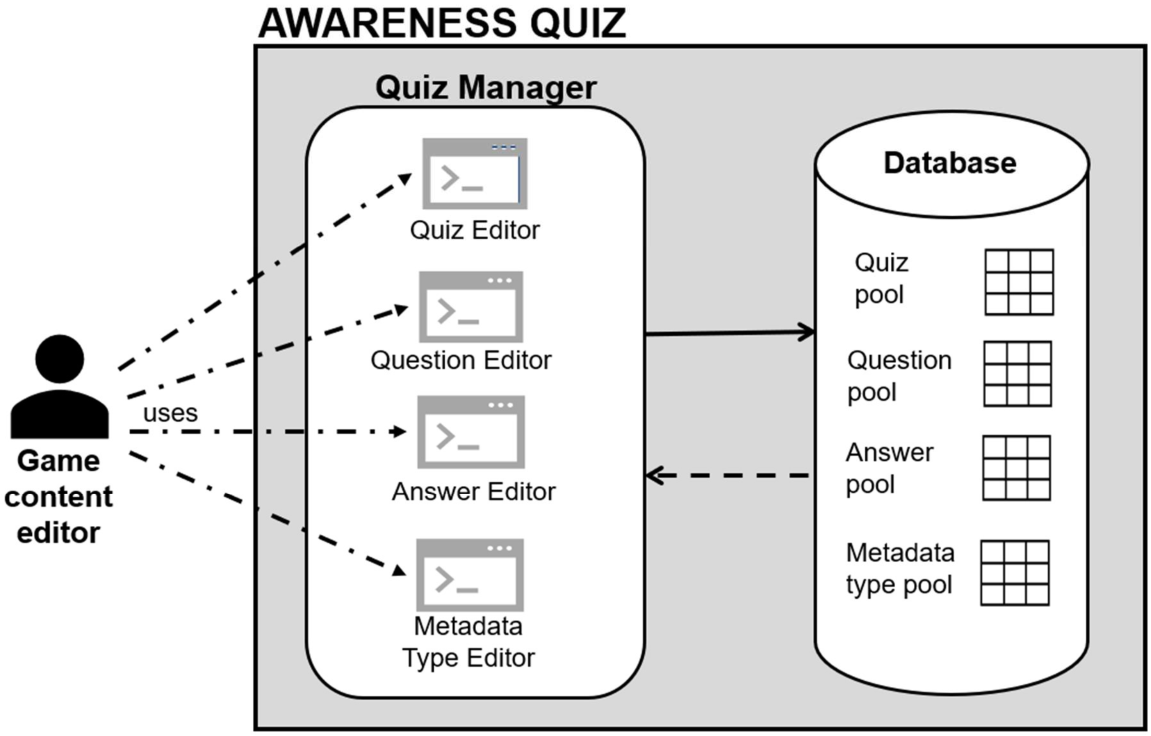


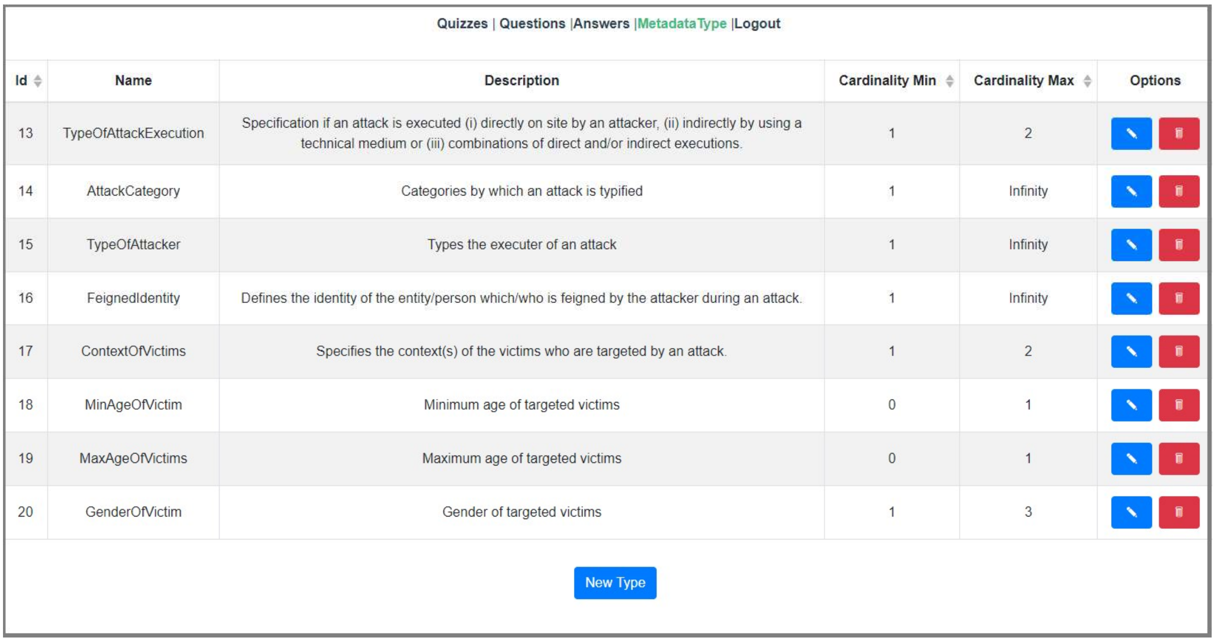
Figure 17: Editors and corresponding pools of the Quiz Manager

The different editor types are discussed in the following.

2.2.7.1 Metadata Type Editor

The *Metadata Type Editor* enables the creation of the metadata types which are specified in Table 3 and Table 4. Of course, the set of metadata types for questions and answers can be extended if necessary.

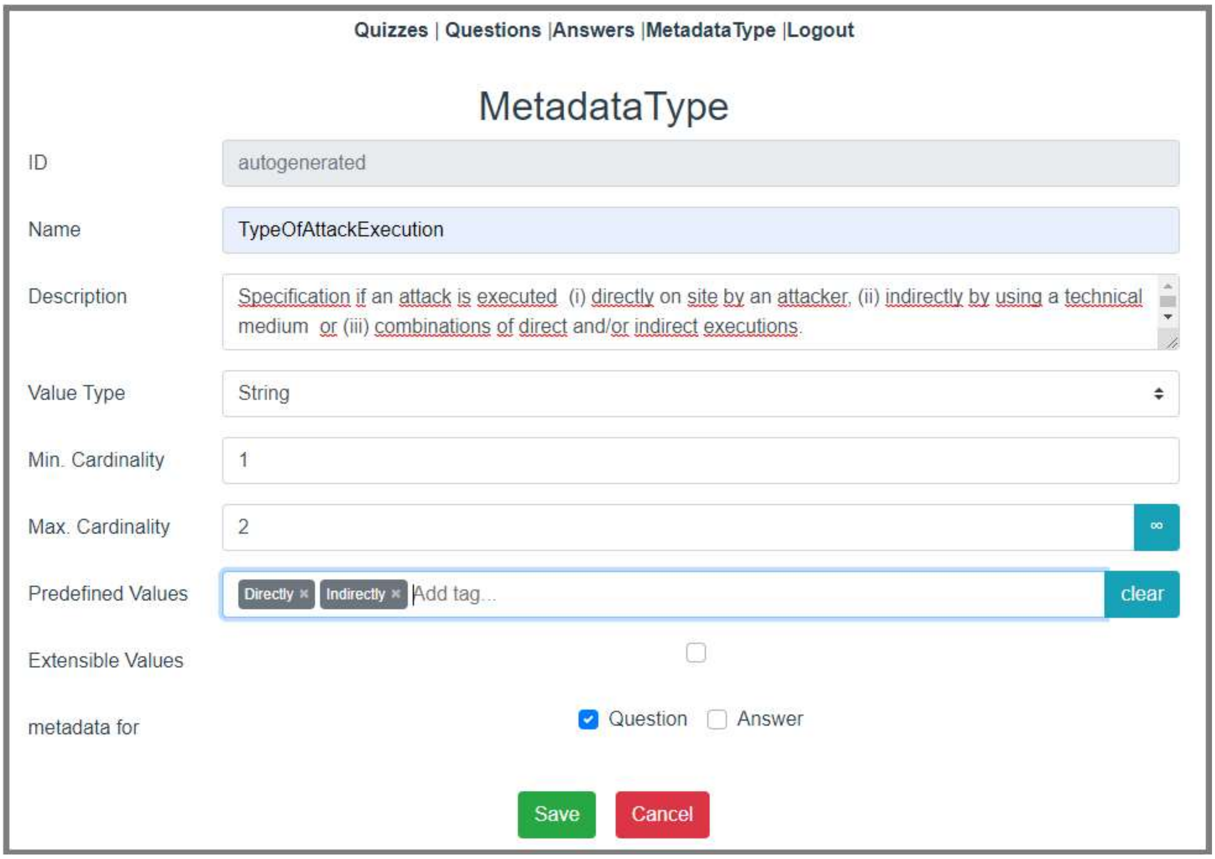
Figure 18 shows the actual implementation of the main view of the Metadata Type Editor which lists the set of defined metadata types. The existing metadata types can be edited and deleted. By clicking the *New Type*-button, a new metadata type can be created.



Id	Name	Description	Cardinality Min	Cardinality Max	Options
13	TypeOfAttackExecution	Specification if an attack is executed (i) directly on site by an attacker, (ii) indirectly by using a technical medium or (iii) combinations of direct and/or indirect executions.	1	2	✎ 🗑
14	AttackCategory	Categories by which an attack is typified	1	Infinity	✎ 🗑
15	TypeOfAttacker	Types the executer of an attack	1	Infinity	✎ 🗑
16	FeignedIdentity	Defines the identity of the entity/person which/who is feigned by the attacker during an attack.	1	Infinity	✎ 🗑
17	ContextOfVictims	Specifies the context(s) of the victims who are targeted by an attack.	1	2	✎ 🗑
18	MinAgeOfVictim	Minimum age of targeted victims	0	1	✎ 🗑
19	MaxAgeOfVictims	Maximum age of targeted victims	0	1	✎ 🗑
20	GenderOfVictim	Gender of targeted victims	1	3	✎ 🗑

Figure 18: Main view of the Metadata Type Editor

Figure 19 represents the creation of the metadata type *Type of attack execution* (see Table 3) in the Metadata Type Editor. It shows that every metadata type is identified by a unique identifier which is generated automatically in the parameter *ID*. The name of the metadata type which is defined by the parameter *Name* is represented in an upper camel case-notation. This notation is also used in the description of metadata types in the corresponding CTTP gamification model to avoid matching errors. A description of the metadata type is specified by the parameter *Description*. The *Value Type* parameter specifies that metadata values of the type *Type of attack execution* are presented as a string. The *Min.* (minimal) and *Max.* (maximal) *Cardinality* parameters define that at least one and at most two metadata values of this type must be or rather can be assigned to a question. The possible metadata values "Directly" and "Indirectly" are defined in the parameter *Predefined Values*. Here, again the upper camel case-notation is used. Because the parameter *Extensible Values* is not set, only the predefined values are potential metadata values for the defined metadata type. The setting of the parameter *metadata for* defines that metadata values of this type can only be assigned to questions.



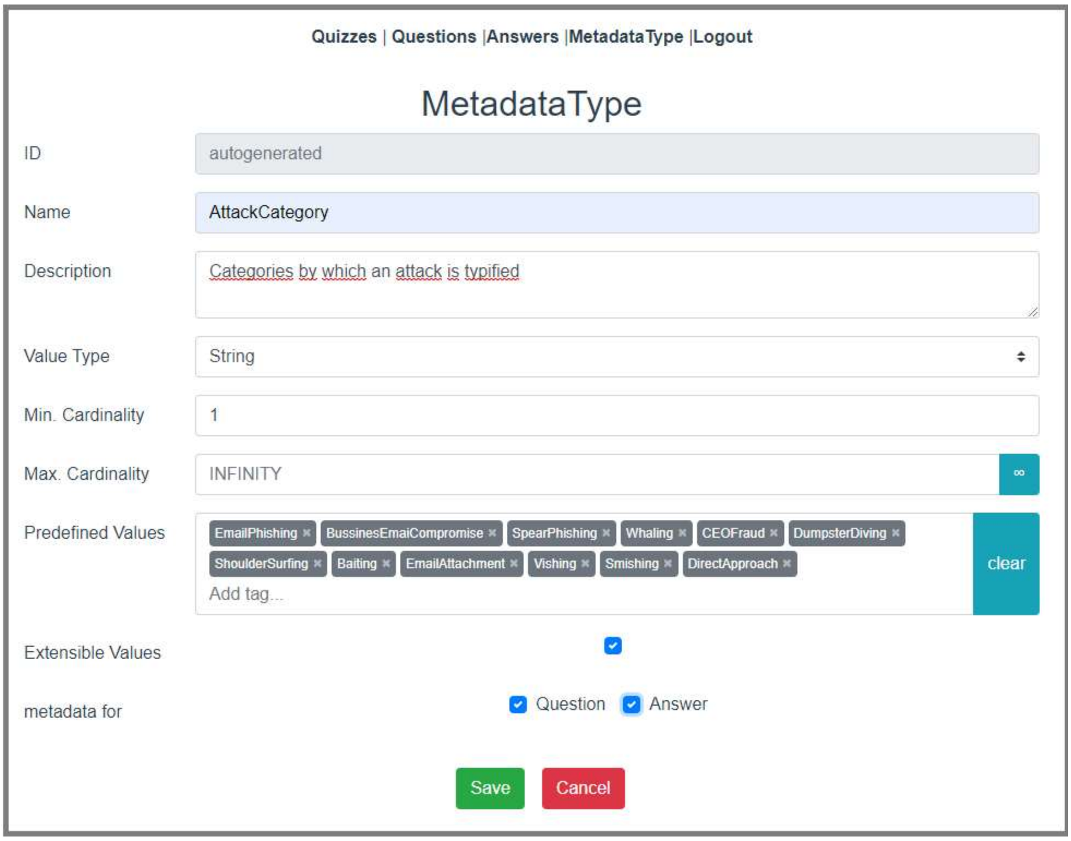
MetadataType

ID	autogenerated
Name	TypeOfAttackExecution
Description	Specification if an attack is executed (i) directly on site by an attacker, (ii) indirectly by using a technical medium or (iii) combinations of direct and/or indirect executions.
Value Type	String
Min. Cardinality	1
Max. Cardinality	2
Predefined Values	Directly × Indirectly × Add tag...
Extensible Values	□
metadata for	☑ Question □ Answer

Figure 19: Creation of the metadata type "Type of attack execution"

Figure 20 shows the creation of the metadata type *Attack category* (see Table 3). Compared to the metadata type *Type of attack execution*, an infinite[11] number of metadata values of the type *Attack category* can be assigned to a question or answer. The fact that metadata values of this type can be assigned to questions and answers is specified by the settings of the parameter *metadata for*. The parameter *Predefined Values* defines possible metadata values. Because this set of predefined values is specified as extensible by the parameter *Extensible Values*, it can be extended by new values during the creation of new questions and answers.

[11] In this context infinite means the upper value range of the numeric type used for the implementation.



MetadataType

ID	autogenerated
Name	AttackCategory
Description	Categories by which an attack is typified
Value Type	String
Min. Cardinality	1
Max. Cardinality	INFINITY ∞
Predefined Values	EmailPhishing × BussinesEmaiCompromise × SpearPhishing × Whaling × CEOFraud × DumpsterDiving × ShoulderSurfing × Baiting × EmailAttachment × Vishing × Smishing × DirectApproach × Add tag...
Extensible Values	☑
metadata for	☑ Question ☑ Answer

Figure 20: Creation of the metadata type "Attack category"

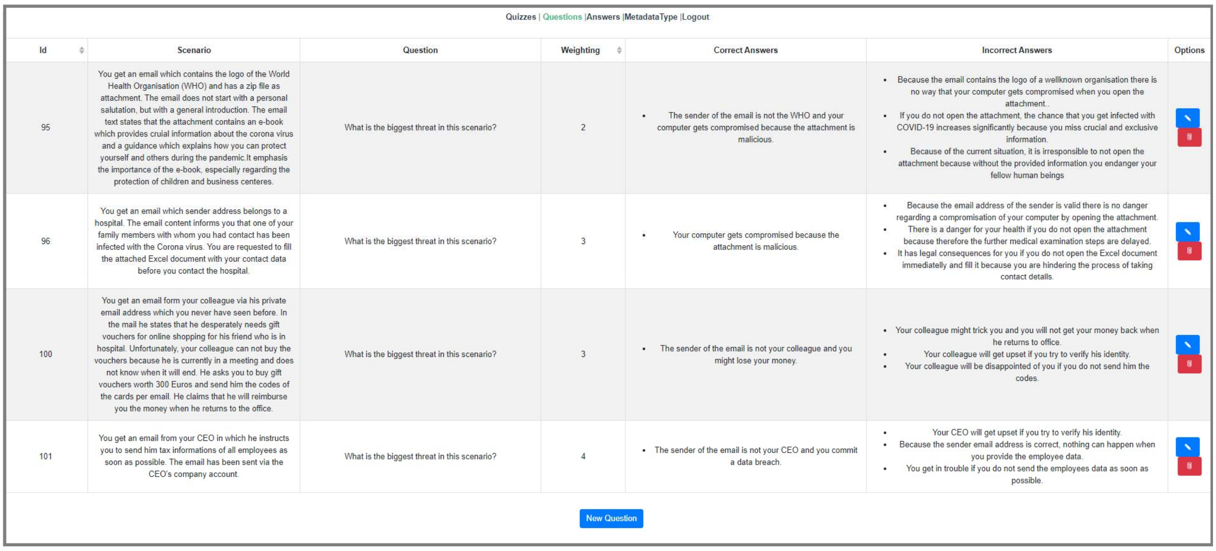
2.2.7.2 Question Editor

The *Question Editor* allows the definition of questions for the question pool (see Figure 17) from which existing question can be:

- added to a predefined quiz, or
- taken into account during the on the fly compilation of a set of questions for playing a context quiz.

Usually, the Question Editor is used for adding a new question to the question pool after information about a new social engineering attack has be identified (see Figure 11).

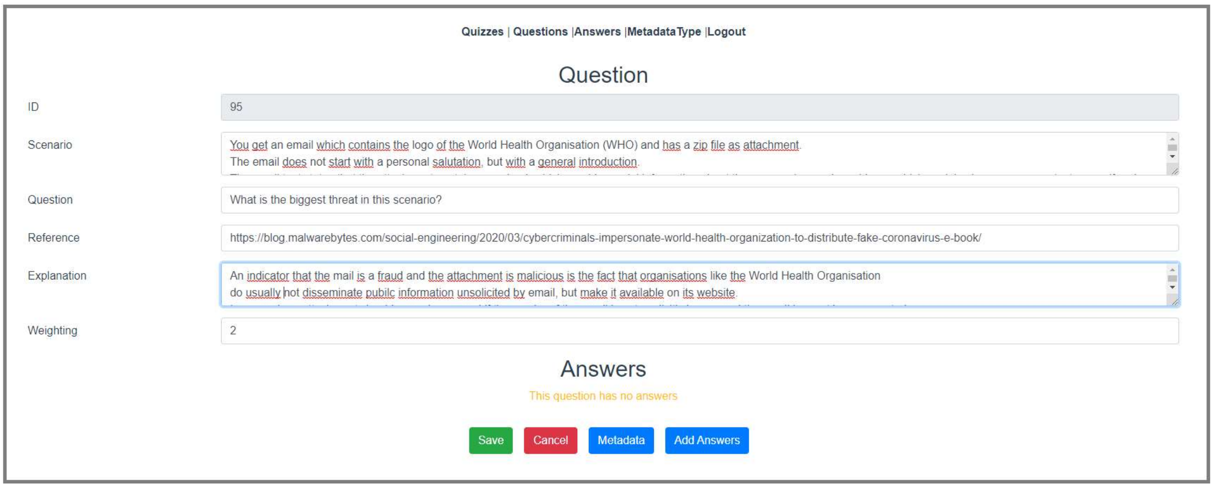
The main view of the Question Editor which lists the predefined questions from the question pool is presented in Figure 21. Figure 22 shows the creation of the question with respect to the malicious email attachment attack which has been introduced in the subsection 2.2.6. Each question is identified by a unique identifier which is generated automatically. Furthermore, the specification of the corresponding attack scenario, the actual question and the explanation of the scenario is performed. Additionally, the URL to the source which provides the content of the original attack description is defined. The value of the *Weighting* parameter (see Figure 22) indicates the level of difficulty for a question. In this connection, numeric values in the range from "1" (very easy) to "9" (extremely difficult) represent the level of difficulty.



Quizzes | Questions |Answers |MetadataType |Logout

Id	Scenario	Question	Weighting	Correct Answers	Incorrect Answers	Options
95	You get an email which contains the logo of the World Health Organisation (WHO) and has a zip file as attachment. The email does not start with a personal salutation, but with a general introduction. The email text states that the attachment contains an e-book which provides cruial information about the corona virus and a guidance which explains how you can protect yourself and others during the pandemic.It emphasis the importance of the e-book, especially regarding the protection of children and business centeres.	What is the biggest threat in this scenario?	2	• The sender of the email is not the WHO and your computer gets compromised because the attachment is malicious.	• Because the email contains the logo of a wellknown organisation there is no way that your computer gets compromised when you open the attachment.. • If you do not open the attachment, the chance that you get infected with COVID-19 increases significantly because you miss crucial and exclusive information. • Because of the current situation, it is irresponsible to not open the attachment because without the provided information.you endanger your fellow human beings	
96	You get an email which sender address belongs to a hospital. The email content informs you that one of your family members with whom you had contact has been infected with the Corona virus. You are requested to fill the attached Excel document with your contact data before you contact the hospital.	What is the biggest threat in this scenario?	3	• Your computer gets compromised because the attachment is malicious.	• Because the email address of the sender is valid there is no danger regarding a compromisation of your computer by opening the attachment. • There is a danger for your health if you do not open the attachment because therefore the further medical examination steps are delayed. • It has legal consequences for you if you do not open the Excel document immediatelly and fill it because you are hindering the process of taking contact details.	
100	You get an email form your colleague via his private email address which you never have seen before. In the mail he states that he desperately needs gift vouchers for online shopping for his friend who is in hospital. Unfortunately, your colleague can not buy the vouchers because he is currently in a meeting and does not know when it will end. He asks you to buy gift vouchers worth 300 Euros and send him the codes of the cards per email. He claims that he will reimburse you the money when he returns to the office.	What is the biggest threat in this scenario?	3	• The sender of the email is not your colleague and you might lose your money.	• Your colleague might trick you and you will not get your money back when he returns to office. • Your colleague will get upset if you try to verify his identity. • Your colleague will be disappointed of you if you do not send him the codes.	
101	You get an email from your CEO in which he instructs you to send him tax informations of all employees as soon as possible. The email has been sent via the CEO's company account.	What is the biggest threat in this scenario?	4	• The sender of the email is not your CEO and you commit a data breach.	• Your CEO will get upset if you try to verify his identity. • Because the sender email address is correct, nothing can happen when you provide the employee data. • You get in trouble if you do not send the employees data as soon as possible.	

Figure 21: Main view of Question Editor which lists predefined questions from the question pool



Quizzes | Questions |Answers |MetadataType |Logout

Question

ID: 95

Scenario: You get an email which contains the logo of the World Health Organisation (WHO) and has a zip file as attachment.
The email does not start with a personal salutation, but with a general introduction.

Question: What is the biggest threat in this scenario?

Reference: https://blog.malwarebytes.com/social-engineering/2020/03/cybercriminals-impersonate-world-health-organization-to-distribute-fake-coronavirus-e-book/

Explanation: An indicator that the mail is a fraud and the attachment is malicious is the fact that organisations like the World Health Organisation
do usually not disseminate pubilc information unsolicited by email, but make it available on its website.

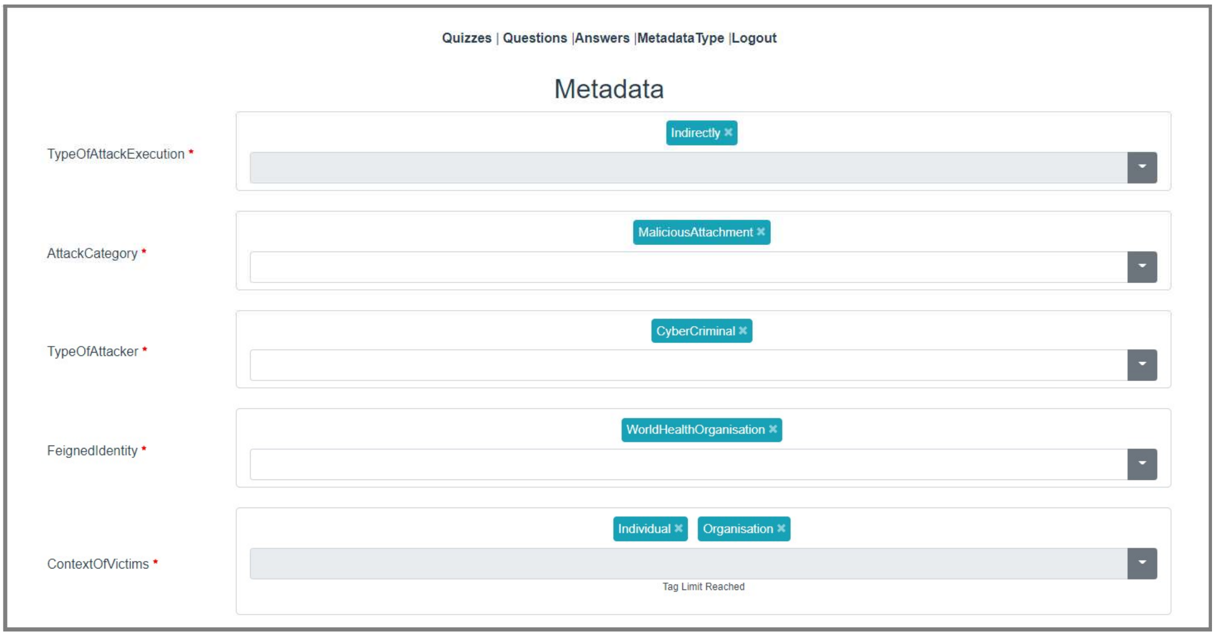
Weighting: 2

Answers

This question has no answers

Figure 22: Creation of question in Quiz Editor

Figure 23 and Figure 24 show the assignment of metadata to the current question in the corresponding view of the Quiz Editor. Here, the parameter names of metadata types of which at least one metadata value has to be assigned (see subsection 2.2.4) are marked by a red coloured start. If predefined metadata values for a certain type already exist, these values can be selected (see subsection 2.2.4). When the set of metadata values of a particular type is extensible, new metadata values can be entered (see subsection 2.2.4).



Metadata

TypeOfAttackExecution * : Indirectly ✖

AttackCategory * : MaliciousAttachment ✖

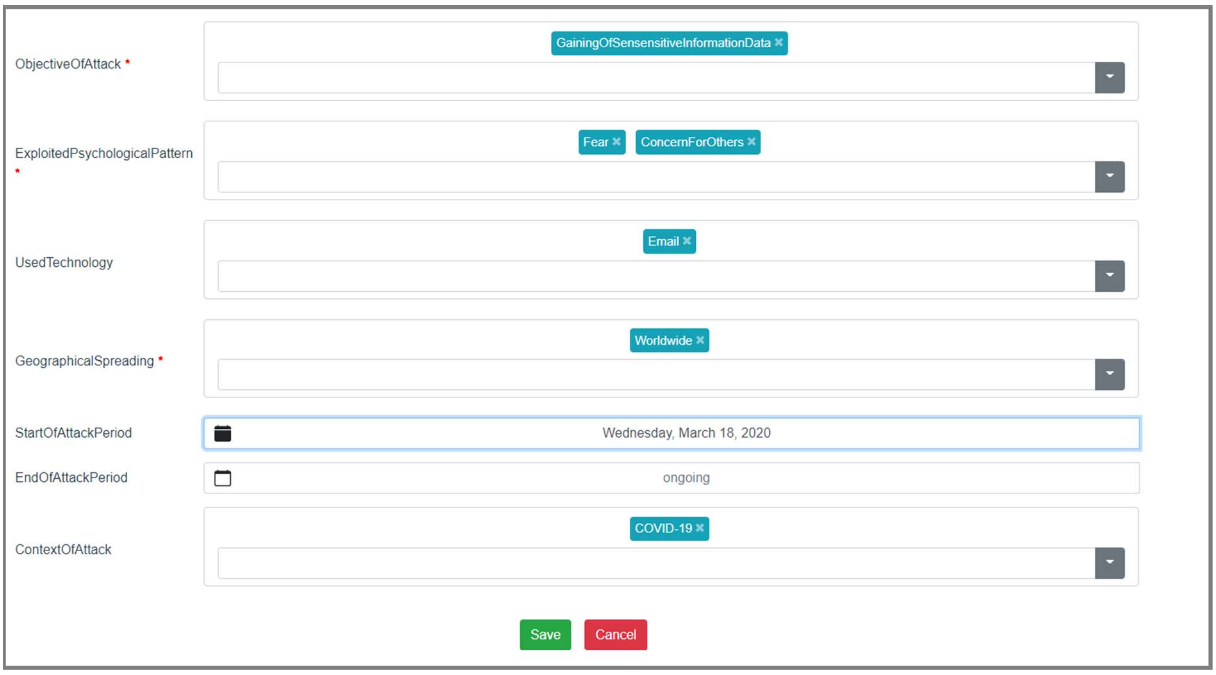
TypeOfAttacker * : CyberCriminal ✖

FeignedIdentity * : WorldHealthOrganisation ✖

ContextOfVictims * : Individual ✖ Organisation ✖

Tag Limit Reached

Figure 23: Assignment of metadata to question part 1


ObjectiveOfAttack * : GainingOfSensensitiveInformationData ✖

ExploitedPsychologicalPattern * : Fear ✖ ConcernForOthers ✖

UsedTechnology : Email ✖

GeographicalSpreading * : Worldwide ✖

StartOfAttackPeriod : Wednesday, March 18, 2020

EndOfAttackPeriod : ongoing

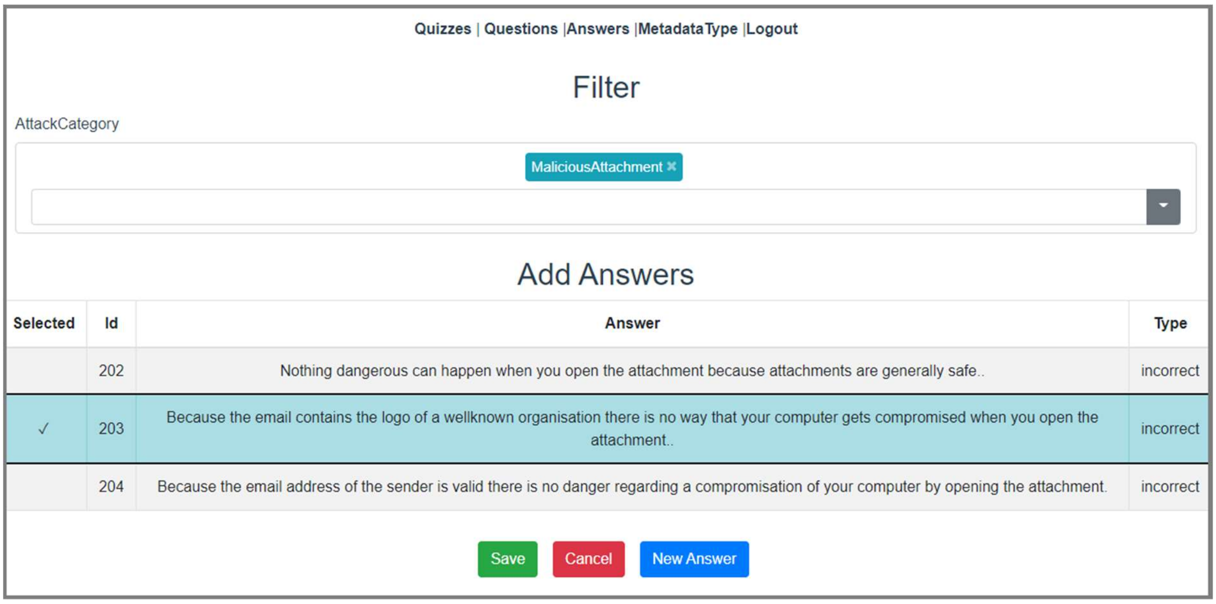
ContextOfAttack : COVID-19 ✖

Figure 24: Assignment of metadata to question part 2

With respect to the adding of questions to the current question, the Quiz Editor enables the:

- addition of predefined answers from the answer pool (see Figure 17), and
- the creation of new answers.

Figure 25 shows the adding of a predefined answer from the answer pool. The set of potential answers has been limited by filtering for answers which are tagged with the metadata value *MaliciousAttachment* of the type *AttackCategory*. It can be seen that the selected answer represents an incorrect answer. The creation of a new answer for the current question is presented in Figure 26. This answer represents the correct answer. Each answer is identified by a unique identifier which is generated automatically. The selection of the *Correct Answer* checkbox indicates that the answer represents a correct answer. Figure 27 shows the assignment of metadata to the created answer.



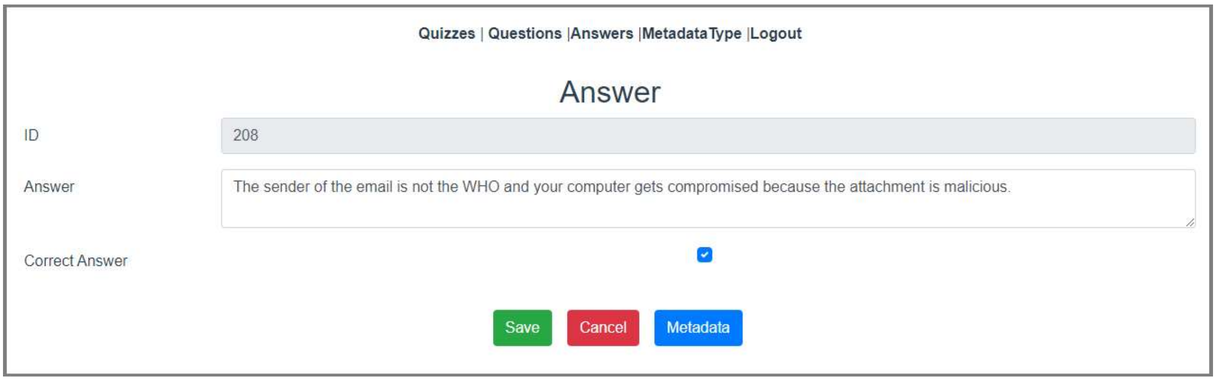
Filter

AttackCategory

Add Answers

Selected	Id	Answer	Type
	202	Nothing dangerous can happen when you open the attachment because attachments are generally safe..	incorrect
✓	203	Because the email contains the logo of a wellknown organisation there is no way that your computer gets compromised when you open the attachment..	incorrect
	204	Because the email address of the sender is valid there is no danger regarding a compromisation of your computer by opening the attachment.	incorrect

Figure 25: Adding of a predefined answer from the question pool to a question inside of Quiz Editor



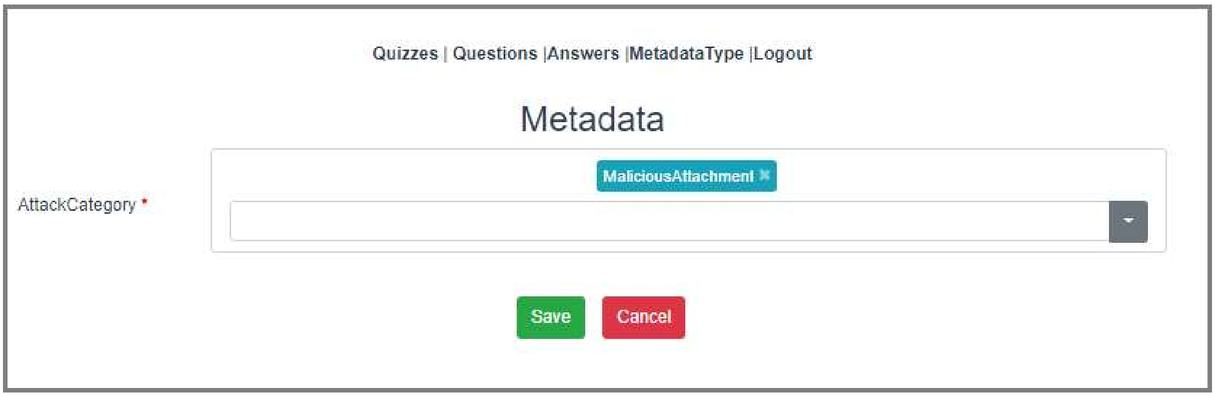
Answer

ID 208

Answer The sender of the email is not the WHO and your computer gets compromised because the attachment is malicious.

Correct Answer ☑

Figure 26: Creation of a new answer for question inside of Quiz Editor

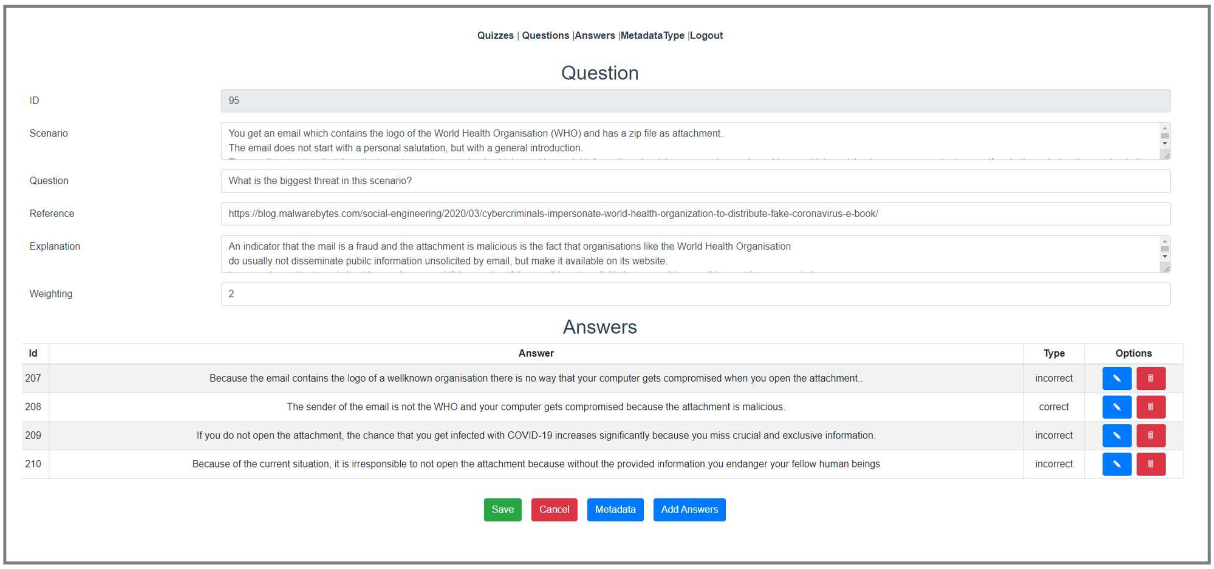


Metadata

AttackCategory *

Figure 27: Adding of metadata to a created answer for a question inside of Quiz Editor

Figure 28 shows the complete definition of the question with all related answers.



Question

ID	95
Scenario	You get an email which contains the logo of the World Health Organisation (WHO) and has a zip file as attachment. The email does not start with a personal salutation, but with a general introduction.
Question	What is the biggest threat in this scenario?
Reference	https://blog.malwarebytes.com/social-engineering/2020/03/cybercriminals-impersonate-world-health-organization-to-distribute-fake-coronavirus-e-book/
Explanation	An indicator that the mail is a fraud and the attachment is malicious is the fact that organisations like the World Health Organisation do usually not disseminate pubilc information unsolicited by email, but make it available on its website.
Weighting	2

Answers

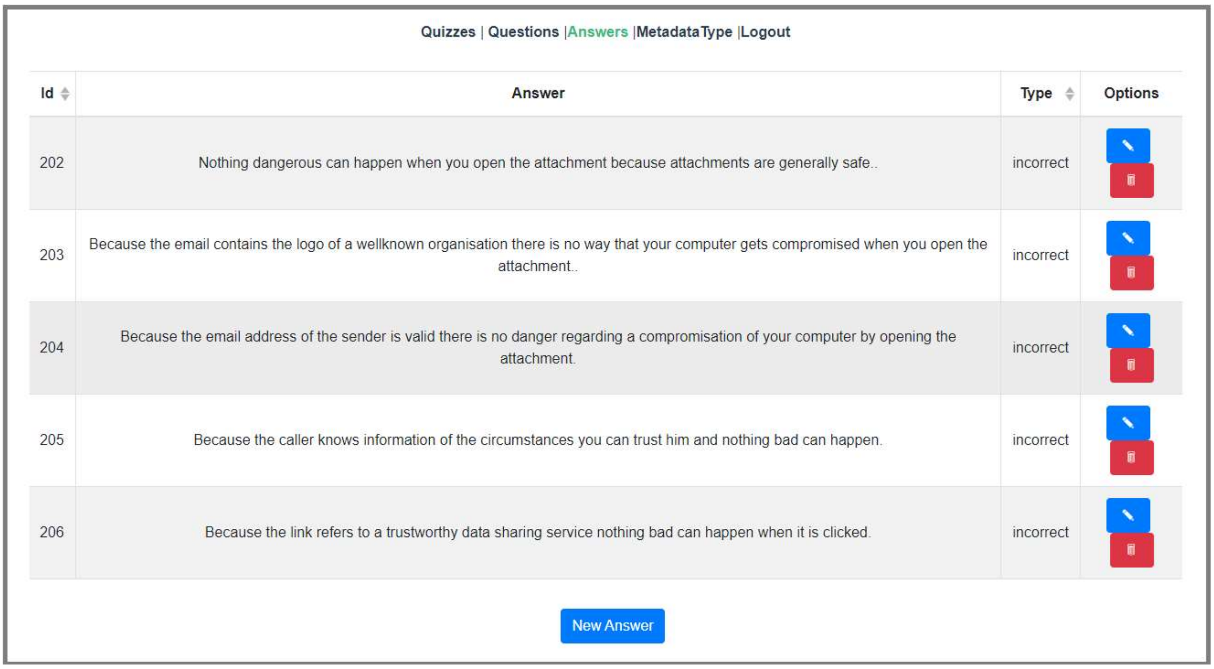
Id	Answer	Type	Options
207	Because the email contains the logo of a wellknown organisation there is no way that your computer gets compromised when you open the attachment..	incorrect	
208	The sender of the email is not the WHO and your computer gets compromised because the attachment is malicious.	correct	
209	If you do not open the attachment, the chance that you get infected with COVID-19 increases significantly because you miss crucial and exclusive information.	incorrect	
210	Because of the current situation, it is irresponsible to not open the attachment because without the provided information you endanger your fellow human beings	incorrect	

Figure 28: Representation of created question with added answers

2.2.7.3 Answer Editor

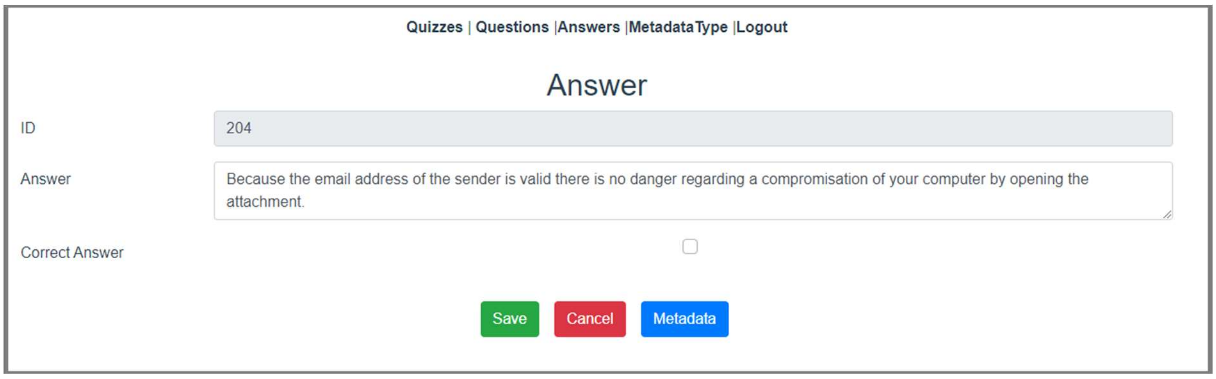
The Answer Editor enables the creation, editing, and deletion of predefined answers which are stored in the answer pool (see Figure 17). These answers can be reused during the creation of a new question. The answer pool includes especially incorrect questions which are usually more suitable for reuse due to their rather general statements.

Figure 29 shows the main view of the Answer Editor which lists the predefined answers from the answer pool. The creating of a new incorrect answer with respect to attacks scenarios with malicious attachments and the assignment of metadata to this answer is presented in Figure 30 and Figure 31.



Id	Answer	Type	Options
202	Nothing dangerous can happen when you open the attachment because attachments are generally safe..	incorrect	
203	Because the email contains the logo of a wellknown organisation there is no way that your computer gets compromised when you open the attachment..	incorrect	
204	Because the email address of the sender is valid there is no danger regarding a compromisation of your computer by opening the attachment.	incorrect	
205	Because the caller knows information of the circumstances you can trust him and nothing bad can happen.	incorrect	
206	Because the link refers to a trustworthy data sharing service nothing bad can happen when it is clicked.	incorrect	

Figure 29: Main view of Answer Editor which lists the predefined answers from the answer pool

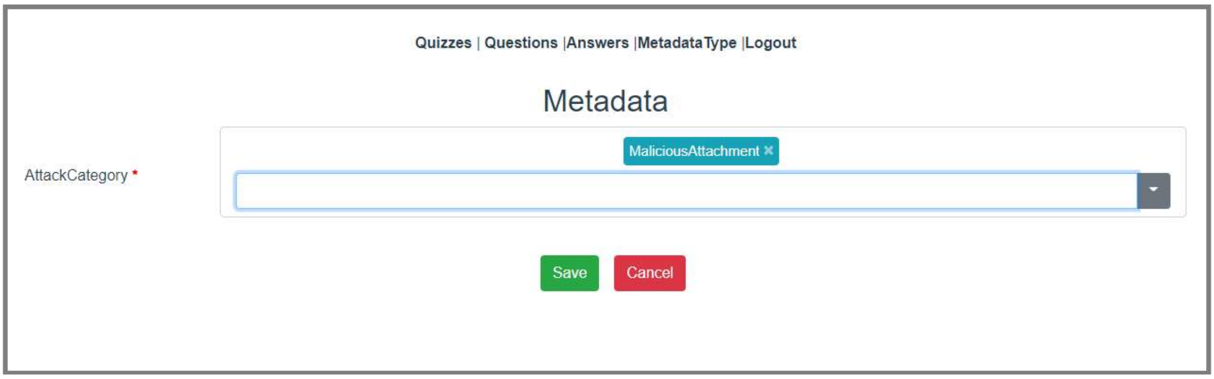


ID: 204

Answer: Because the email address of the sender is valid there is no danger regarding a compromisation of your computer by opening the attachment.

Correct Answer: □

Figure 30: Creation of a new answer inside the Answer Editor



AttackCategory *: MaliciousAttachment ×

Figure 31: Assignment of metadata to a newly created answer inside the Answer Editor

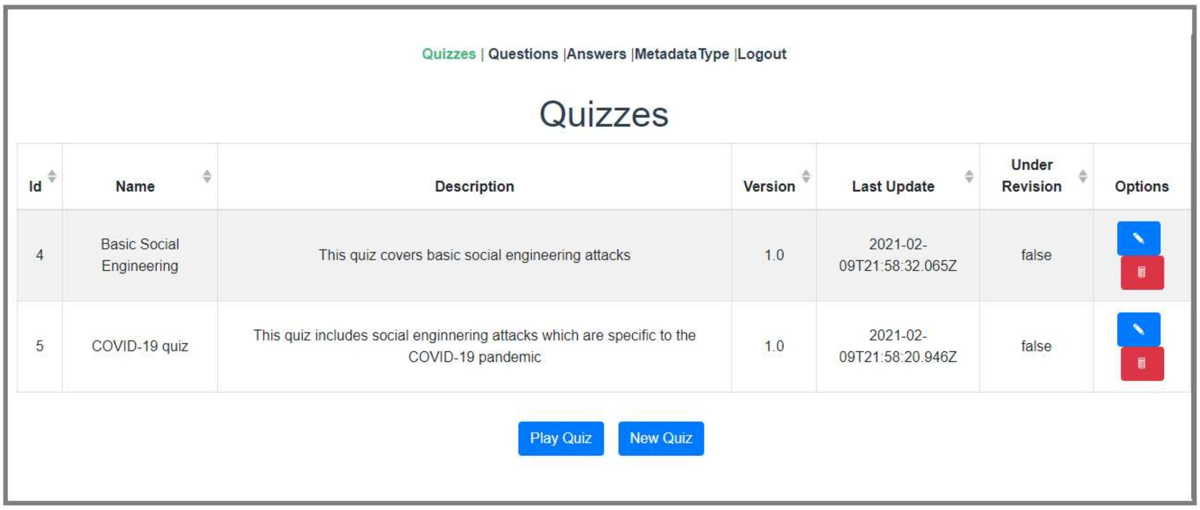
2.2.7.4 Quiz Editor

The *Quiz Editor* provides functionality for the creation, editing, and deletion of quizzes. Figure 32 shows the main view of the Quiz Editor in which all available predefined quizzes from the quiz pool (see Figure 17) are listed. In this context, for each quiz there is provided:

- its uniquely identifier,
- its name,
- the description of the theme of the quiz, and
- editorial information regarding its version, the date of the last update and its current revision status.

For example, the quiz “COVID-19 quiz” includes questions with respect to social engineering attacks which are specific for the COVID-19 pandemic.

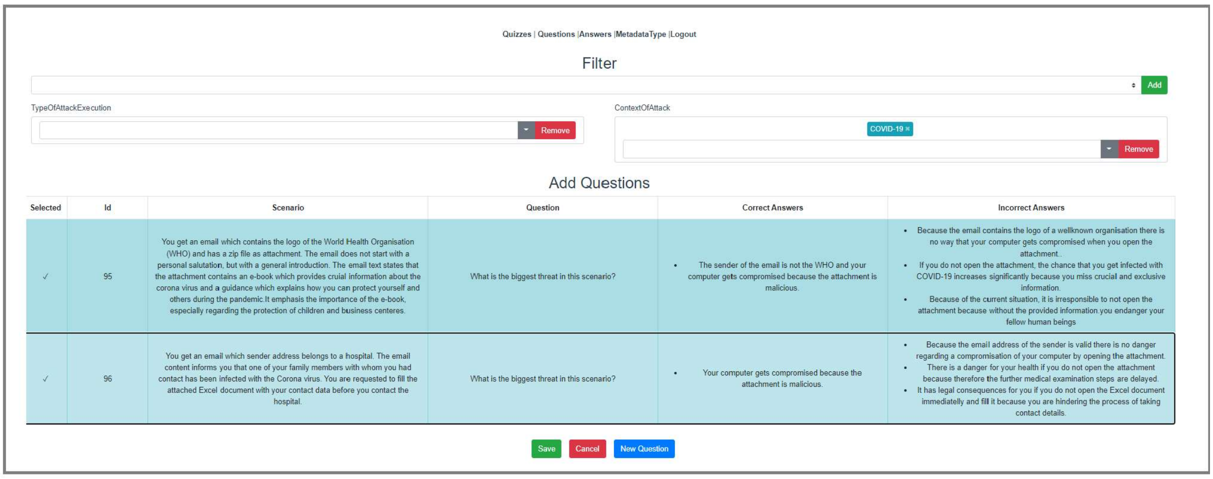
In Figure 33, predefined questions from the question pool are added to the *COVID-19 quiz*. To this, the set of potential questions for reuse has been specialized via filtering by the metadata value “COVID-19” of the metadata type *Context of attack* (see Table 3). The Quiz Editor also provides functionality for creating new questions for the current quiz. The editor views for creating questions correspond to the particular views of the Question Editor (see subsection 2.2.7.2). If appropriate, a newly created question can additionally be added to the question manager for further reuse. Figure 34 shows the definition of the COVID-19 quiz after questions have been added.



Quizzes

Id	Name	Description	Version	Last Update	Under Revision	Options
4	Basic Social Engineering	This quiz covers basic social engineering attacks	1.0	2021-02-09T21:58:32.065Z	false	✎ 🗑
5	COVID-19 quiz	This quiz includes social enginnering attacks which are specific to the COVID-19 pandemic	1.0	2021-02-09T21:58:20.946Z	false	✎ 🗑

Figure 32: Main view of Quiz Editor which lists available quizzes



Filter

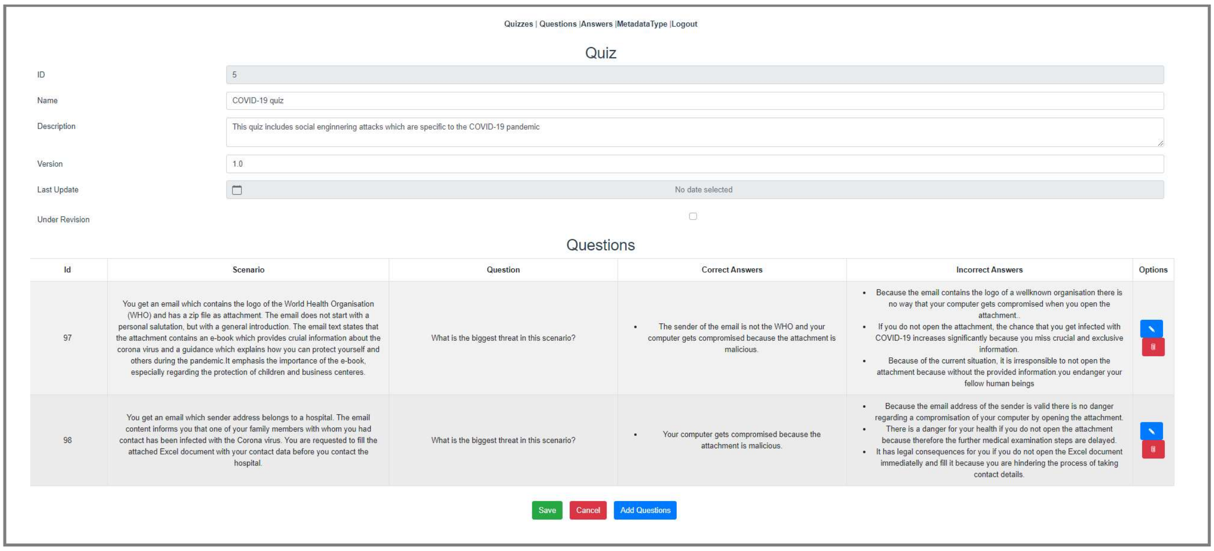
TypeOfAttackExecution

ContextOfAttack: COVID-19 ×

Add Questions

Selected	Id	Scenario	Question	Correct Answers	Incorrect Answers
✓	95	You get an email which contains the logo of the World Health Organisation (WHO) and has a zip file as attachment. The email does not start with a personal salutation, but with a general introduction. The email text states that the attachment contains an e-book which provides cruial information about the corona virus and a guidance which explains how you can protect yourself and others during the pandemic.It emphasis the importance of the e-book, especially regarding the protection of children and business centeres.	What is the biggest threat in this scenario?	• The sender of the email is not the WHO and your computer gets compromised because the attachment is malicious.	• Because the email contains the logo of a wellknown organisation there is no way that your computer gets compromised when you open the attachment.. • If you do not open the attachment, the chance that you get infected with COVID-19 increases significantly because you miss crucial and exclusive information. • Because of the current situation, it is irresponsible to not open the attachment because without the provided information.you endanger your fellow human beings
✓	96	You get an email which sender address belongs to a hospital. The email content informs you that one of your family members with whom you had contact has been infected with the Corona virus. You are requested to fill the attached Excel document with your contact data before you contact the hospital.	What is the biggest threat in this scenario?	• Your computer gets compromised because the attachment is malicious.	• Because the email address of the sender is valid there is no danger regarding a compromisation of your computer by opening the attachment. • There is a danger for your health if you do not open the attachment because therefore the further medical examination steps are delayed. • It has legal consequences for you if you do not open the Excel document immediatelly and fill it because you are hindering the process of taking contact details.

Figure 33: Addition of predefined questions to current quiz



Quiz

ID	5
Name	COVID-19 quiz
Description	This quiz includes social enginnering attacks which are specific to the COVID-19 pandemic
Version	1.0
Last Update	No date selected
Under Revision	□

Questions

Id	Scenario	Question	Correct Answers	Incorrect Answers	Options
97	You get an email which contains the logo of the World Health Organisation (WHO) and has a zip file as attachment. The email does not start with a personal salutation, but with a general introduction. The email text states that the attachment contains an e-book which provides cruial information about the corona virus and a guidance which explains how you can protect yourself and others during the pandemic.It emphasis the importance of the e-book, especially regarding the protection of children and business centeres.	What is the biggest threat in this scenario?	• The sender of the email is not the WHO and your computer gets compromised because the attachment is malicious.	• Because the email contains the logo of a wellknown organisation there is no way that your computer gets compromised when you open the attachment.. • If you do not open the attachment, the chance that you get infected with COVID-19 increases significantly because you miss crucial and exclusive information. • Because of the current situation, it is irresponsible to not open the attachment because without the provided information.you endanger your fellow human beings	✎ 🗑
98	You get an email which sender address belongs to a hospital. The email content informs you that one of your family members with whom you had contact has been infected with the Corona virus. You are requested to fill the attached Excel document with your contact data before you contact the hospital.	What is the biggest threat in this scenario?	• Your computer gets compromised because the attachment is malicious.	• Because the email address of the sender is valid there is no danger regarding a compromisation of your computer by opening the attachment. • There is a danger for your health if you do not open the attachment because therefore the further medical examination steps are delayed. • It has legal consequences for you if you do not open the Excel document immediatelly and fill it because you are hindering the process of taking contact details.	✎ 🗑

Figure 34: Representation of current quiz after questions have been added

2.2.8 Quiz Games of AWARENESS QUIZ

At the date of this deliverable, the following quiz games are under development:

- *COVID-19 Quiz:* This quiz addresses real-world social engineering attacks which are specific to the COVID-19 pandemic.
- *Botnet Quiz:* This quiz considers different aspects of botnet attacks.

2.2.9 Summary of Features

The features of AWARENESS QUIZ are summarized in Table 5.

Table 5: Features of AWARENESS QUIZ

Name	AWARENESS QUIZ
Objectives	Training of awareness against social engineering attacks
Game type	Quiz
Implementation	Online game
Number of players	• One player in two different single player modes
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 11)
Role within THREAT-ARREST	Training of awareness against social engineering attacks by a quiz game

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 the subsection 2.3.1.

The game concepts of PROTECT are based on the work of Aladawy et al. (Aladawy, et al., 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 completely new implementation of the game concepts of (Aladawy, et al., 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.

Since the first version of this deliverable (Goeke, et al., 2019), the graphical user interface (GUI) of PROTECT and further functional features have been improved. These improvements include:

- animations regarding the scoring,
- a highlighted representation of the expiring game time,
- a new placing of Attack cards,
- a diversified representation of the card deck, and
- an enhanced shuffle algorithm.

A detailed description of the improvements occurs in the subsection 2.3.3. Additionally, new learning content in the form of the card decks for the different THREAT-ARREST pilot scenarios has been created. These card decks are described in subsection 2.3.4. The features of PROTECT are summarized in subsection 2.3.5.

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, et al., 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. PERSUADED represents only a proof of concept which has been developed for the evaluation of the game concepts and mechanisms of (Aladawy, et al., 2018).

PROTECT is a completely new implementation of the design goals and game concepts of (Aladawy, et al., 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, et al., 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 35 and Figure 36). Compared to PERSUADED, the user interface of PROTECT (see Figure 36) 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 friendlier game atmosphere that results in more gaming fun.

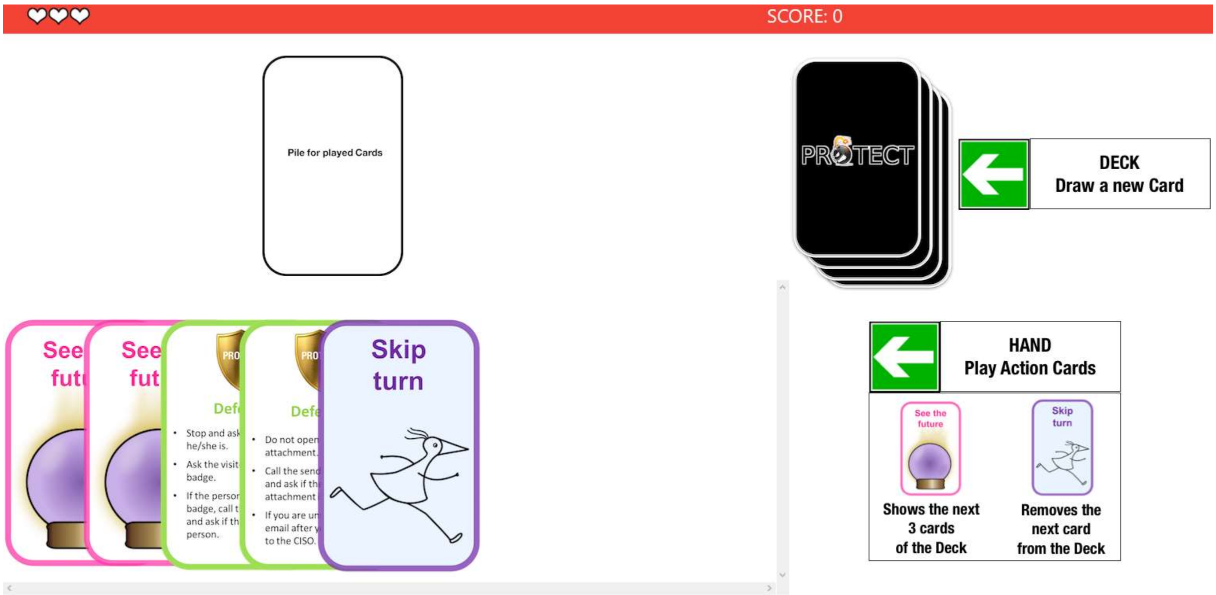
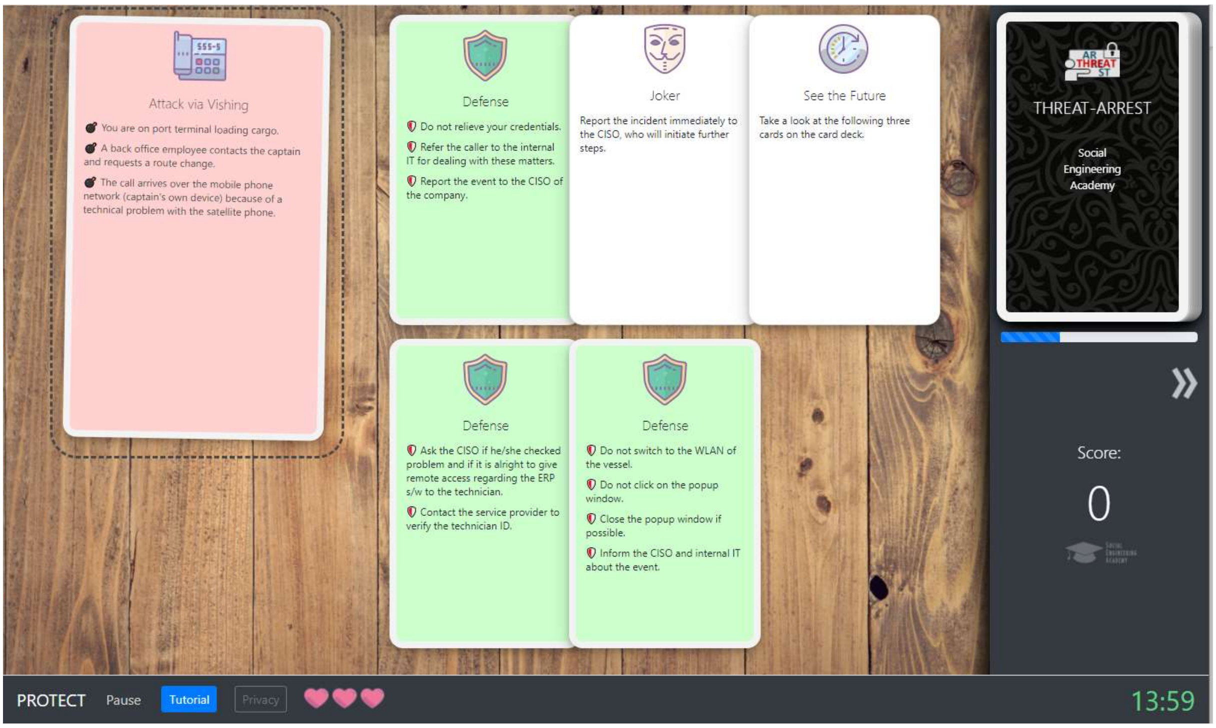


Figure 35: Graphical User Interface of PERSUADED



Attack via Vishing

- You are on port terminal loading cargo.
- A back office employee contacts the captain and requests a route change.
- The call arrives over the mobile phone network (captain's own device) because of a technical problem with the satellite phone.

Defense

- Do not relieve your credentials.
- Refer the caller to the internal IT for dealing with these matters.
- Report the event to the CISO of the company.

Joker

Report the incident immediately to the CISO, who will initiate further steps.

See the Future

Take a look at the following three cards on the card deck.

Defense

- Ask the CISO if he/she checked problem and if it is alright to give remote access regarding the ERP s/w to the technician.
- Contact the service provider to verify the technician ID.

Defense

- Do not switch to the WLAN of the vessel.
- Do not click on the popup window.
- Close the popup window if possible.
- Inform the CISO and internal IT about the event.

Figure 36: Graphical User Interface of PROTECT

Compared to PERSUADED, 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,
- number of lives of a player, 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. A detailed discussion of the configuration parameters of PROTECT is provided in subsection 5.2.

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 6 compares the features of PERSUDED and PROTECT.

Table 6: 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 a 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, et al., 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, et al., 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, et al., 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.

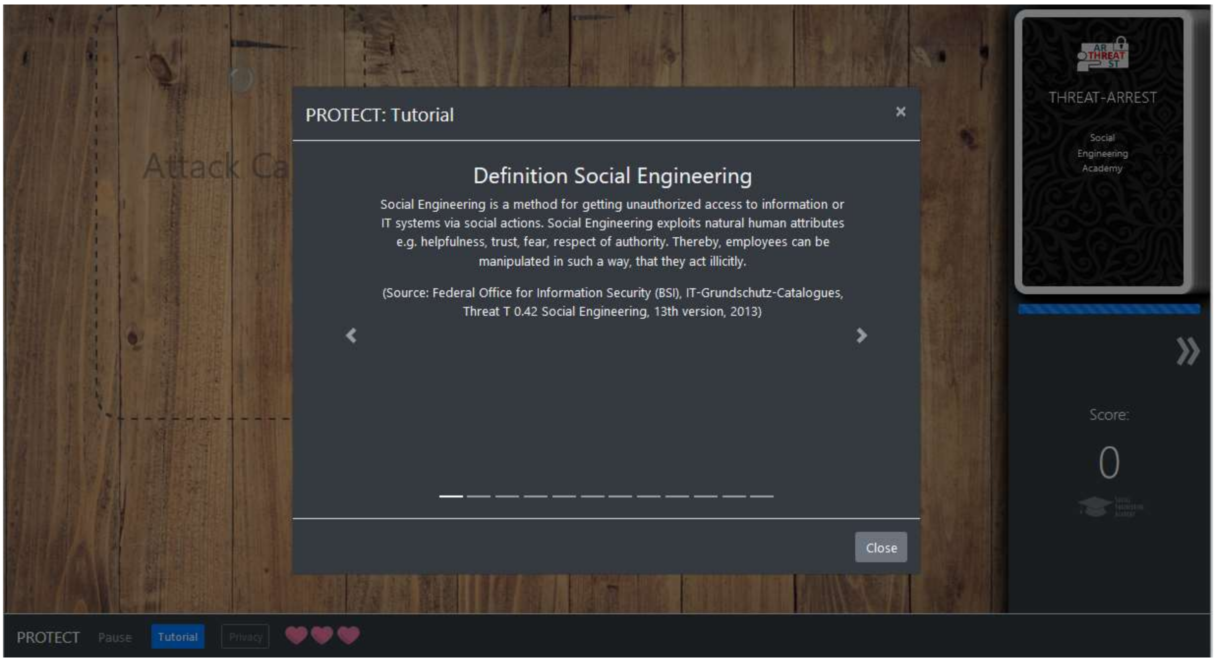
Before the first game of PROTECT in a certain web browser on a particular device starts, a tutorial is displayed which explains the game concepts and mechanisms of PROTECT to the player (see Figure 37). This tutorial is also represented before a game when the data of the web browser has been deleted. Before subsequent games of PROTECT and during a game, the tutorial can be opened by clicking the *Tutorial*-button in the menu (see Figure 38).

At the beginning of a game of PROTECT, all cards are included in a random order in the card deck that is positioned in the top right corner of the PROTECT GUI (see Figure 38). Compared to the prior version of the PROTECT GUI, the card deck is now displayed in a fanned presentation. Due to this, it can now clearly be identified as a card deck and not be mistaken for a single card. During the evaluation of the first version of the THREAT-ARREST platform by the THREAT-ARREST pilot owners (under WP7), it happened that only one Defense card was on the hand of a player when an Attack card has been drawn. Thereupon, the shuffling algorithm has been modified in a way that the order of cards ensures that at least two Defense cards are on the player's hand when an Attack card has to be defended.

Below the card deck, a progress bar has been added which informs the player about the number of remaining cards in the deck (see Figure 38). The representation of the current game score is positioned right center under the progress bar (see Figure 38).

The expiring game time is positioned bottom right in the PROTECT GUI, whereby its graphical representation has been improved (see Figure 38). Thus, the time starts with a representation in green color which turns to yellow color in the second third of the game. In the last third, the time representation is colored red and starts blinking in the last minute.

The remaining lives of the player are represented by pink heart symbols at the bottom of the GUI (see Figure 38). A running game can be interrupted by the player by pressing the *Pause*-button in the menu. The *Restart*-button for restarting a running game of PROTECT has been removed because this functionality was inappropriate in the context of THREAT-ARREST training programmes.



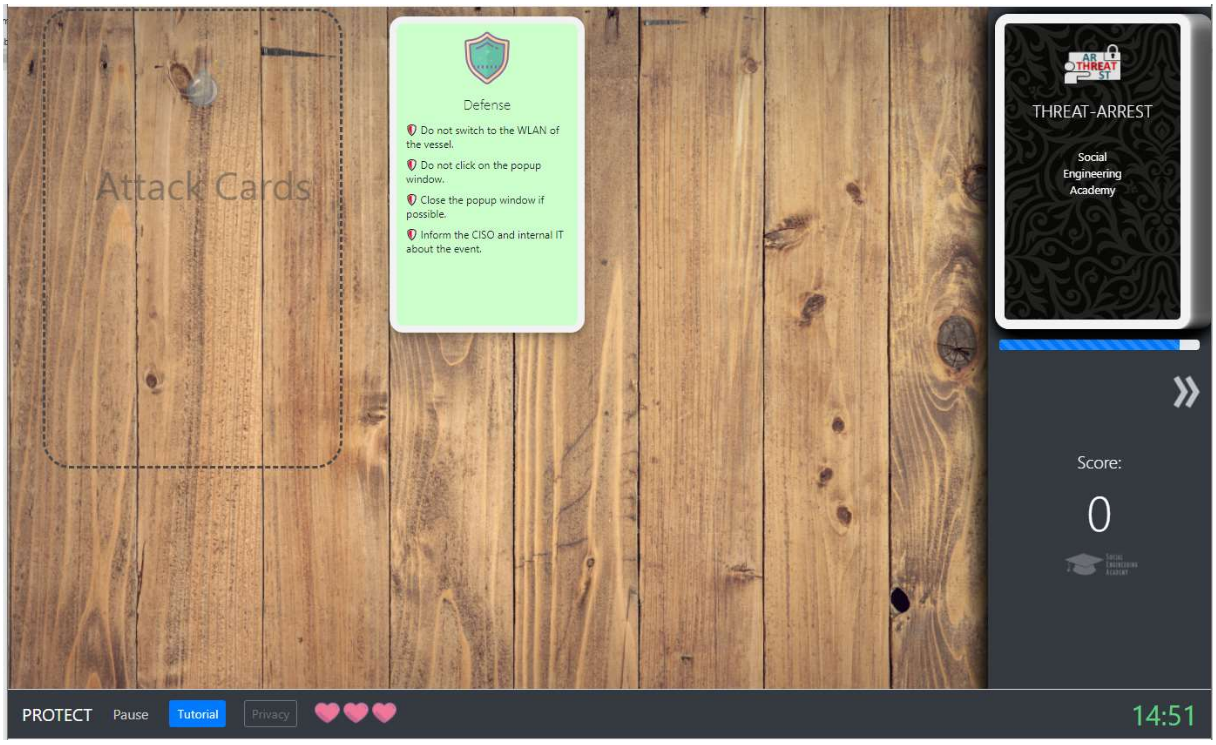
PROTECT: Tutorial

Definition Social Engineering

Social Engineering is a method for getting unauthorized access to information or IT systems via social actions. Social Engineering exploits natural human attributes e.g. helpfulness, trust, fear, respect of authority. Thereby, employees can be manipulated in such a way, that they act illicitly.

(Source: Federal Office for Information Security (BSI), IT-Grundschutz-Catalogues, Threat T 0.42 Social Engineering, 13th version, 2013)

Figure 37: Tutorial before the first game of PROTECT



Defense

- Do not switch to the WLAN of the vessel.
- Do not click on the popup window.
- Close the popup window if possible.
- Inform the CISO and internal IT about the event.

Figure 38: Properties of the PROTECT GUI

The first game of PROTECT starts by an automatic drawing of the top card from the card deck after the tutorial has been closed. Subsequent games are started when the first card is drawn by clicking on the card deck.

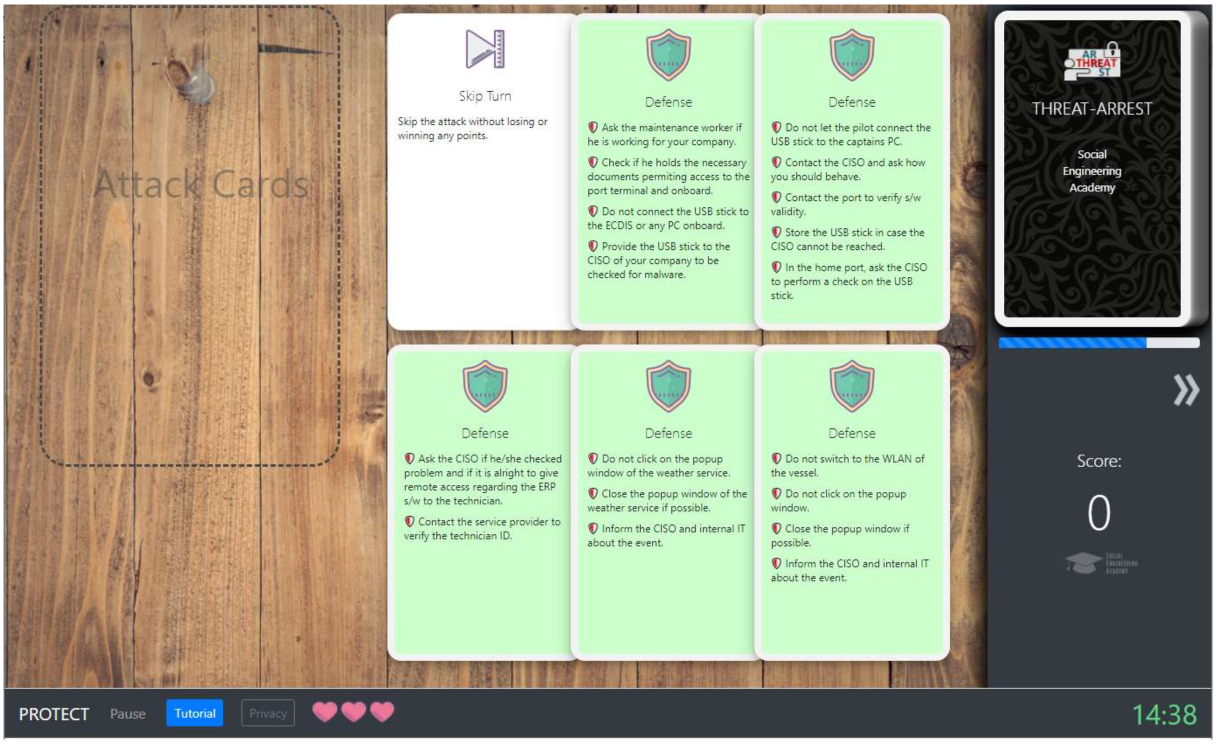
When the card deck is empty, the game is won. The game is lost when:

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 39).



Skip Turn

Skip the attack without losing or winning any points.

Defense

- Ask the maintenance worker if he is working for your company.
- Check if he holds the necessary documents permiting access to the port terminal and onboard.
- Do not connect the USB stick to the ECDIS or any PC onboard.
- Provide the USB stick to the CISO of your company to be checked for malware.

Defense

- Do not let the pilot connect the USB stick to the captains PC.
- Contact the CISO and ask how you should behave.
- Contact the port to verify s/w validity.
- Store the USB stick in case the CISO cannot be reached.
- In the home port, ask the CISO to perform a check on the USB stick.

Defense

- Ask the CISO if he/she checked problem and if it is alright to give remote access regarding the ERP s/w to the technician.
- Contact the service provider to verify the technician ID.

Defense

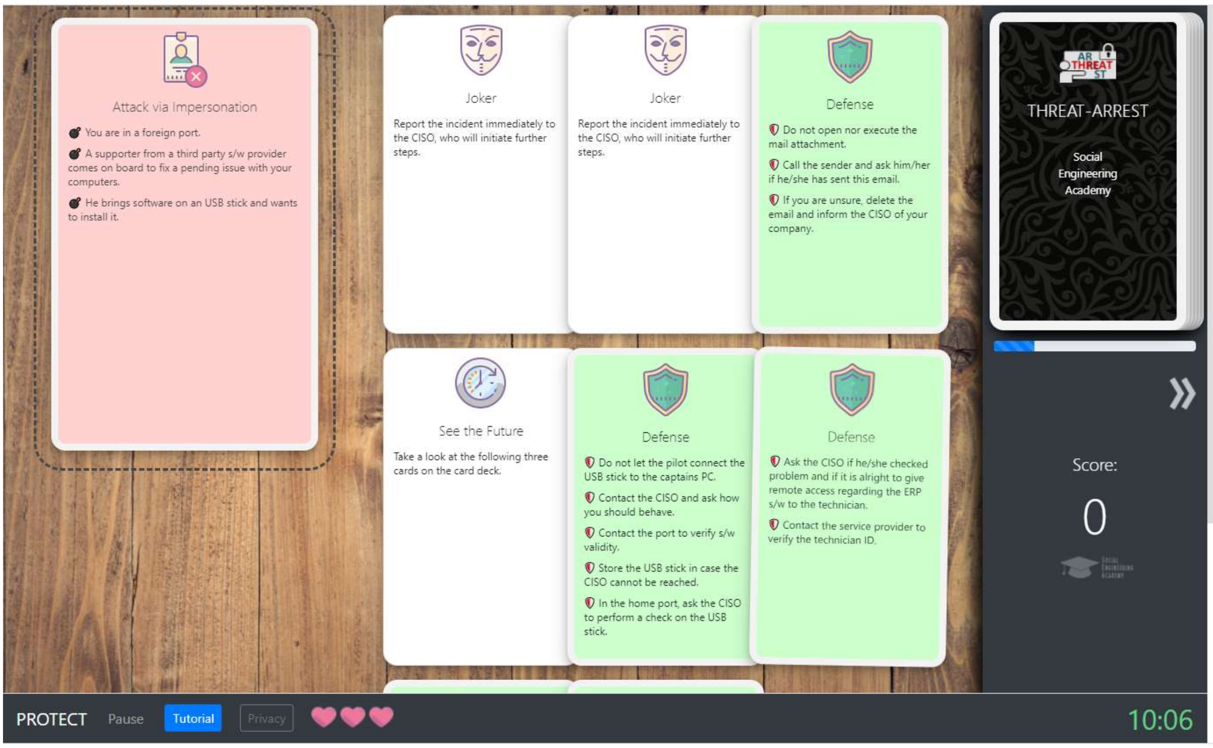
- Do not click on the popup window of the weather service.
- Close the popup window of the weather service if possible.
- Inform the CISO and internal IT about the event.

Defense

- Do not switch to the WLAN of the vessel.
- Do not click on the popup window.
- Close the popup window if possible.
- Inform the CISO and internal IT about the event.

Figure 39: Drawn cards on the hand of the player

If the drawn top card represents an Attack card, it is placed on a new special field which is positioned top left in the GUI (see Figure 40) Thus, the action of drawing an Attack card and its textual content are more emphasized compared to its representation in the previous PROTECT GUI version, in which a drawn attack card was represented inverted on the top of the card deck. The drawing of an attack card is additionally indicated by a displayed dialog which also represents the text of the attack card (see Figure 41). After clicking the *Select Defense*-button, the player has to select the appropriate Defense card for the drawn Attack card. The selection of the correct Defense card is confirmed by a certain dialog (see Figure 42) and the score is increased. A new animation informs the player by which number of points the score has been increased (see Figure 43). Both, the drawn Attack card and the selected Defense card are removed from the game.



Attack via Impersonation

- You are in a foreign port.
- A supporter from a third party s/w provider comes on board to fix a pending issue with your computers.
- He brings software on an USB stick and wants to install it.

Joker

Report the incident immediately to the CISO, who will initiate further steps.

Joker

Report the incident immediately to the CISO, who will initiate further steps.

Defense

- Do not open nor execute the mail attachment.
- Call the sender and ask him/her if he/she has sent this email.
- If you are unsure, delete the email and inform the CISO of your company.

See the Future

Take a look at the following three cards on the card deck.

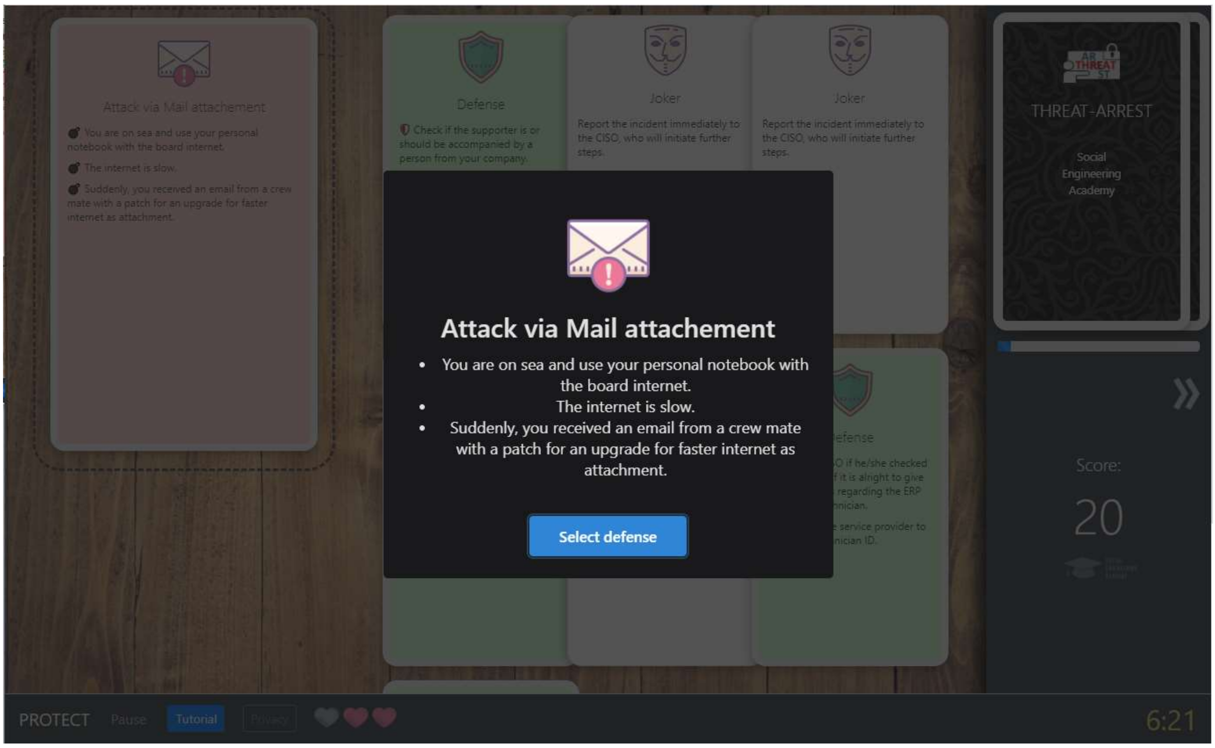
Defense

- Do not let the pilot connect the USB stick to the captains PC.
- Contact the CISO and ask how you should behave.
- Contact the port to verify s/w validity.
- Store the USB stick in case the CISO cannot be reached.
- In the home port, ask the CISO to perform a check on the USB stick.

Defense

- Ask the CISO if he/she checked problem and if it is alright to give remote access regarding the ERP s/w to the technician.
- Contact the service provider to verify the technician ID.

Figure 40: Drawing of an Attack Card



Attack via Mail attachement

- You are on sea and use your personal notebook with the board internet.
- The internet is slow.
- Suddenly, you received an email from a crew mate with a patch for an upgrade for faster internet as attachment.

Defense

- Check if the supporter is or should be accompanied by a person from your company.

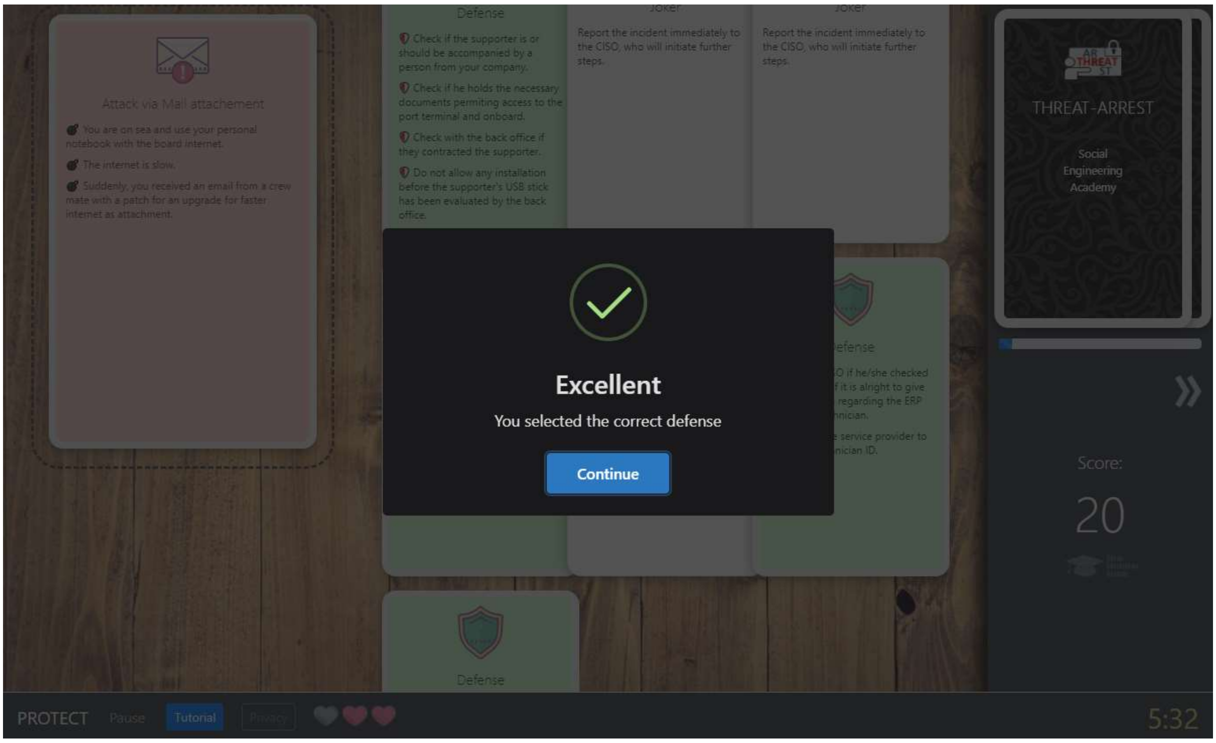
Joker

Report the incident immediately to the CISO, who will initiate further steps.

Joker

Report the incident immediately to the CISO, who will initiate further steps.

Figure 41: Dialog to indicate the drawing of an Attack card



Attack via Mail attachement

You are on sea and use your personal notebook with the board internet.

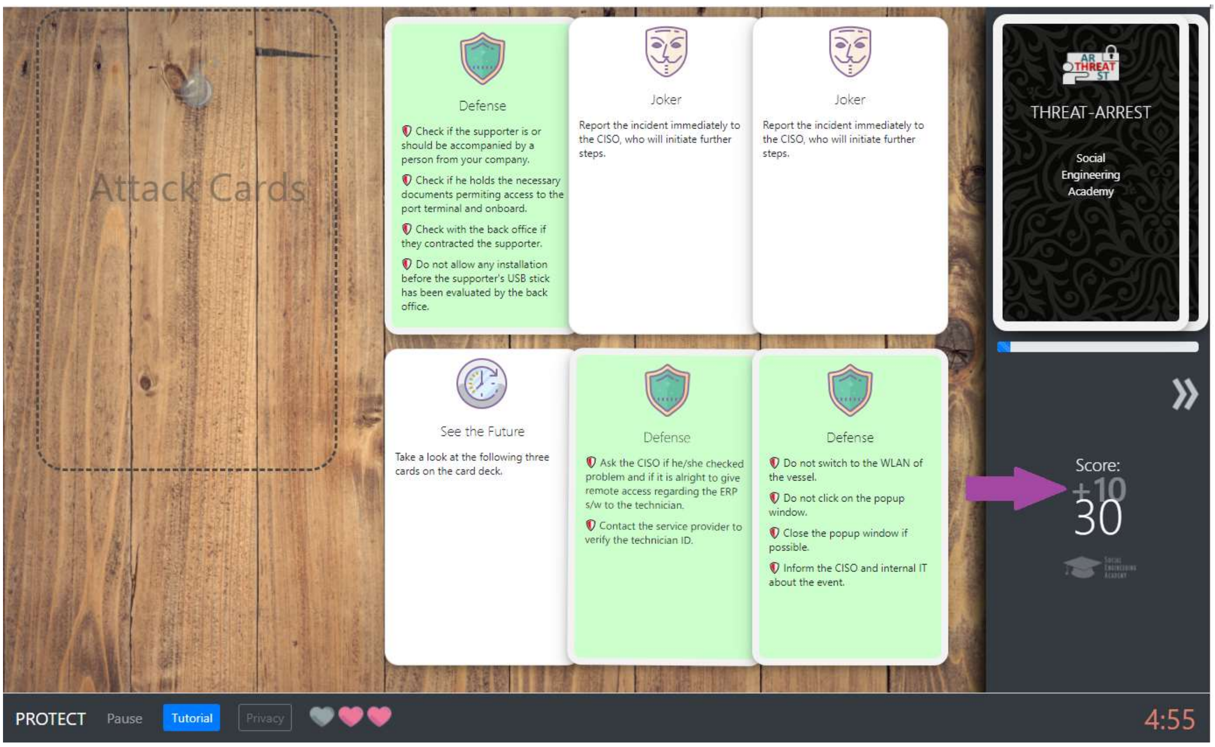
The internet is slow.

Suddenly, you received an email from a crew mate with a patch for an upgrade for faster internet as attachment.

Excellent

You selected the correct defense

Figure 42: Dialog after the correct Defense card has been selected



Defense

Check if the supporter is or should be accompanied by a person from your company.

Check if he holds the necessary documents permiting access to the port terminal and onboard.

Check with the back office if they contracted the supporter.

Do not allow any installation before the supporter's USB stick has been evaluated by the back office.

Joker

Report the incident immediately to the CISO, who will initiate further steps.

Joker

Report the incident immediately to the CISO, who will initiate further steps.

See the Future

Take a look at the following three cards on the card deck.

Defense

Ask the CISO if he/she checked problem and if it is alright to give remote access regarding the ERP s/w to the technician.

Contact the service provider to verify the technician ID.

Defense

Do not switch to the WLAN of the vessel.

Do not click on the popup window.

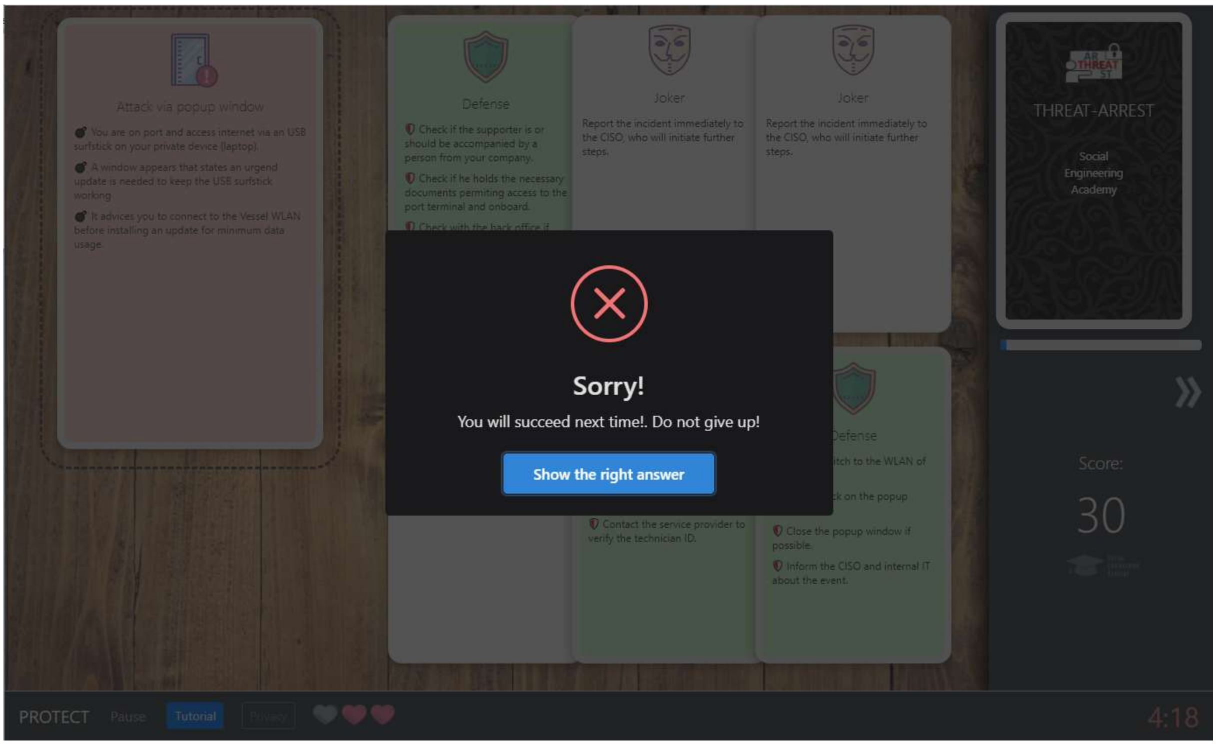
Close the popup window if possible.

Inform the CISO and internal IT about the event.

Figure 43: Animation for increasing the score

If an incorrect Defense card has been chosen, an appropriate dialog is shown (see Figure 44) and the text of the correct defense is displayed to the player in a further dialog (see Figure 45). Additionally, the player loses a life and the score is decreased. The decreasing of the score is graphically presented by an animation. A further animation which is displayed above the pink heart symbols informs the player about the number of remaining lives (see Figure 46). The drawn Attack card is removed from the card deck. The selected Defense card stays on the hand of the player.

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.



Attack via popup window

- You are on port and access internet via an USB surfstick on your private device (laptop).
- A window appears that states an urgend update is needed to keep the USB surfstick working.
- It advices you to connect to the Vessel WLAN before installing an update for minimum data usage.

Defense

- Check if the supporter is or should be accompanied by a person from your company.
- Check if he holds the necessary documents permiting access to the port terminal and onboard.
- Check with the back office if

Joker

Report the incident immediately to the CISO, who will initiate further steps.

Joker

Report the incident immediately to the CISO, who will initiate further steps.

- Contact the service provider to verify the technician ID.

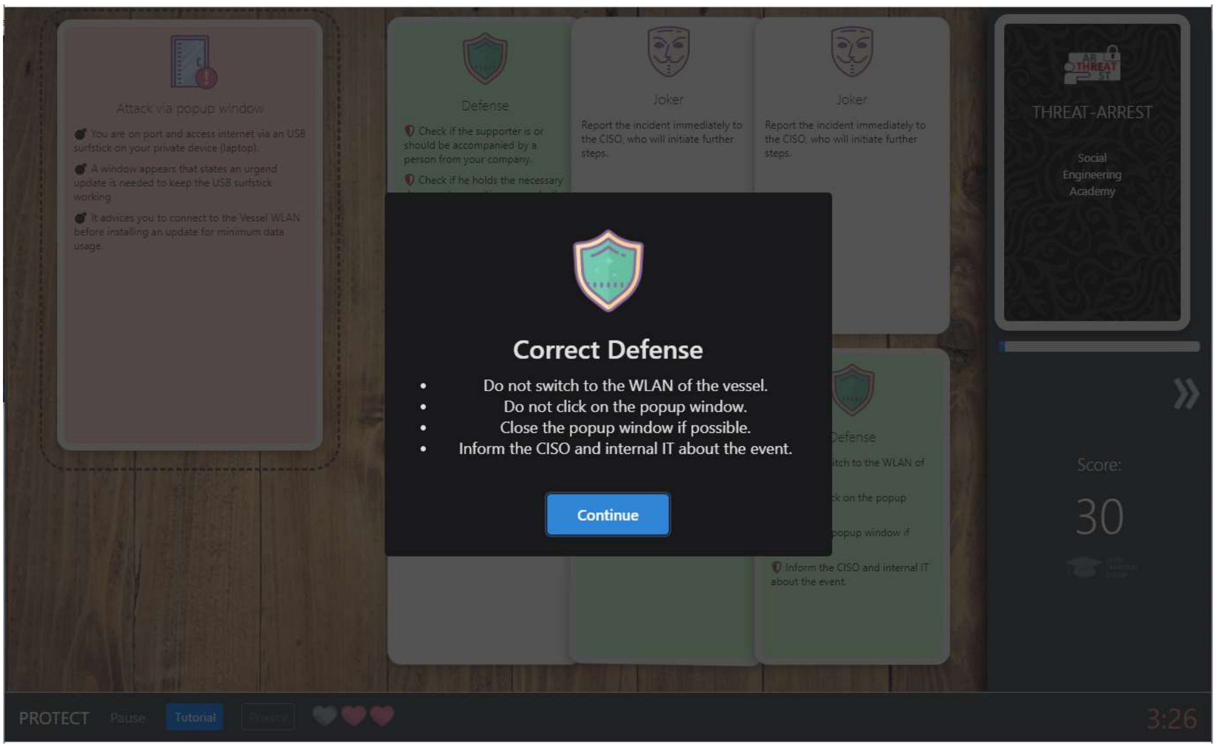
Defense

- itch to the WLAN of
- k on the popup
- Close the popup window if possible.
- Inform the CISO and internal IT about the event.

Sorry!

You will succeed next time!. Do not give up!

Figure 44: Dialog after selection of an incorrect Defense Card



Attack via popup window

- You are on port and access internet via an USB surfstick on your private device (laptop).
- A window appears that states an urgend update is needed to keep the USB surfstick working
- It advices you to connect to the Vessel WLAN before installing an update for minimum data usage.

Defense

- Check if the supporter is or should be accompanied by a person from your company.
- Check if he holds the necessary

Joker

Report the incident immediately to the CISO, who will initiate further steps.

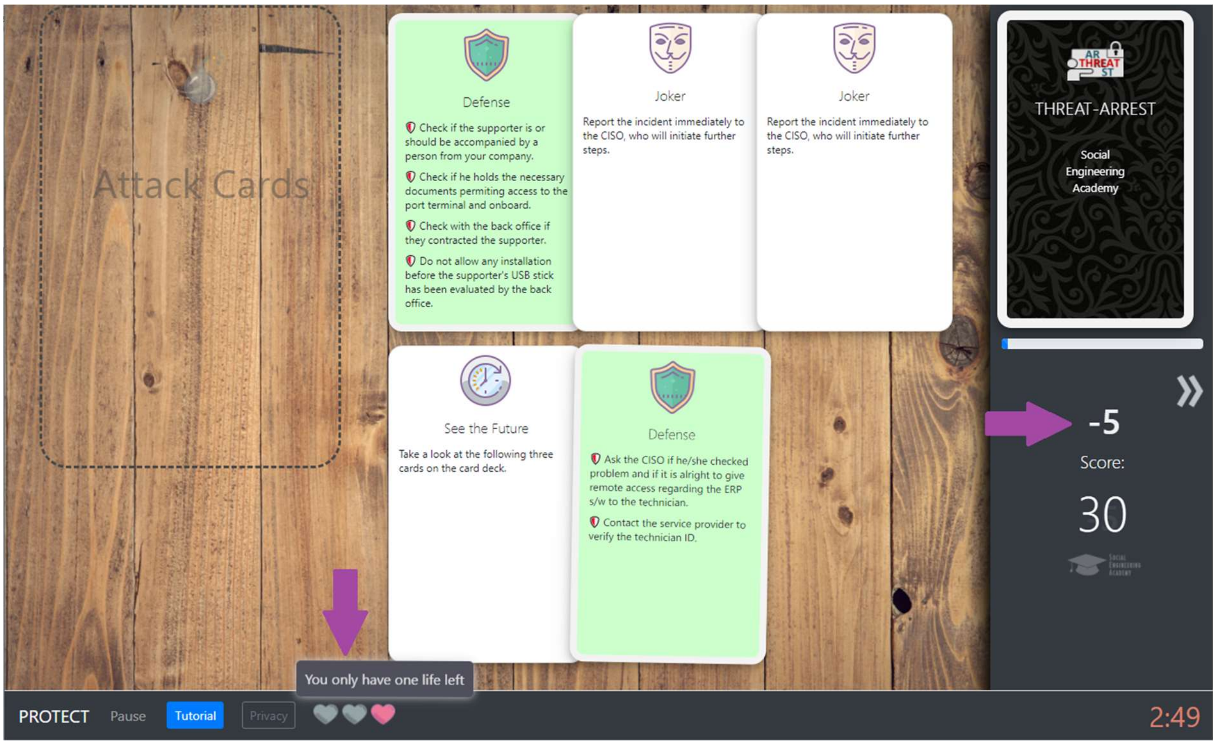
Joker

Report the incident immediately to the CISO, who will initiate further steps.

Correct Defense

- Do not switch to the WLAN of the vessel.
- Do not click on the popup window.
- Close the popup window if possible.
- Inform the CISO and internal IT about the event.

Figure 45: Display of the correct defense after an incorrect Defense Card has been selected



Defense

- Check if the supporter is or should be accompanied by a person from your company.
- Check if he holds the necessary documents permiting access to the port terminal and onboard.
- Check with the back office if they contracted the supporter.
- Do not allow any installation before the supporter's USB stick has been evaluated by the back office.

Joker

Report the incident immediately to the CISO, who will initiate further steps.

Joker

Report the incident immediately to the CISO, who will initiate further steps.

See the Future

Take a look at the following three cards on the card deck.

Defense

- Ask the CISO if he/she checked problem and if it is alright to give remote access regarding the ERP s/w to the technician.
- Contact the service provider to verify the technician ID.

You only have one life left

Figure 46: Animations after incorrect answer

As it can be seen in Figure 46, 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 subsection 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, et al., 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 47) 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:

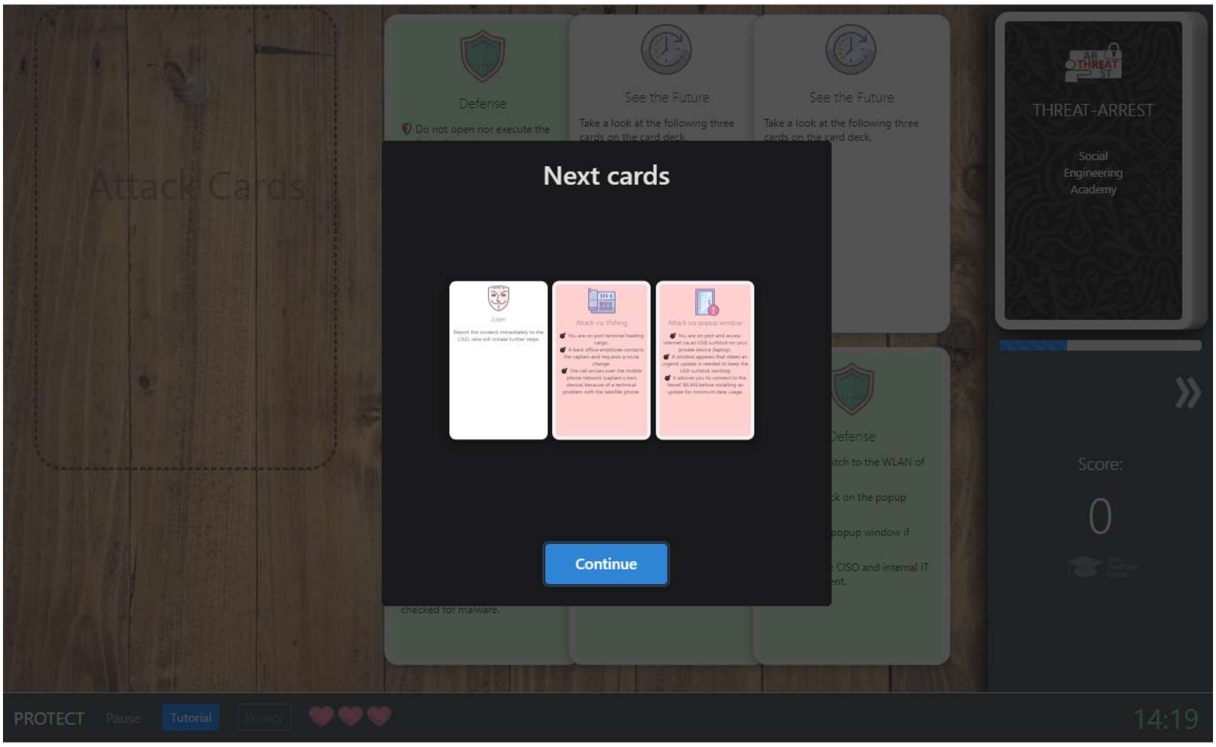
- on his/her hand, or
- contained in the future cards itself at the right position.

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.

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 is used for players at the beginner level. Accordingly, the original algorithm is used for advanced players in more ambitious training programmes. During an instantiation of PROTECT, it can be configured which concept shall be used.



Do not open nor execute the

Take a look at the following three cards on the card deck.

Take a look at the following three cards on the card deck.

Report the incident immediately to the USO, who will initiate further steps.

- You are on port terminal loading cargo.
- A back office employee contacts the captain and requests a route change.
- The call arrives over the mobile phone network (captain's own device) because of a technical problem with the satellite phone.

- You are on port and access internet via an USB surfstick on your private device (laptop).
- A window appears that states an urgend update is needed to keep the USB surfstick working.
- It advises you to connect to the Vessel WLAN before installing an update for minimum data usage.

checked for malware.

Figure 47: Display of the next three cards on the top of the deck after playing a "See the future" card

2.3.4 PROTECT Card Decks

At the date of this deliverable, the following card decks have been created:

- *Smart Shipping card deck:* This card deck considers different social engineering attacks in the context of the THREAT-ARREST smart shipping pilot. The attack scenarios address the crew abroad ships as well as personnel onshore.
- *Health Care card deck:* This card deck has been created in the context of the THREAT-ARREST health care pilot. It includes several social engineering attacks with respect to employees of a cancer registry.
- *Smart Home card deck:* The content of this card deck addresses a scenario regarding the THREAT-ARREST smart home pilot. Because this card deck does not consider social engineering scenarios, it shows that the usage of PROTECT can be extended to further aspects of information security. The smart home card deck has been developed for training product-owners of smart home devices. To this, the content of the card deck addresses information security and data protection aspects which have to be considered in the design of smart home devices. In this connection, the first card type represents potential threats to smart home devices. The second card type represents corresponding security requirements which have to implemented by a smart home device to counteract the different threats. Accordingly, for a threat card the corresponding security requirement card has to be selected.
- *General Social Engineering card deck:* This card deck considers general social engineering attacks which do not correspond to any of the THREAT-ARREST pilots.

2.3.5 Summary of Features

Table 7 summarizes the features of PROTECT.

Table 7: 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 address the THREAT-ARREST pilot scenarios *smart shipping*, *smart home* and *health care*.

3 Trainee performance assessment design for Serious Games

3.1 Trainee Assessment Concept

As also described in detail in D4.8 (Hildebrandt, et al., 2021), the Training Tool acts as the main entry point and interface of the whole of the THREAT-ARREST platform. Apart from delivering user authentication, it provides an overview of all the available *Cyber Threat and Training Preparation* (CTTP) scenarios that are retrieved from the Assurance Tool, which can be assigned by the trainers to individual trainees.

Both trainers and trainees have access to detailed information pertaining to scenario information as well as assessment of each trainee's performance and scores from engaging the available courses and scenarios.

The detailed trainees' information also includes their profile details, such as their company role and expertise, that enables the trainers to create tailored courses based on the trainees' individual abilities.

The overall trainees' assessment is based on a multitude of metrics reported to the Training Tool by all participating modalities, such as the duration of gameplays, usage of hints, etc., are then compared and scored based on the expected action traces that are defined in the CTTP models.

3.2 Integration with Serious Games

When a scenario gameplay commences, the Training Tool first performs an overall health check of all participating modalities to ensure a priori the availability of all gameplay features and functionalities. With regards to the Gaming Tool this is done by a *Hypertext Transfer Protocol* (HTTP) request.

After the successful health check, the Training Tool releases the gameplay and instantiates and configures all modalities by providing their respective CTTP model. More details about the sequence of communications can be found in D4.11 (Koshutanski, et al., 2021).

The initialisation of the Gamification Tool is performed through a dedicated JWT-token-based URL call, which includes the CTPP model 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 interconnection with the Gamification Tool can be found in D4.11 (Koshutanski, et al., 2021).

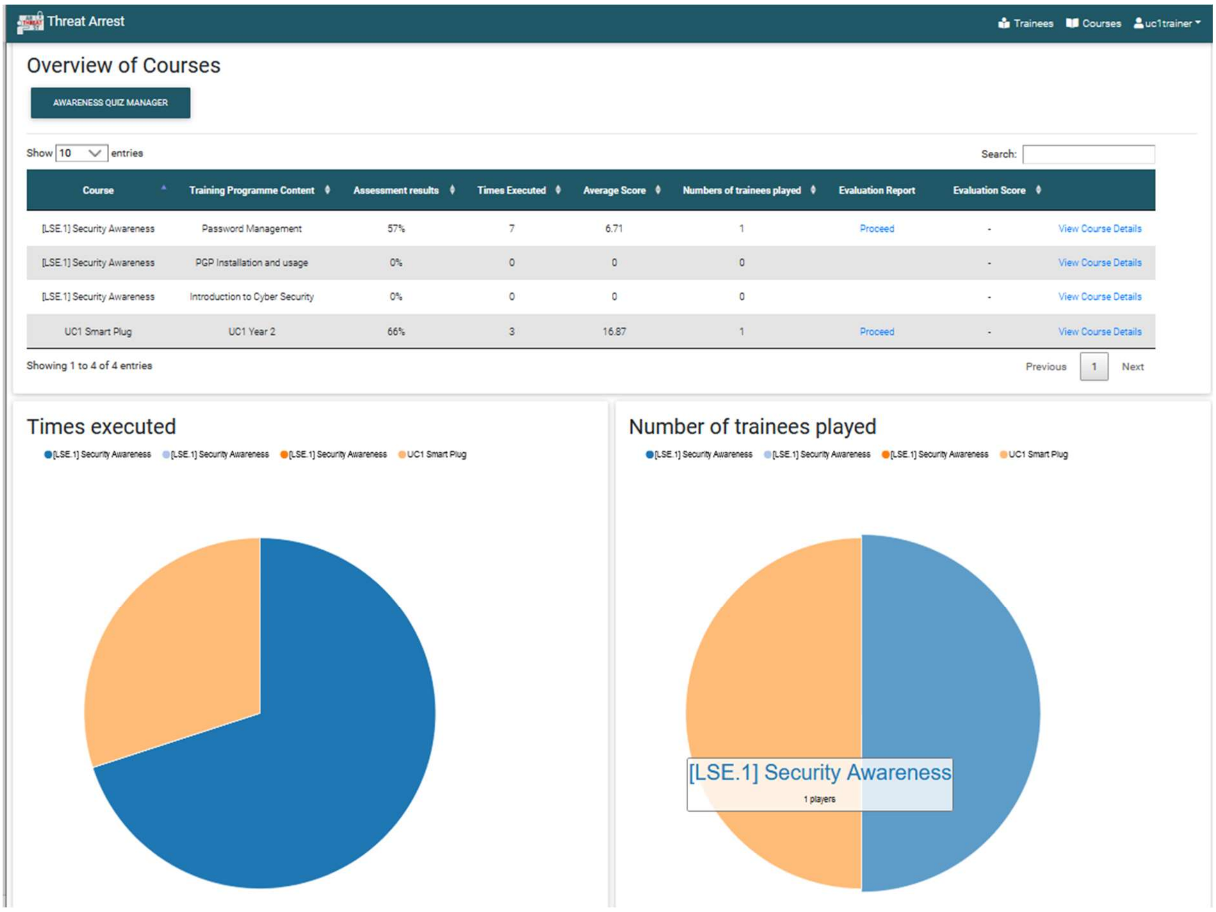
Upon completion of a gaming tool gameplay phase, detailed information is reported by the Gamification Tool to the Training Tool, containing the trainee's accumulated score, gameplay duration, etc., which is then portrayed in the overall trainee's performance dashboard.

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. The trainer/administrator will be able to have an overview of all scenarios, as depicted in Figure 48, and assign them to trainees. For the scenarios that include the playing of a game, the trainee is given secure links to connect to the interface of the relevant gaming tool. Upon completion of a trainee's gameplay, his/her score assessment is reported back to the Training Tool.

In terms of assessment, the trainer will have access to both an aggregated overview of all trainees (see Figure 49) and of more details for each trainee (see Figure 50).

Finally, each trainee will have an overview of his/her status through his/her personal dashboard (see Figure 51). More details about the functionalities of the Dashboard are presented in the deliverable "D4.8 – THREAT-ARREST visualisation tools v2" (Hildebrandt, et al., 2021).



Overview of Courses

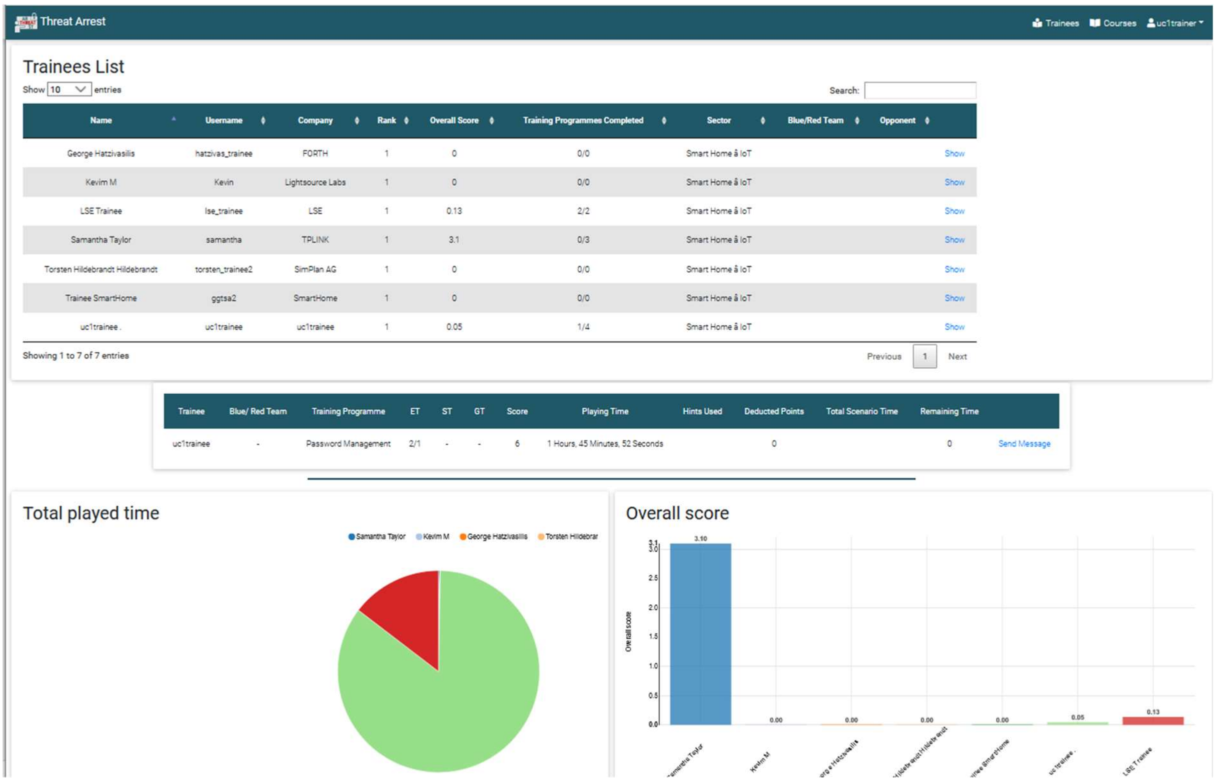
Course	Training Programme Content	Assessment results	Times Executed	Average Score	Numbers of trainees played	Evaluation Report	Evaluation Score	
[LSE.1] Security Awareness	Password Management	57%	7	6.71	1	Proceed	-	View Course Details
[LSE.1] Security Awareness	PGP Installation and usage	0%	0	0	0		-	View Course Details
[LSE.1] Security Awareness	Introduction to Cyber Security	0%	0	0	0		-	View Course Details
UC1 Smart Plug	UC1 Year 2	66%	3	16.87	1	Proceed	-	View Course Details

Showing 1 to 4 of 4 entries

Times executed

Number of trainees played

Figure 48: Visualisation of available scenarios in THREAT-ARREST Dashboard



Trainees List

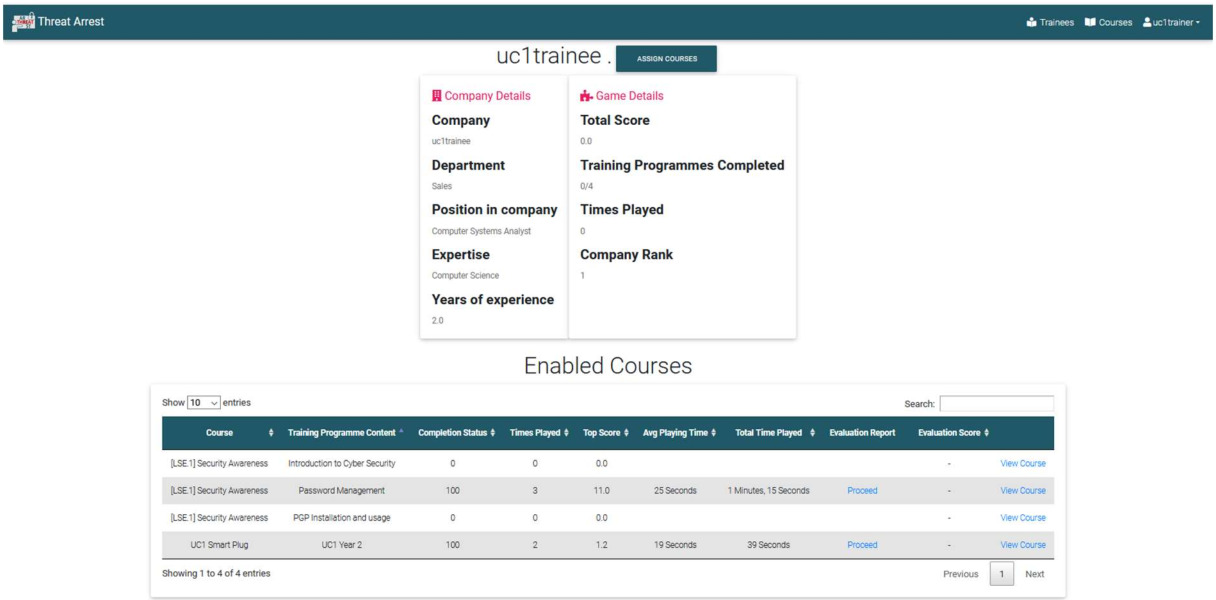
Show 10 entries Search:

Name	Username	Company	Rank	Overall Score	Training Programmes Completed	Sector	Blue/Red Team	Opponent	
George Hatzivasilis	hatzivas_trainee	FORTH	1	0	0/0	Smart Home â IoT			Show
Kevim M	Kevin	Lightsource Labs	1	0	0/0	Smart Home â IoT			Show
LSE Trainee	lse_trainee	LSE	1	0.13	2/2	Smart Home â IoT			Show
Samantha Taylor	samantha	TPLINK	1	3.1	0/3	Smart Home â IoT			Show
Torsten Hildebrandt Hildebrandt	torsten_trainee2	SimPlan AG	1	0	0/0	Smart Home â IoT			Show
Trainee SmartHome	ggtsa2	SmartHome	1	0	0/0	Smart Home â IoT			Show
uc1trainee .	uc1trainee	uc1trainee	1	0.05	1/4	Smart Home â IoT			Show

Showing 1 to 7 of 7 entries Previous 1 Next

Trainee	Blue/ Red Team	Training Programme	ET	ST	GT	Score	Playing Time	Hints Used	Deducted Points	Total Scenario Time	Remaining Time	
uc1trainee	-	Password Management	2/1	-	-	6	1 Hours, 45 Minutes, 52 Seconds		0		0	Send Message

Figure 49: Visualisation of trainees' assessment in THREAT-ARREST Dashboard



uc1trainee .

Company Details	Game Details
Company uc1trainee	**Total Score** 0.0
Department Sales	**Training Programmes Completed** 0/4
Position in company Computer Systems Analyst	**Times Played** 0
Expertise Computer Science	**Company Rank** 1
Years of experience 2.0	

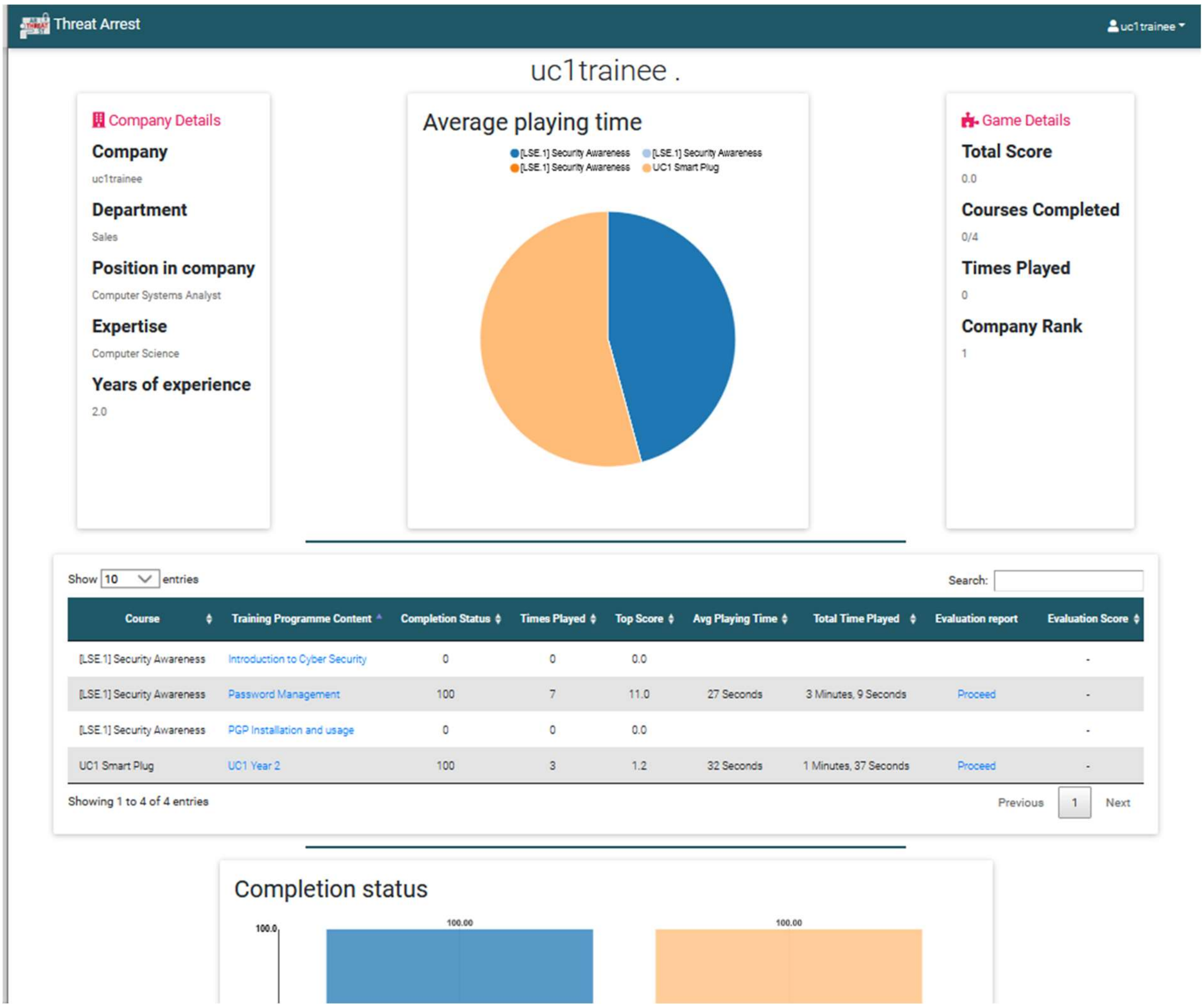
Enabled Courses

Show 10 entries Search:

Course	Training Programme Content	Completion Status	Times Played	Top Score	Avg Playing Time	Total Time Played	Evaluation Report	Evaluation Score	
[LSE.1] Security Awareness	Introduction to Cyber Security	0	0	0.0				-	View Course
[LSE.1] Security Awareness	Password Management	100	3	11.0	25 Seconds	1 Minutes, 15 Seconds	Proceed	-	View Course
[LSE.1] Security Awareness	PGP Installation and usage	0	0	0.0				-	View Course
UC1 Smart Plug	UC1 Year 2	100	2	1.2	19 Seconds	39 Seconds	Proceed	-	View Course

Showing 1 to 4 of 4 entries Previous 1 Next

Figure 50: Visualisation of individual trainee's assessment status in THREAT-ARREST Dashboard for trainers


Threat Arrest
uc1trainee
Average playing time
● [LSE.1] Security Awareness
● [LSE.1] Security Awareness
● [LSE.1] Security Awareness
● UC1 Smart Plug
100.0
100.00
100.00

uc1trainee .

Company Details

Company
uc1trainee

Department
Sales

Position in company
Computer Systems Analyst

Expertise
Computer Science

Years of experience
2.0

Game Details

Total Score
0.0

Courses Completed
0/4

Times Played
0

Company Rank
1

Show 10 entries Search:

Course	Training Programme Content	Completion Status	Times Played	Top Score	Avg Playing Time	Total Time Played	Evaluation report	Evaluation Score
[LSE.1] Security Awareness	Introduction to Cyber Security	0	0	0.0				-
[LSE.1] Security Awareness	Password Management	100	7	11.0	27 Seconds	3 Minutes, 9 Seconds	Proceed	-
[LSE.1] Security Awareness	PGP Installation and usage	0	0	0.0				-
UC1 Smart Plug	UC1 Year 2	100	3	1.2	32 Seconds	1 Minutes, 37 Seconds	Proceed	-

Showing 1 to 4 of 4 entries Previous 1 Next

Completion status

Figure 51: 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[12] (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.

[12] 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, 2020; 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 Training Scenarios for Serious Games

This chapter describes in a general way how trainings scenarios can be implemented for the serious gaming tools AWARENESS QUIZ (see subsection 5.1) and PROTECT (see subsection 5.2).

5.1 Implementation of a Training Scenarios for AWARENESS QUIZ

When a game of AWARENESS QUIZ is invoked in the TRAINING TOOL, the latter passes a CTTP gamification model to the AWARENESS QUIZ. This model includes all necessary information for playing a quiz game in the context of a particular training scenario. Based on the information from the passed CTTP gamification model, the parameters of the corresponding quiz to be played are configured. The value of the CTTP gamification model parameter *quizMode* indicates if a quiz is played with a predefined quiz or as a context quiz (see subsection 2.2.2). By means of this information, the backend of the AWARENESS QUIZ generates a configuration file for the instantiation of a quiz which contains the configuration parameters for the relevant mode. The configuration parameters for a quiz in the different quiz modes are defined in Table 8.

Table 8: Configuration parameters for a quiz

Configuration parameter name	Description	Relevant quiz modes
numberOfAvailableLives	Number of lives a player has during a quiz	both
timeForQuestion	Time in which a question shall be answered	both
pointsAddedToScore	Number of points by which the score is increased when a question is answered correctly	both
pointsRemovedFromScore	Number of points by which the score is decreased when a question is answered incorrectly	both
quizId	Identifier of the predefined quiz to be played	Predefined quiz
numberOfQuestions	The number of questions which shall be played in a context quiz	Context quiz
minDifficulty	Defines the minimum level of difficulty (weighting) for questions within the question set	Context quiz
maxDifficulty	Defines the maximum level of difficulty (weighting) for questions within the question set	Context quiz
questionMetdata	Defines the set of metadata parameters and corresponding types based on which the questions for the question set are determined	Context quiz
metadataType	Defines the type of metadata	Context quiz
metadataValue	Represents the metadata value(s) of the corresponding type	Context quiz

5.2 Implementation of Training Scenarios for PROTECT

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 which 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.

A game of PROTECT is invoked by the Training Tool. During the invocation the Training Tool passes a CTTP model which contains the necessary information on the basis of which of PROTECT is instantiated. This information includes the identifier of the card deck to be played and the time for the game. A further model information indicates the level of difficulty in which the game shall be played. In this context, a certain level of difficulty is mapped to the values of certain configuration parameters of PROTECT which are defined in Table 9. Every card deck can be played on different levels of difficulty. 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.

Table 9: 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
Gaming algorithm	Specifies the gaming mode: • *Beginner mode*: The needed Defense card to repel a drawn attack card is always on the player’s hand • *Advanced mode*: The needed Defense card to repel a drawn attack card is not necessarily on the player’s hand

6 Conclusions

This deliverable represents the second and last version of the documentation of the serious gaming tools. It describes the implementation of the serious games HATCH, AWARENESS QUIZ, and PROTECT.

With respect to HATCH, a newly implemented game scenarios and a new process for the creation of new game scenarios have been introduced. For AWARNESS QUIZ, its game concepts as well as the architecture of its components and the corresponding implementation have been described. Additionally, we introduced a modified approach for the management of content for AWARENESS QUIZ, including the definition of types for meta-information. Regarding PROTECT, the new implementation and partial improvement of the concepts of (Aladawy, et al., 2018) by PROTECT have been discussed. As an update, further improvements to PROTECT which have been implemented since the first version of this deliverable were described.

Furthermore, this deliverable has provided an updated version regarding the design for the assessment of trainees and the communication between the Training Tool and the Gamification Tool. Also, we discussed the compliances to the GDPR.

The main contributions of this deliverable are the concepts and implementation of the gaming tools as well as their integration into the THREAT-ARREST platform. At this, the integration includes the configuration of games within the gaming tools based on CTTP model information and their interactions with the Training Tool. An additional integration aspect addresses the creation of appropriate learning content which is provided by the gaming tools in the context of the THREAT-ARREST training programmes. During the creation of learning content for the different THREAT-ARREST pilots, it has been shown that the gaming tools provide the necessary flexibility to address most different scenarios.

The introduced process for the creation of new content for the AWRENESS QUIZ is supportive by keeping the learning content up to date. The tagging of learning content by metadata enables a straightforward realization of quizzes for certain themes.

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

Finally, this deliverable is part of the milestone “MS6 – Final version of THREAT-ARREST components”, due at M30.

7 References

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

Anon., 2019. *Falsche Polizei am Telefon.* [Online]
Available at: http://www.vorsicht-trickbetrug.de/telefon/falsche-polizei-telefon/
[Accessed 23 August 2019].

Anon., 2019. *Infromationspool.* [Online]
Available at: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/_function/Informationspool_Formular.html?nn=6651414
[Accessed 23 August 2019].

Anon., 2019. *Public Awareness and Prevention Guides.* [Online]
Available at: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides
[Accessed 23 August 2019].

Anon., 2019. *Real World Examples.* [Online]
Available at: http://www.social-engineer.org/framework/general-discussion/real-world-examples/
[Accessed 21 August 2019].

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

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

BSI ed., 2019. *Awareness-Poster - Psychotricks und Phishing-Maschen.*

dpa, 2016. *Deutsche Industrie zieht Cyberkriminelle an.* [Online]
Available at: http://www.xing-news.com/reader/news/articles/264892?link_position=digest&newsletter_id=12800&xng_share_origin=email
[Accessed 21 August 2019].

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.*

Faily, S. & Flechais, I., 2011. *Persona cases: a technique for grounding personas.*

Franceschi-Bicchierai, L., 2016. *Hacker Publishes Personal Info of 20,000 FBI Agents.* [Online]
Available at: https://www.vice.com/en_us/article/wnxdxq/hacker-publishes-personal-info-of-20000-fbi-agents
[Accessed 23 August 2019].

Fysarakis, K., Smyrlis, M., Frati, F. & Prusa, J., 2019. *D3.1: CTTP Models and Programmes Specification Language.*

Goeke, L., Pape, S., Beckers, K. & Bravos, G., 2019. *D4.2: THREAT-ARREST serious games v1.*

Goeke, L., Quintanar, A., Beckers, K. & Pape, S., 2019. *PROTECT - An Easy Configurable Serious Game to Train Employees Against Social Engineering.* Springer International Publishing.

Goodin, D., 2017. *Chrome, Firefox, and Opera users beware: This isn't the apple.com you want.* [Online]
Available at: https://arstechnica.com/information-technology/2017/04/chrome-firefox-and-opera-users-beware-this-isnt-the-apple-com-you-want/
[Accessed 21 August 2019].

Hazilov, V. & Pape, S., 2020. *Systematic Scenario Creation for Serious Security-Awareness Games.* Springer International Publishing.

Hesse, D. C., 2015. *Keine Geheimnisse mehr. - Methoden des Social Engineering.*

Hildebrandt, T. et al., 2019. *D4.1: THREAT-ARREST Visualisation Tools v1.*

Hildebrandt, T. et al., 2021. *D4.8: THREAT-ARREST Visualisation Tools v2.*

Koshutanski, H., Hildebrandt, T., Bravos, G. & Goeke, L., 2019. *D4.3: Training and Visualisation tools IO mechanisms v1,* THREAT-ARREST.

Koshutanski, H., Hildebrandt, T., Bravos, G. & Goeke, L., 2021. *D4.11: Training and Visualisation tools IO mechanisms v2.*

Lemos, R., 2013. *How Hacktivists Have Targeted Major Media Outlets.* [Online]
Available at: https://www.darkreading.com/vulnerabilities---threats/how-hacktivists-have-targeted-major-media-outlets/d/d-id/1140341
[Accessed 21 August 2019].

Pape, S., Goeke, L., Quintanar, A. & Beckers, K., 2020. *Conceptualization of a CyberSecurity Awareness.*

Peterson, C., 2016. *23 Social Engineering Attacks You Need To Shut Down.* [Online]
Available at: https://www.smartfile.com/blog/social-engineering-attacks/
[Accessed 21 August 2019].

Peters, S., 2015. *The 7 Best Social Engineering Attacks Eve.* [Online]
Available at: https://www.darkreading.com/the-7-best-social-engineering-attacks-ever/d/d-id/1319411?_mc=RSS%5FDR%5FEDT&amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;amp;piddl_msgorder=&image_number=1
[Accessed 21 August 2019].

Ries, U., 2016. *Sicherheits-Report: Unternehmen setzen selbst simple Schutzmechanismen nicht um.* [Online]
Available at: https://www.heise.de/security/meldung/Sicherheits-Report-Unternehmen-setzen-selbst-simple-Schutzmechanismen-nicht-um-3184485.html
[Accessed 21 August 2019].

Schaab, P., Beckers, K. & Pape, S., 2016. *A systematic Gap Analysis of Social Engineering Defence Mechanisms considering Social Psychology.*

Schaab, P., Beckers, K. & Pape, S., 2017. *Social Engineering Defence Mechanisms and Counteracting Training Strategies.*

Schaible, I., 2016. *Als Chef getarnt fordern Internet-Kriminelle Geld von Firmen.* [Online]
Available at: https://www.heise.de/security/meldung/Als-Chef-getarnt-fordern-

Internet-Kriminelle-Geld-von-Firmen-3208796.html
[Accessed 21 August 2019].

Terlizzi, M. A., Cunha, M. A. & Fernando , M. S., 2016. *Cybersecurity Governance: an experiment with Brazilian banks' employees on Facebook.* ResearchGate.

Threat Intelligence Team, 2020. *Cybercriminals impersonate World Health Organization to distribute fake coronavirus e-book.* [Online]
Available at: https://blog.malwarebytes.com/social-engineering/2020/03/cybercriminals-impersonate-world-health-organization-to-distribute-fake-coronavirus-e-book/
[Accessed 11 February 2021].