



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

D4.4: Real time trainee performance assessment v1[†]

Abstract: This deliverable provides the outline of the development of the THREAT-ARREST Training Tool, that will be the basis for the delivery of real time trainee performance assessment based on comparing trainee performance with expectations set by the Cyber Threat and Training Preparation (CTTP) programme itself in real time and producing qualitative and quantitative assessments as appropriate. In this first iteration, a preliminary version of trainee assessment is also presented in terms of results' visualisation.

Contractual Date of Delivery	29/02/2020
Actual Date of Delivery	29/02/2020
Deliverable Security Class	Public
Editor	<i>George Tsakirakis (ITML)</i>
Contributors	<i>George Bravos (ITML), George Leftheriotis (TUV), Martin Kunc (CZNIC)</i>
Quality Assurance	<i>Hristo Koshutanski (ATOS), Michalis Smyrlis (STS), George Hatzivasilis (FORTH)</i>

[†]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. *Hristo Koshutanski (ATOS)*
2. *Michalis Smyrlis (STS)*
3. *George Hatzivasilis (FORTH)*

Revisions Version	Date	By	Overview
1.0	28/02/2020	George Bravos, George Tsakirakis	Final version
0.5	17/02/2020	George Bravos	First version for internal reviewers
0.1	15/02/2020	George Tsakirakis	First Draft

Executive Summary

To facilitate the access of the end users (trainees, trainers, administrators) to the THREAT-ARREST training modules and the efficient assessment and monitoring of the results of the training sessions, in this deliverable we design and deploy the first version of the THREAT-ARREST Training Tool that enables real time assessment monitoring. Through the training tool, described in detail in this deliverable, both trainees and trainers are able to monitor performance of trainees in the different THREAT-ARREST scenarios. Last, a first approach for the trainees' performance assessment methodology has been deployed and described. This work is the initial result of the task "T4.3 – Real time trainee performance assessment".

Table of Contents

1	INTRODUCTION	9
2	REAL TIME TRAINEE ASSESSMENT	10
2.1	INDIVIDUAL TRAINEE ASSESSMENT	10
2.1.1	<i>Course evaluation</i>	<i>10</i>
2.1.2	<i>Serious game evaluation</i>	<i>10</i>
2.1.3	<i>Virtual lab evaluation.....</i>	<i>11</i>
2.1.3.1	Evaluation with a Report – Healthcare digital forensics scenario.....	12
2.1.3.2	Evaluation with an Event captor – Smart Shipping Navigation combo attack scenario.....	13
2.1.3.3	Evaluation with a Simulated attack – Smart Energy Secure configuration scenario.....	14
2.1.4	<i>Qualitative Report.....</i>	<i>14</i>
2.2	AGGREGATED METRICS.....	15
3	IMPLEMENTED USER ROLES AND PRIVILEGES	16
3.1	ADMINISTRATOR	16
3.2	TRAINER.....	16
3.3	TRAINEE	16
4	FUNCTIONALITY & DASHBOARD INTERFACES.....	17
4.1	LOGIN SCREEN	17
4.2	PASSWORD RECOVERY	17
4.3	ADMINISTRATOR PERSPECTIVE	18
4.3.1	<i>Users View (Admin)</i>	<i>18</i>
4.3.2	<i>Trainees View (Admin).....</i>	<i>19</i>
4.3.3	<i>Scenarios View (Admin).....</i>	<i>22</i>
4.4	TRAINER PERSPECTIVE	25
4.4.1	<i>Trainee View (Trainer).....</i>	<i>25</i>
4.4.2	<i>Scenario View (Trainer).....</i>	<i>27</i>
4.5	TRAINEE PERSPECTIVE	29
4.5.1	<i>Profile (Trainee).....</i>	<i>29</i>
5	CONCLUSIONS.....	32
	REFERENCES.....	33
	APPENDIX I	34
	APPENDIX II.....	36

List of Abbreviations

CTTP Cyber Threat and Training Preparation

DB Database

ET Emulation Tool

GT Gamification Tool

MS Milestone

ST Simulation Tool

TA THREAT-ARREST

TT Training Tool

VM Virtual Machine

VT Visualization Tool

List of Tables

Table 1. Trainee performance references	36
---	----

List of Figures

Figure 1 – Preliminary scoring method for trainees’ performance assessment	15
Figure 2 – Login Page	17
Figure 3 – Password Recovery	17
Figure 4 – Example of Password Change Email.....	18
Figure 5 – All Users Screen	18
Figure 6 – Add a User	19
Figure 7 – User Details.....	19
Figure 8 – Trainees List	20
Figure 9 – Trainees General Statistics.....	20
Figure 10 – Trainee Details	21
Figure 11 – Assigned Scenarios	21
Figure 12 – Edit Scenario Role	22
Figure 13 – Overview of Scenarios.....	22
Figure 14 – Scenarios Global Graphs	23
Figure 15 – Scenario Details	24
Figure 16 – Scenario Graphs	24
Figure 17 – Trainees List	25
Figure 18 – Trainees General Statistics.....	25
Figure 19 – Trainee Details	26
Figure 20 – Assigned Scenarios	26
Figure 21 – Edit Scenario Role	27
Figure 22 – Overview of Scenarios for Trainer	27
Figure 23 – Scenario Details	28
Figure 24 – Scenario Graphs	28
Figure 25 – Trainee Profile	29
Figure 26 – Statistics of Trainee	30
Figure 27 – Scenario Details	31

1 Introduction

The real time trainee performance assessment is designed based on a wider framework entitled “THREAT-ARREST Training Tool” that, according to the refined THREAT-ARREST architecture is one of the core modules in the THREAT-ARREST platform and acts as the entry point for all THREAT-ARREST users in order for them to use the provided features and functionalities of the platform. Its main goal is to provide real time assessment of the trainees’ performance while they engage with the available training scenarios provided by the Cyber Threat and Training Preparation (CTTP) models. In order to facilitate this, the Training Tool (TT) offers all required services that mainly consist of:

- Main Authentication Server for the THREAT-ARREST (TA) Platform.
- Association of trainers and trainees with their sector and respective CTTP scenarios.
- Retrieval of the CTTP models and sub models from the CTTP Database (DB) and instantiation of the relevant THREAT-ARREST modules.
- Real time overview of the trainees’ progress while they engage in the individual modules (Gamification Tool (GT) / Emulation Tool (ET) / Simulation Tool (ST)).

Due to the fact that the relevant THREAT-ARREST modules and the finalized definition of their integration in the THREAT-ARREST platform was not yet fully achieved at the time of the development of this initial version of the TT, a number of proactive assumptions and steps were made to provide a temporary solution in order to be able to fully portray the TT’s functionalities.

For instance, advanced processing of CTTP models for comparing trainee performance with expectations set by the CTTP programme according to real time user activities reported by GT, ET, and ST, and producing qualitative and quantitative assessments will be completed once sufficient level of platform and tools integration is achieved to allow for such assessment.

The Training Tool and the first version of the trainee assessment procedures have been successfully populated in the THREAT-ARREST dedicated server provided by the system’s integrator (ATOS).

The rest of the document is structured as follows: **Chapter 2** details the trainee assessment methods, **Chapter 3** introduces the TT, **Chapter 4** presents the visualization perspectives of the Dashboard concerning the trainee’s assessment, and **Chapter 5** concludes and links the deliverable content with other related tasks/deliverables.

Moreover, Appendix I documents the CTTP model elements that drive the automated assessment of the trainee. Appendix II summarizes a list of related methods for trainee and programme evaluation that are also examined under THREAT-ARREST and the final CTTP programme evaluation, which will be defined in the next iteration of T4.3 (“D4.6 – Real time trainee performance assessment v2” due at M28).

2 Real Time Trainee Assessment

As the trainee goes through the various training phases, means to assess his/her *individual performance* at each stage (e.g. at courses, games, and virtual labs) are needed. Also, *techniques* for the continuous evaluation and adjustment a CTPP programme for all the trainees for an examined organization are required (e.g. (Manifavas et al., 2014; Fysarakis et al., 2015)). The next subsections detail the individual as well as the aggregated evaluation methods for the first version of the THREAT-ARREST platform.

2.1 Individual Trainee Assessment

2.1.1 Course evaluation

The individual learning process starts from the traditional training procedures in the **Training Tool (TT)**. Here, the evaluation methods of the ordinary training platforms can be used. Therefore, the trainee takes courses on the involved security topics (e.g. on social-engineering, network security, etc.) and can be evaluated based on on-line examinations, exercises, and/or capstone projects. In general, for each of these elements the trainee receives a grade from *0-10* (from minimum to maximum) and the final course grade is a weighted summation of them. In the aggregated trainee assessment formula (detailed in the subsection 2.2), this score is called as **SCR 1.1**. Indicative cases may include:

- $SCR\ 1.1 = 100\% \text{ on-line test score}$
- $SCR\ 1.1 = 80\% \text{ on-line test score} + 20\% \text{ average exercises score}$
- $SCR\ 1.1 = 70\% \text{ on-line test score} + 30\% \text{ capstone project score}$
- $SCR\ 1.1 = 50\% \text{ on-line test score} + 30\% \text{ capstone project score} + 20\% \text{ average exercises score}$

Then, the trainee proceeds to the advance training, including serious games or virtual labs with emulated/simulated components. Here is the main contribution of THREAT-ARREST in this deliverable.

2.1.2 Serious game evaluation

The first version of the **Gamification Tool (GT)** is described in the deliverable “D4.2 – THREAT-ARREST serious games v1”. In general, the THREAT-ARREST serious games have their own point system, which takes into account the difficulty level. Here, it can be defined by how many points the score is increased for a correct action and by how many points the score is decreased for an incorrect action. Additionally, it can be defined if the score can be less than zero during a game. The difficulty level can also be affected by further parameters. By using the example of the game PROTECT, it can be affected among others by the game time and the number of lives and joker cards.

Thus, the GT knows by its own which are the correct actions that the trainee has to perform. When a game is over, the score is returned back to the TT. This score is called **SCR 1.2**, its range is defined by the CTPP model, e.g. *0-10*, and it is calculated as follows:

$$SCR\ 1.2 = \sum Scores\ of\ correct\ actions - \sum Score\ of\ incorrect\ actions \\ - Remaining\ time\ impact$$

In the next version of the platform, the calculation of the score will take into account if the trainee uses any hints during a game. The impacts of these hints will be driven by the CTPP model (given as input to the GT by the Gamification sub-model during the game instantiation).

2.1.3 Virtual lab evaluation

On the other hand, for the **Emulation Tool (ET)** and **Simulation Tool (ST)**, the evaluation of the trainee is modelled by the '*expected trace*' of the CTP model. For the evaluation of the trainee, three (3) methods will be supported:

1. Evaluation report

- a. **Description:** The evaluation report is the ordinary way to evaluate trainees in cyber-ranges. The trainee is given a scenario and the virtual lab (with emulated/simulated components) to work with. Then, he/she has to examine the problem and perform the designated actions. At the end, a report must be fulfilled, where the trainee answers specific questions regarding this virtual lab (e.g. which was the problem, how many nodes were compromised, which mitigation actions were performed, etc.).
The *expected trace* contains the correct answers for an evaluation report and the TT can automatically evaluate the trainee based on the actual trace which will be reported by the tool.
- b. **Advantages:** The report is a generic evaluation method that can cover the evaluation requirements for a high variety of scenarios that could not be verified automatically otherwise.
- c. **Drawbacks:** The report captures the fact that the trainee knows the correct answer in a question, and which are the correct actions that he/she should have performed. However, the tools do not verify that these actions have been actually performed in the virtual environment.

2. Event captors

- a. **Description:** The event captors are software modules, which we have been deployed beforehand in the virtual components and capture specific trainee's actions. For example, event captors can be triggered when the trainee interacts with the Graphical User Interface (GUI), e.g. press a button in a simulator or change the configurations of an emulated system. The captors are part of the architecture of the Emulation and Simulation Tools, as they are described in the deliverables "D2.1 – Emulated components' generator module v1" and "D5.2 – Simulated components and network generator v1", respectively.
- b. **Advantages:** The captors can capture a specific type of interaction. In contrast to the evaluation report, with the captors we can verify that the trainee has actually perform the designated actions.
- c. **Drawbacks:** However, it requires time and effort to implement them. Moreover, in some cases THREAT-ARREST users are not authorized to change the original software and deploy them; thus, their applicability may be constrained.

3. Simulated attacks

- a. **Description:** With the simulated attacks, the injected vulnerabilities of the virtual system are exploited by performing an attack (e.g. (Hatzivasilis et al., 2019b; Hatzivasilis et al., 2019c; Hatzivasilis et al., 2017)). For example, in case that one needs to check if the trainee has changed the default password for a service, a simulated attack (triggered automatically or performed by the trainer) can try to login the service with the default credentials. If it succeeds, the trainee fails the evaluation.
- b. **Advantages:** The THREAT-ARREST users can test if the trainee has actually safeguarded a software or other module for which we cannot deploy an event captor.

- c. **Drawbacks:** The main drawback is that the exploit for an injected vulnerability needs to be prepared. As with the event captors, this demands time and effort.

In the following subsections, the related content of the CTPP models for three indicative scenarios documented in the deliverable “D3.3 – Reference CTPP Models and Programmes Specifications v1” is described, as they are retrieved by the TT and contain information for the evaluation of the trainee based on a report, an event captor, and a simulated attack, respectively. At these examples, the three evaluation methods are described independently, but combinatory settings can be driven by the model in a later development phase.

2.1.3.1 Evaluation with a Report – Healthcare digital forensics scenario

For the healthcare use case, digital forensics scenario will be demonstrated. The trainee is given a Virtual Machine (VM) (emulated component with the ET) that contains the backend system of the ARESS registry that has been attacked. The trainee must perform a digital forensics analysis, discover what has happened, mitigate the malicious side-effects, and fix the problem. However, it is not easy (and in some cases it is not feasible either) to monitor all these actions via event captors or simulated attacks. Thus, when the trainee completes the exercise, he/she must complete a related evaluation report.

The generation of the report is driven by the CTPP model. Based on the vulnerabilities that we have instantiated in the emulated component and the response actions that must be performed, the *expected trace* is formed. The trace contains the questions, the correct answers, and their score. The information is parsed by the TT and creates the evaluation report as an HTML form. A simple example of the expected trace for this use case is presented below:

- Evaluation report
 - Question Set
 - Question
 - Number: 1
 - Description: “Was there any attack performed”
 - Type (HTML): radio
 - Answers: [“Yes”, “No”]
 - Correct Option: “Yes”
 - SuccessScore: 2.5
 - Hint: “The logs must be carefully examined!”
 - HintImpact: 0.5
 - Question
 - Number: 2
 - Description: “Which was the attack”
 - Type (HTML): custom-select
 - Answers: [[“0”, “Denial of service”], [“1”, “Disclosure of health records”], [“2”, “Ransomware”], [“3”, “Crypto-miner”], [“4”, “Botnization”]]
 - Correct Option: [“1”, “Disclosure of health records”]
 - SuccessScore: 2.5
 - Hint: “Check the examined logs for the nature of the attack”
 - HintImpact: 0.5
 - Question
 - Number: 3
 - Description: “Was there any compromised user account”

- Type (HTML): text
 - Answers: ["If yes, input compromised user account here"]
 - Correct Option: ["User-2"]
- SuccessScore:2.5
- Hint: "Check the user's ID inside the log file"
- HintImpact: 0.5
- Question
 - Number: 4
 - Description: "Which was the mitigation actions that you performed"
 - Type (HTML): checkbox
 - Answers: ["None", "Anti-virus update", "Anti-virus scan", "Restore system from a previous unaffected time-point", "Suspend compromised user's access", "Inform compromised user"]
 - Correct Option: ["Suspend compromised user's access", "Inform compromised user"]
 - SuccessScore:2.5
 - Hint: "These kinds of attacks usually needs strong mitigation actions"
 - HintImpact: 0.5

The related information in a JSON format is detailed in Appendix I.

The score for the evaluation report is the summation of the underlying scores for the correctly answered questions, modelled as **SCR 1.3**.

$$SCR\ 1.3 = \sum Scores\ of\ correct\ answers$$

This is a number between 0-10.

2.1.3.2 Evaluation with an Event captor – Smart Shipping Navigation combo attack scenario

For the Smart Shipping use case and the navigation combo attack scenario, the captain will be evaluated based on the events that are reported to the TT by related captors that are pre-installed in the ST. In this scenario, the trainee must first identify from the received emails (legitimate or malicious ones) the destination for the trip and then detect and mitigate the GPS-spoofing attack during the journey. Thus, the *expected trace* contains these two actions:

- The final destination of the journey
 - The trainee inputs the destination to the Visualization Tool (VT) and presses a button to start the trip to this destination. The action triggers the event captor that informs the TT and may also start the related simulation, if the destination is the correct one.
- The navigation of the ship based on the manual procedures and not the automated via the GPS signals (which are under attack)
 - The trainee performs this type of action by pressing a related button in the visualized view (by the VT) of the simulated environment. The pressed button triggers the event captor that reports the event back to the TT.

The *expected trace* as well as the reported events by the captors in a JSON format are reported

in Appendix I.

The score for the event captor is the summation of the underlying scores for the correctly performed actions (as reported in the *expected trace*), modelled as **SCR 1.3**.

$$SCR\ 1.3 = \sum Scores\ of\ correct\ actions$$

This is a number between 0-10.

In the next version of the platform, the CTTP model will penalize the trainee as time elapses and the correct actions are not performed or if the user uses a hint or other assistance (given as input to the TT by the Emulation/Simulation sub-models during the virtual lab instantiation).

2.1.3.3 Evaluation with a Simulated attack – Smart Energy Secure configuration scenario

For the Secure configuration scenario of the Smart Energy use case, the technician will be evaluated based on the events that are reported to the TT by related simulated attacks that are pre-installed in the ST. In this scenario, the technician must cross-check if the current deployment of the LSE system in a house preforms correctly. During the instantiation of the virtual lab from the CTTP model, we may inject compromised smart plugs or smart-home devices (e.g. (Fysarakis et al., 2014; Hatzivasilis et al., 2019a)). For each of these devices, the simulator models the malicious behaviour. This results to specific energy readings that are observable by the trainee. Therefore, he/she must detect them and restore the firmware (specific interaction that is performed via the VT). When this action is actually performed, the simulated attack is stopped and the related module sends a message back to the TT, informing that the attack was successfully blocked.

As in the previous case, the score for the simulated attacks is the summation of the underlying scores for the correctly performed actions (as reported in the *expected trace*), modelled as **SCR 1.3**.

$$SCR\ 1.3 = \sum Scores\ of\ blocked\ attacks$$

This is a number between 0-10.

In the next version of the platform, the CTTP model will penalize the trainee as time elapses and the simulated attacks are not blocked or if the user uses a hint or other assistance (given as input to the TT by the Emulation/Simulation sub-models during the virtual lab instantiation).

2.1.4 Qualitative Report

After the completion of the training programme, the THREAT-ARREST evaluation approach gives also the opportunity to the trainer to provide a qualitative feedback for the trainee. This is supported in the form of a report based on a pre-defined *Trainer's Checklist*. Thus, the trainer fulfils these reports for all the underlying trainees of the programme. This checklist will cover aspects of the training process that are not currently captured by the aforementioned automated and quantitative mechanisms, like the cooperation of the trainee, his/her overall attitude during the training, etc. In the aggregated trainee assessment formula, this score is called as **SCR 2** and it will be also mapped in a numeric value in the range 0-10.

This type of trainee assessment will be the subject for the next version of the integrated platform.

2.2 Aggregated Metrics

For this initial version of the TT, a first approach has been also deployed with respect to the aggregated scoring of the trainees in the several training scenarios, in order to provide real time assessment information through the interface of the TT (described in more detail in Section 4). Based on a number of research efforts (see Appendix II), we have come up with a preliminary methodology that is briefly depicted in Figure 1. Based on that, two complementary basic scoring sources (already described in Section 2.1) are being used: a quantitative (automated), based on the aforementioned TREAT-ARREST platform tools and the relevant information derived from the CTPP models; and a qualitative (manual), e.g. a checklist from the trainer. The first one can be broken down to three sub-scores from the TT, the GT, and the virtual labs with the ET and ST; and the overall score is computed based on the formula presented in the figure, with the weights of each score to be defined by the administrator or the trainer.

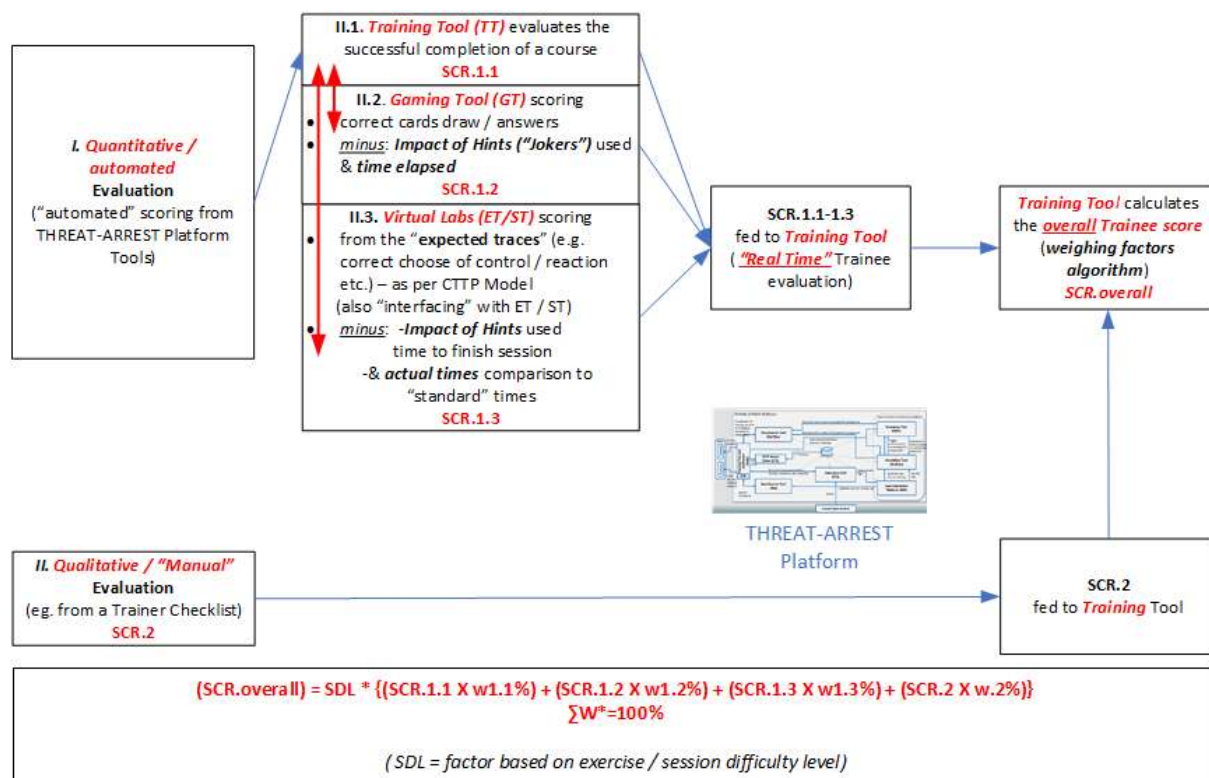


Figure 1 – Preliminary scoring method for trainees' performance assessment

Except from the individual progress of each trainee, we also need a way to evaluate a CTPP programme for an organization as a whole. Thus, in the next version of the platform, we will also need aggregated metrics to capture the success of all organization trainees. Some of them presented in the Section 4 below.

On top of all that, a number of references have been identified (see Appendix II) and will be further analysed towards the final trainee performance assessment methodology to be applied in the next version of the TT.

3 Implemented User Roles and privileges

The TT Dashboard offers different views and functionalities per user's role. The implemented roles are the ones of:

- Administrator
- Trainer
- Trainee

3.1 Administrator

The Administrator can do any the following actions:

- Manage users imported from the Core CTP model or add new (trainers and trainees)
- Access an overview of all trainers'/trainees' information and Scenarios regardless of his/her sector
- Enable/Disable the available scenarios for all Trainees
- Appoint/Change a Trainee's Role for a given scenario

3.2 Trainer

Trainers can do any the following actions:

- Access an overview of all trainers/trainees and scenarios belonging to each trainer's sector
- Enable/Disable scenarios for trainees belonging to each trainer's sector
- Appoint/Change Scenario Role for Trainees belonging to each trainer's sector

3.3 Trainee

Trainees can do any the following actions:

- Access an overview of their info, Statistics & Scores per Scenario
- Play a scenario

4 Functionality & Dashboard Interfaces

This Section presents the main functionality of the TT and the involved Dashboard interfaces for monitoring the trainee's assessment.

4.1 Login Screen

The users can log in to the platform by entering their Username and Password (Figure 2 – Login Page).

The screenshot shows the 'Login Page' of the THREAT-ARREST system. On the left is a dark teal sidebar with the system logo (a stylized 'A' with 'THREAT' and 'ARREST' text) and a 'Login' link. The main content area is light gray and contains the title 'Login Page'. Below the title are two input fields: 'Username *' and 'Password *', each with a small red asterisk indicating a required field. Below the password field is a dark teal 'Log In' button. At the bottom of the form is a purple link that says 'Reset your password'.

Figure 2 – Login Page

4.2 Password recovery

By clicking on the “Reset your password” link on the Login Screen, the user enters his/her registered email and receives an email containing a unique web link that can be used to reset a password. For security reasons the link is valid for 10 minutes (Figure 3 – Password Recovery, Figure 4 – Example of Password Change Email).

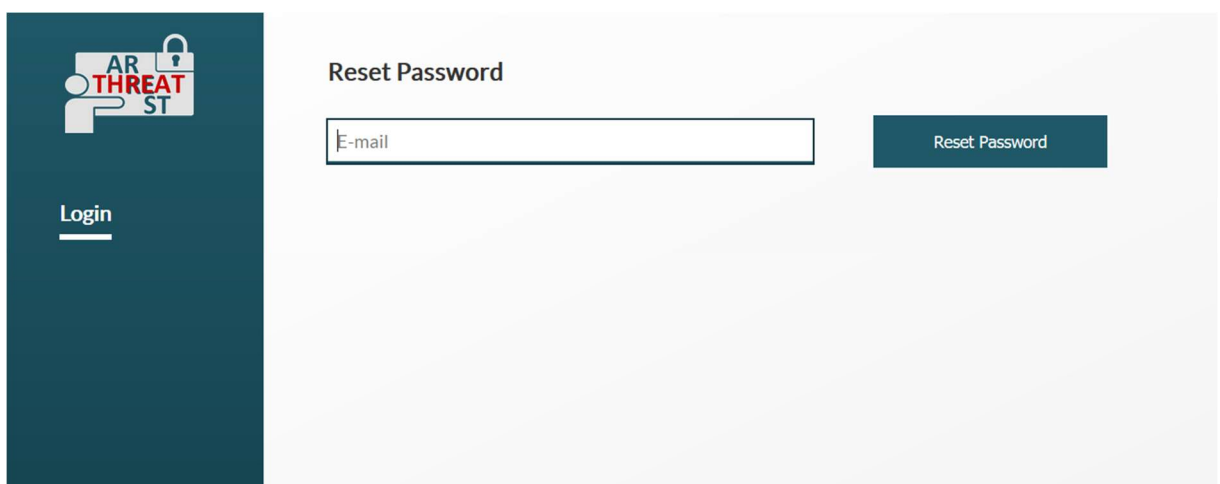
The screenshot shows the 'Reset Password' interface. On the left is the same dark teal sidebar as in Figure 2, with the logo and a 'Login' link. The main content area is light gray and contains the title 'Reset Password'. Below the title is a single input field labeled 'E-mail'. To the right of the input field is a dark teal button labeled 'Reset Password'.

Figure 3 – Password Recovery

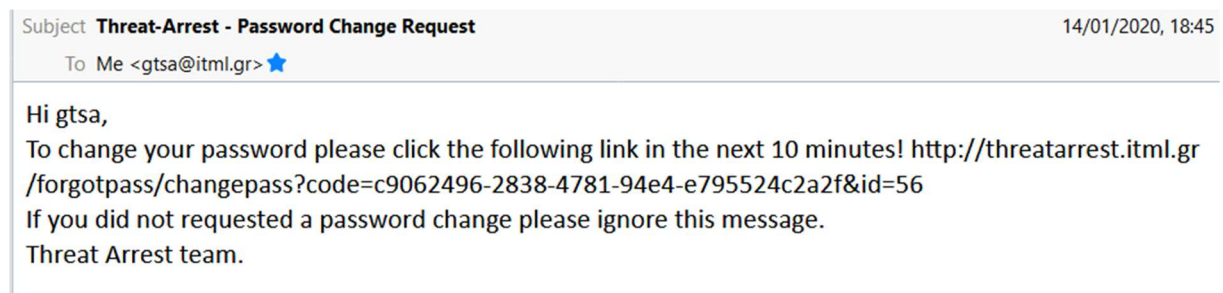


Figure 4 – Example of Password Change Email

4.3 Administrator Perspective

The administrator perspective provides several views and information available to the administrator.

4.3.1 Users View (Admin)

The administrator, after successfully logs in to the platform, he/she has a condensed view of all TA users (trainers and trainees) consisting of their Name, Username and Role in the platform. (Figure 5 – All Users Screen).

Show All Users

Show entries Search:

Name	Username	Role	
Eleni Liarou	eleni	Trainee	Show
George Tsakirakis	gtsa	Trainer	Show
Julio Iglesias	julio	Trainer	Show
Manolis Theodosiou	manolis	Trainee	Show
Mary Johnson	maria	Trainee	Show
Michael Atkinson	health_trainee1	Trainee	Show
Michael Smith	michael	Trainer	Show
Mixalis Stergiou	mixalis	Trainer	Show
T R	trainer	Trainer	Show

Showing 1 to 9 of 9 entries

Previous Next

[Add a user](#)

Figure 5 – All Users Screen

Administrators can add new users by clicking the button [Add a User](#) and insert their personal and company details (Figure 6 – Add a User).

Additionally, a role (trainer/trainee) and a sector is appointed to the new user. This enables the TT to provide the relative CTPP scenarios per sector/group, as well as enable the trainer to have an overview only of trainees of the same sector. A finer grained view of the trainers will be considered in next stage of the project (the second version of the tool) where trainers will be limited to per organization view.

Users
Add User

User Details	Company Details	Role & Sector
Username * Password * Email * Name Surname	Company Department Position in company Expertise Years of experience	ROLE_TRAINER Smart Home – IoT Submit user

Figure 6 – Add a User

By clicking on an individual user entry ([Show](#)), the Admin can view and update users' information as well as disable or delete them (Figure 7 – User Details).

User Details


User Details	Company Details
Name George Surname Tsakirakis Email gtsa@itml.gr Company ITML	Department IT Position in company Technical Manager Expertise Network and App Development Years of experience 10

Update
[Delete](#) - [Disable](#)

Figure 7 – User Details

4.3.2 Trainees View (Admin)

The Trainees View contains all trainees' information regardless of their sector together with their rank, overall score and the scenarios that they have successfully completed. (Figure 8 – Trainees List).



Users
Trainees
Scenarios
Logout

Trainees List

Show 10 entries

Search:

Name	Username	Company	Rank	Overall Score	Scenarios Completed	
Eleni Liarou	eleni	Microsoft	1	7.2	0/1	Show
Manolis Theodosiou	manolis	GNT	2	6.38	1/2	Show
Mary Johnson	maria	Amazon	1	4.77	0/1	Show
Michael Atkinson	health_trainee1	GNT	1	7.54	1/2	Show

Showing 1 to 4 of 4 entries

Previous 1 Next

Figure 8 – Trainees List

Furthermore, at the bottom of the page there are graphs with statistics of Total played Time and Overall Score (Figure 9 – Trainees General Statistics).

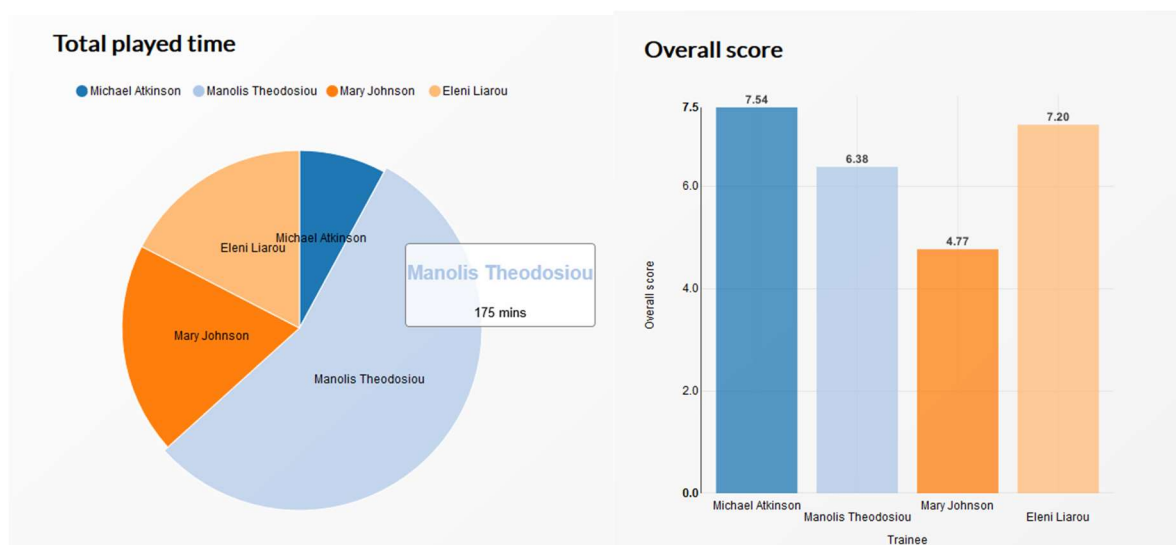


Figure 9 – Trainees General Statistics

By clicking the [Show](#) button on any Trainee, you are presented with the Company details and Game details of the specific trainee as well as his/her enabled scenarios (Figure 10 – Trainee Details).

Trainees
Eleni Liarou

Company Details

Company
Microsoft

Department
Human Resources

Position in company
Head of HR

Expertise

Years of experience

Game Details

Total Score
3.1

Scenarios Completed
0/3

Times Played
3

Company Rank
1

[Assign Scenarios](#)

Enabled Scenarios
Show 10 entries

Search:

Scenario	Completion Status	Times Played	Top Score	Avg Playing Time	Total Time Played	
Smart Shipping 1 - Vishing	87	3	9.3	18	55	View Scenario
Smart Shipping 2 - Phishing email	0	0	0.0	0	0	View Scenario
Smart Shipping 3 - GPS spoofing	0	0	0.0	0	0	View Scenario

Showing 1 to 3 of 3 entries

Previous 1 Next

Figure 10 – Trainee Details

By clicking the button [Assign Scenarios](#) in any Trainee's Detail screen, the admin can enable a new scenario for the trainee and assign him/her a scenario specific role. For the scenarios already enabled for the trainee there is an enable/disable option (Figure 11 – Assigned Scenarios) as well as an option to change the trainee's scenario role (Figure 12 – Edit Scenario Role).

Trainee: Eleni Liarou

Assigned Scenarios
Show 10 entries

Search:

Scenario	User Role	Status	
Smart Shipping 1 - Vishing	Crew / Offshore officers	Disable	Edit Role
Smart Shipping 2 - Phishing email	Captain	Disable	Edit Role
Smart Shipping 3 - GPS spoofing	Captain	Disable	Edit Role

Showing 1 to 3 of 3 entries

Previous 1 Next

Available Scenarios

☒ Smart Shipping 4 - Digital forensics

[Assign](#)

Select

Captain

Crew / Offshore officers

IT Administrators of the shipping company

Figure 11 – Assigned Scenarios

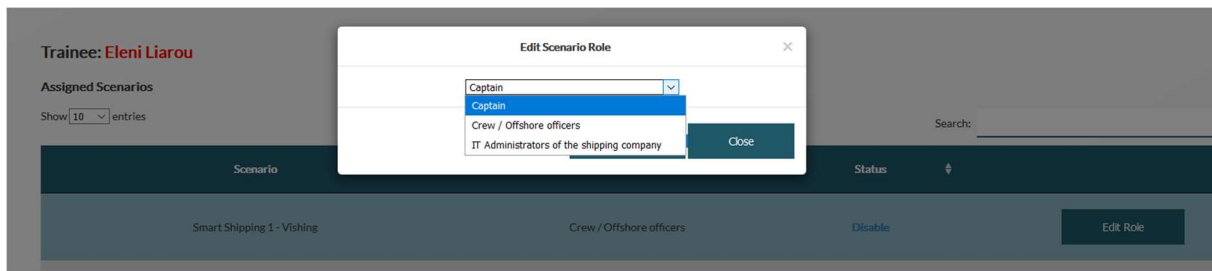


Figure 12 – Edit Scenario Role

4.3.3 Scenarios View (Admin)

The Scenarios View contains all available scenarios together with the Assessment Results, how many times each scenario has been executed, the Average Score, the Difficulty Level and the Number of Trainees that have already played a specific scenario (Figure 13 – Overview of Scenarios).

Scenario	Assessment results	Times Executed	Average Score	Difficulty Level	Numbers of trainees played	
Healthcare 1 - Incident Response	81%	3	6.03	2	1	View Scenario Details
Healthcare 2 - Social Engineering	48%	2	9.8	5	1	View Scenario Details
Healthcare 3 - Secure Configuration	0%	0	0	3	0	View Scenario Details
Healthcare 4 - Procedures	0%	0	0	4	0	View Scenario Details
Smart Home & IOT 1 - Secure Configuration	0%	0	0	6	0	View Scenario Details
Smart Home & IOT 2 - Bad Actor - Cloned Gateway	0%	0	0	4	0	View Scenario Details
Smart Home & IOT 3 - Compromised Devices - Botnet	0%	0	0	2	0	View Scenario Details
Smart Home & IOT 4 - Attacks on the Backend System	0%	0	0	1	0	View Scenario Details
Smart Shipping 1 - Vishing	55%	6	5.98	1	2	View Scenario Details
Smart Shipping 2 - Phishing email	60%	2	6.97	2	1	View Scenario Details

Figure 13 – Overview of Scenarios

By scrolling down there are two graphs that illustrate the Times of Execution of each scenario and the Number of Trainees that have already played the specific scenario (Figure 14 – Scenarios Global Graphs).

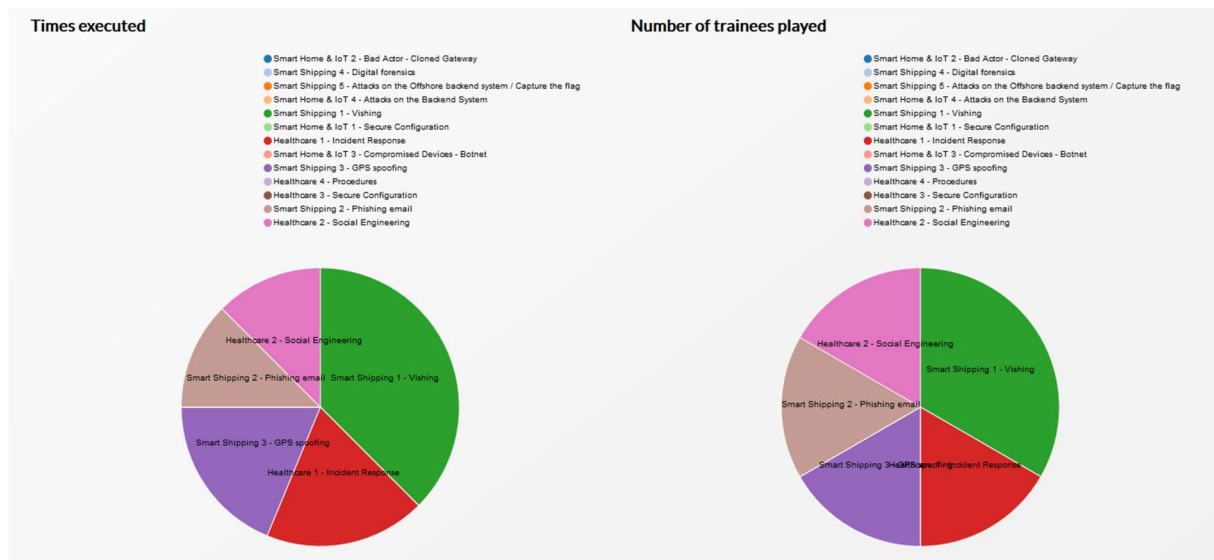
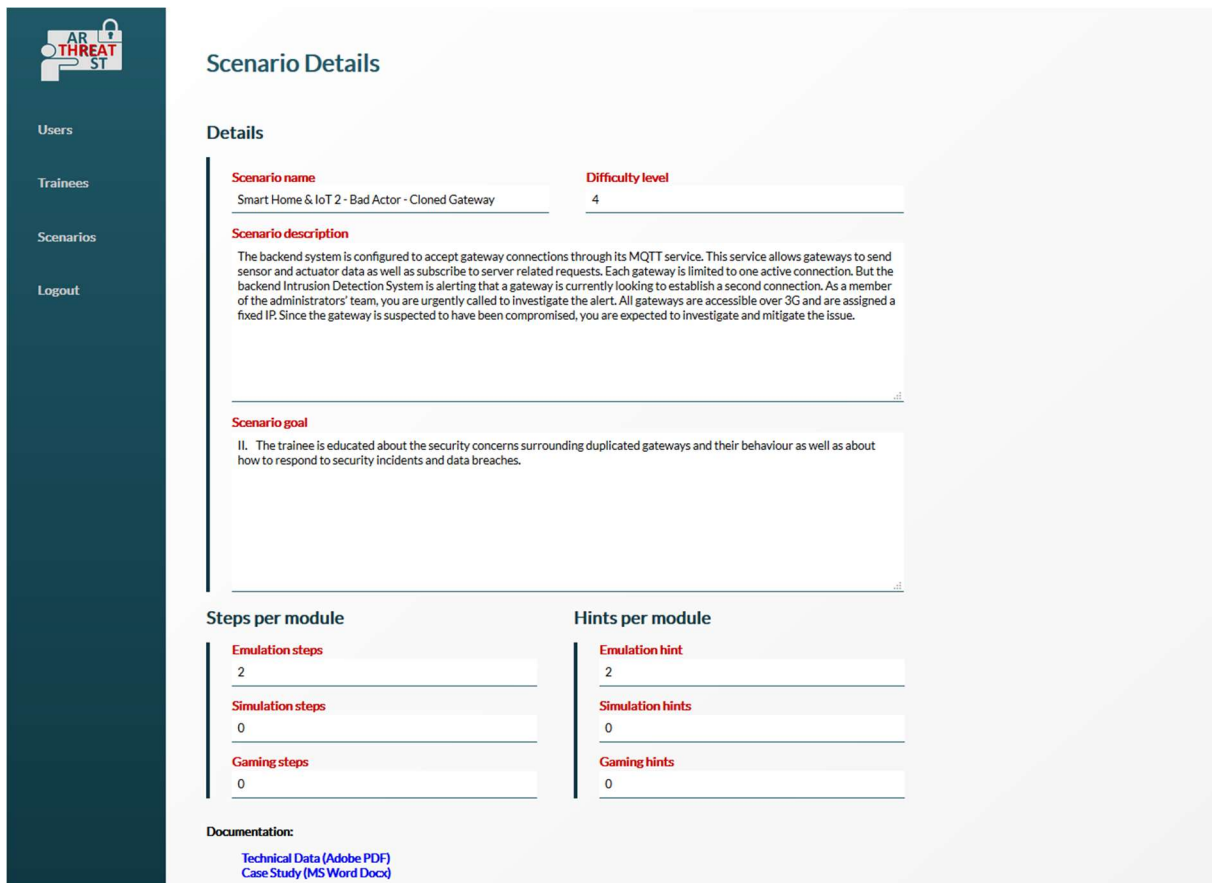


Figure 14 – Scenarios Global Graphs

On the screen Overview of Scenarios, by clicking the button [View Scenario Details](#), a new screen appears giving in detail several useful information about the relevant Scenario (Figure 15 – Scenario Details).

Specifically, it includes the following information of a Scenario:

- Scenario Name
- Difficulty Level
- Scenario Description
- Scenario Goal
- Steps per Tool/Module
- Max hints per Tool/Module
- Documentation Links



Scenario Details

Details

Scenario name
Smart Home & IoT 2 - Bad Actor - Cloned Gateway

Difficulty level
4

Scenario description
The backend system is configured to accept gateway connections through its MQTT service. This service allows gateways to send sensor and actuator data as well as subscribe to server related requests. Each gateway is limited to one active connection. But the backend Intrusion Detection System is alerting that a gateway is currently looking to establish a second connection. As a member of the administrators' team, you are urgently called to investigate the alert. All gateways are accessible over 3G and are assigned a fixed IP. Since the gateway is suspected to have been compromised, you are expected to investigate and mitigate the issue.

Scenario goal
II. The trainee is educated about the security concerns surrounding duplicated gateways and their behaviour as well as about how to respond to security incidents and data breaches.

Steps per module

Emulation steps
2

Simulation steps
0

Gaming steps
0

Hints per module

Emulation hint
2

Simulation hints
0

Gaming hints
0

Documentation:
[Technical Data \(Adobe PDF\)](#)
[Case Study \(MS Word Docx\)](#)

Figure 15 – Scenario Details

By scrolling down there are two graphs that illustrate the Times of Execution of the scenario and the Average Score (Figure 16 – Scenario Graphs), calculated based on the analysis described in Section 4.

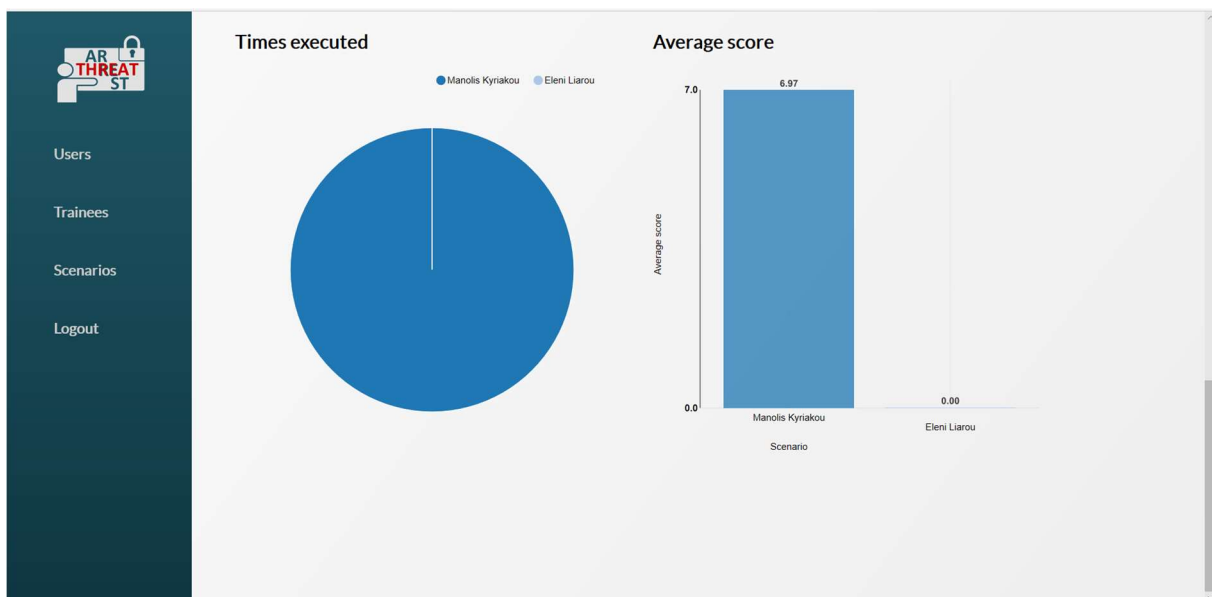


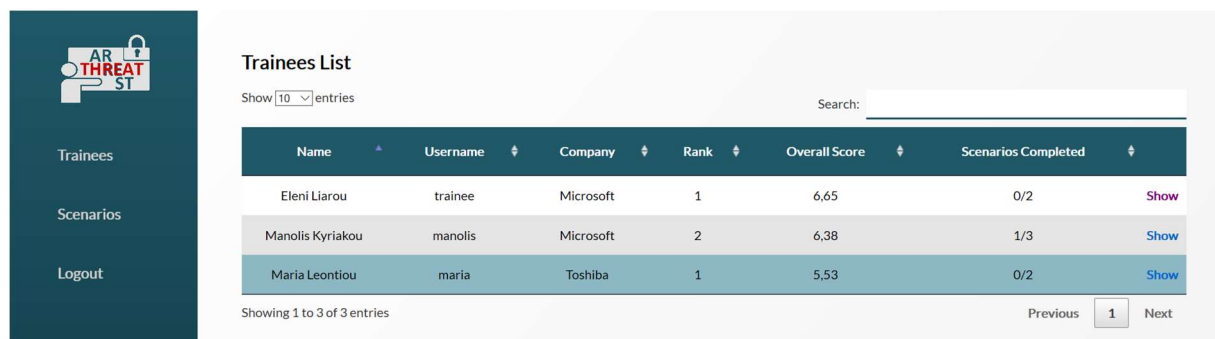
Figure 16 – Scenario Graphs

4.4 Trainer Perspective

The trainer perspective provides the same views and information available to the admin, but filtered to portray only the information related to trainees belonging to the same sector.

4.4.1 Trainee View (Trainer)

A trainer, after successfully logs in to the platform, is presented with the list of trainees accompanied with Names, Usernames, Companies, Rank, Overall Scores and Scenarios Completed (Figure 17 – Trainees List).



Name	Username	Company	Rank	Overall Score	Scenarios Completed	
Eleni Liarou	trainee	Microsoft	1	6,65	0/2	Show
Manolis Kyriakou	manolis	Microsoft	2	6,38	1/3	Show
Maria Leontiou	maria	Toshiba	1	5,53	0/2	Show

Showing 1 to 3 of 3 entries

Figure 17 – Trainees List

At the bottom of the same screen there are two graphs that depict the statistics of Total played Time and Overall Score (Figure 18 – Trainees General Statistics).

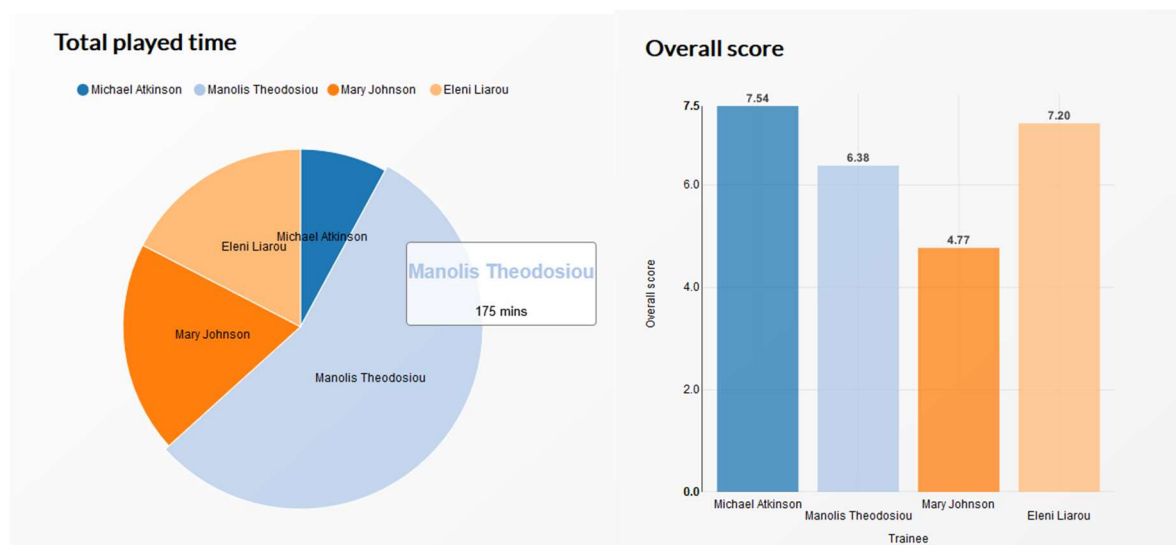
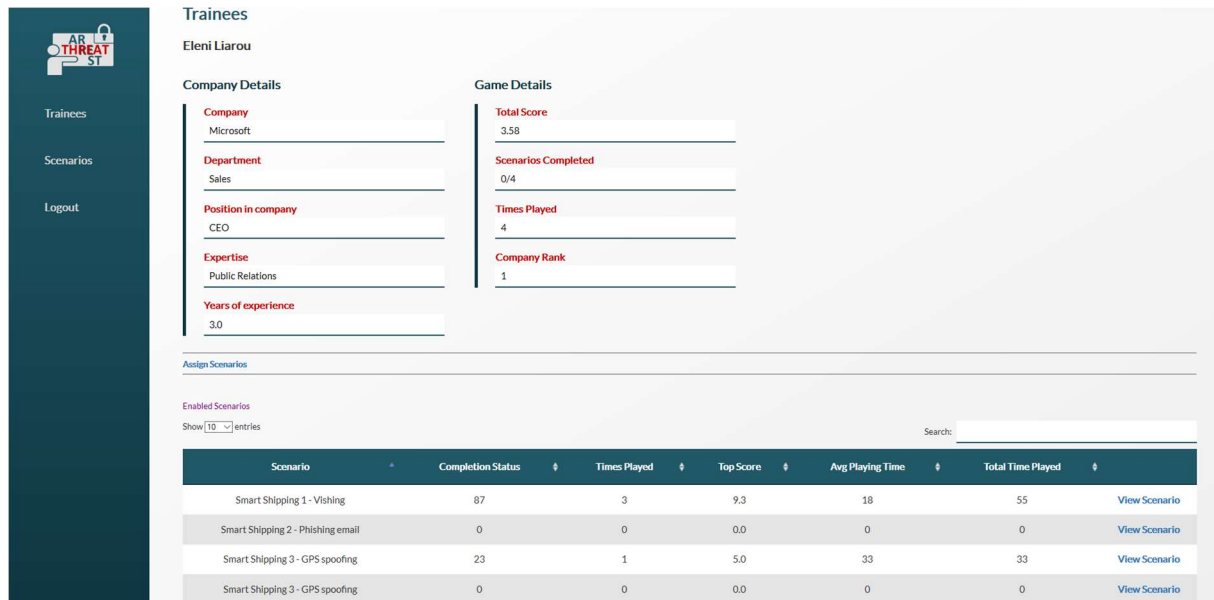


Figure 18 – Trainees General Statistics

By clicking the [Show](#) button on any Trainee, the Company details and Game details of the specific trainee are presented as well as the scenarios that he/she can participate (Figure 19 – Trainee Details).



Trainees
Eleni Liarou

Company Details

- Company: Microsoft
- Department: Sales
- Position in company: CEO
- Expertise: Public Relations
- Years of experience: 3.0

Game Details

- Total Score: 3.58
- Scenarios Completed: 0/4
- Times Played: 4
- Company Rank: 1

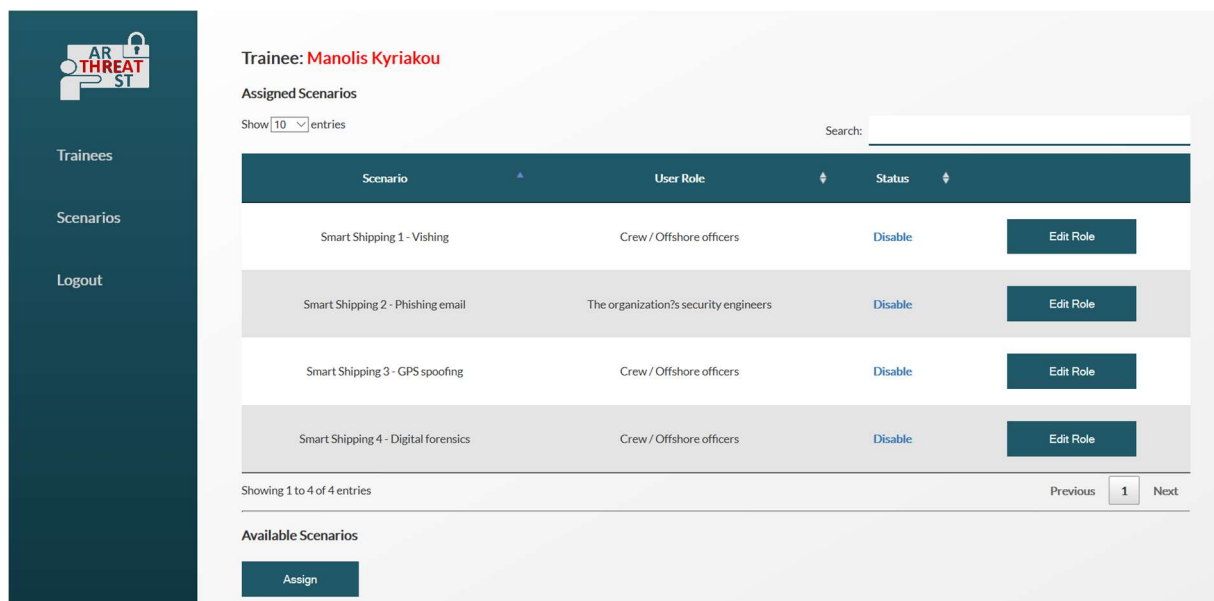
Assign Scenarios

Enabled Scenarios
Show 10 entries

Scenario	Completion Status	Times Played	Top Score	Avg Playing Time	Total Time Played	
Smart Shipping 1 - Vishing	87	3	9.3	18	55	View Scenario
Smart Shipping 2 - Phishing email	0	0	0.0	0	0	View Scenario
Smart Shipping 3 - GPS spoofing	23	1	5.0	33	33	View Scenario
Smart Shipping 3 - GPS spoofing	0	0	0.0	0	0	View Scenario

Figure 19 – Trainee Details

By clicking the button [Assign Scenarios](#) in any Trainee's Detail screen, the admin can enable a new scenario for the trainee and assign him/her a scenario specific role. For the already enabled trainee's scenarios there is an enable/disable option (Figure 20 – Assigned Scenarios) as well as an option to change the trainee's scenario role (Figure 21 – Edit Scenario Role).



Trainee: Manolis Kyriakou

Assigned Scenarios
Show 10 entries

Scenario	User Role	Status	
Smart Shipping 1 - Vishing	Crew / Offshore officers	Disable	Edit Role
Smart Shipping 2 - Phishing email	The organization's security engineers	Disable	Edit Role
Smart Shipping 3 - GPS spoofing	Crew / Offshore officers	Disable	Edit Role
Smart Shipping 4 - Digital forensics	Crew / Offshore officers	Disable	Edit Role

Showing 1 to 4 of 4 entries

Previous **1** Next

Available Scenarios
[Assign](#)

Figure 20 – Assigned Scenarios

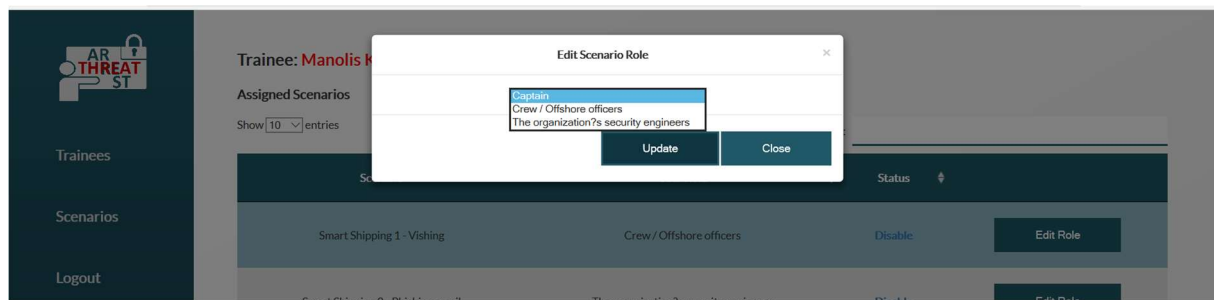


Figure 21 – Edit Scenario Role

4.4.2 Scenario View (Trainer)

By clicking the Scenario Button on the main screen, a new screen appears which shows the scenarios that are available for the specific trainer, the Assessment Results, how many times each scenario has been executed, the Average Score, the Difficulty Level and the Number of Trainees that have already played the specific scenario.

Moreover, two pie charts represent how many times each scenario has been executed and the number of trainees that have already played the specific scenario (Figure 22 – Overview of Scenarios for Trainer).

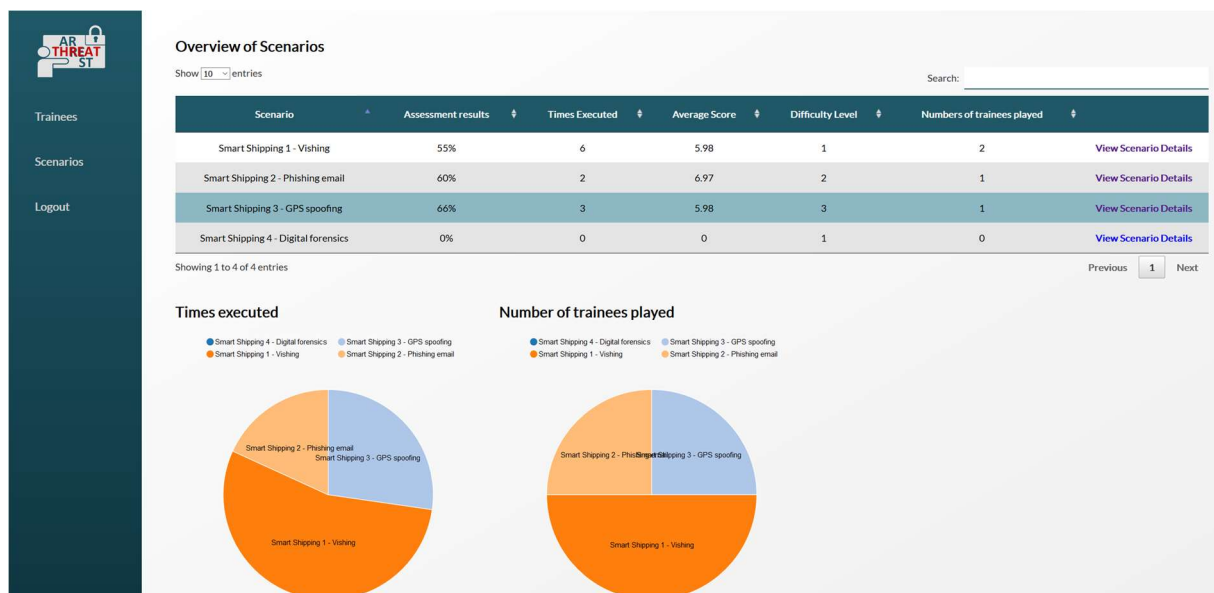


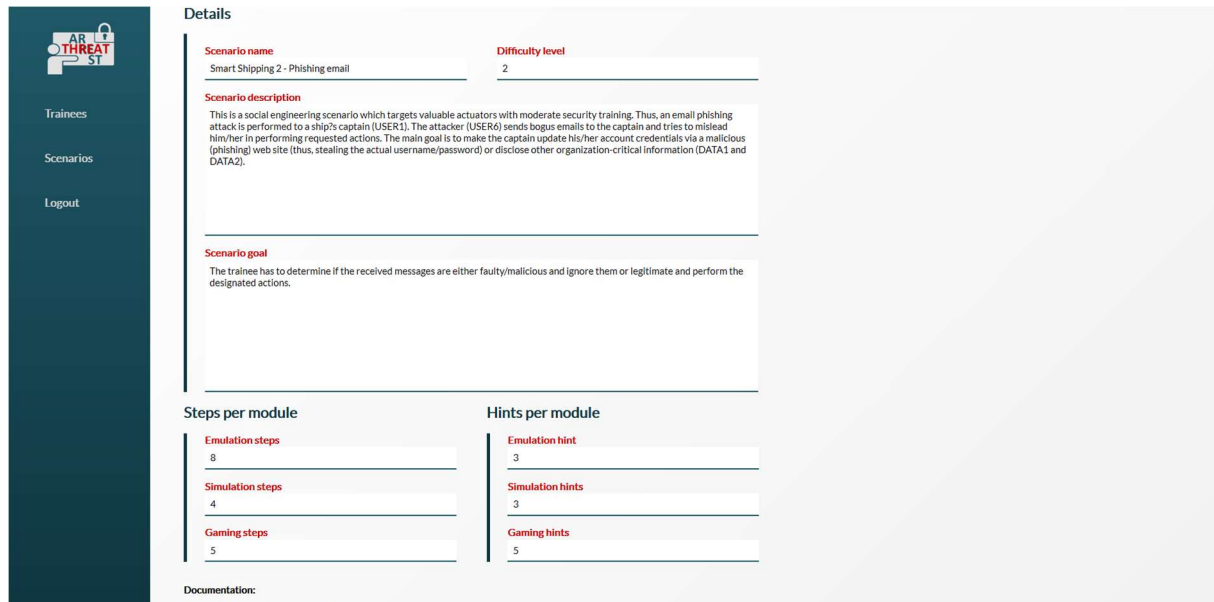
Figure 22 – Overview of Scenarios for Trainer

On the Overview of Scenarios screen, by clicking the button [View Scenario Details](#), a new screen that details several useful information about the relevant Scenario is included (Figure 23 – Scenario Details).

Specifically, it includes the following information of a Scenario:

- Scenario Name
- Difficulty Level
- Scenario Description

- Scenario Goal
- Steps per Tool/Module
- Max hints per Tool/Module
- Documentation Links



The screenshot displays the 'Details' section of a scenario in the THREAT-ARREST system. On the left is a dark sidebar with navigation links: 'Trainees', 'Scenarios', and 'Logout'. The main content area is titled 'Details' and contains the following information:

- Scenario name:** Smart Shipping 2 - Phishing email
- Difficulty level:** 2
- Scenario description:** This is a social engineering scenario which targets valuable actuators with moderate security training. Thus, an email phishing attack is performed to a ship's captain (USER1). The attacker (USER6) sends bogus emails to the captain and tries to mislead him/her in performing requested actions. The main goal is to make the captain update his/her account credentials via a malicious (phishing) web site (thus, stealing the actual username/password) or disclose other organization-critical information (DATA1 and DATA2).
- Scenario goal:** The trainee has to determine if the received messages are either faulty/malicious and ignore them or legitimate and perform the designated actions.
- Steps per module:**
 - Emulation steps: 8
 - Simulation steps: 4
 - Gaming steps: 5
- Hints per module:**
 - Emulation hint: 3
 - Simulation hints: 3
 - Gaming hints: 5
- Documentation:** (link area)

Figure 23 – Scenario Details

By scrolling down there are two graphs that illustrate the Times of Execution of the scenario and the Average Score (Figure 24 – Scenario Graphs).

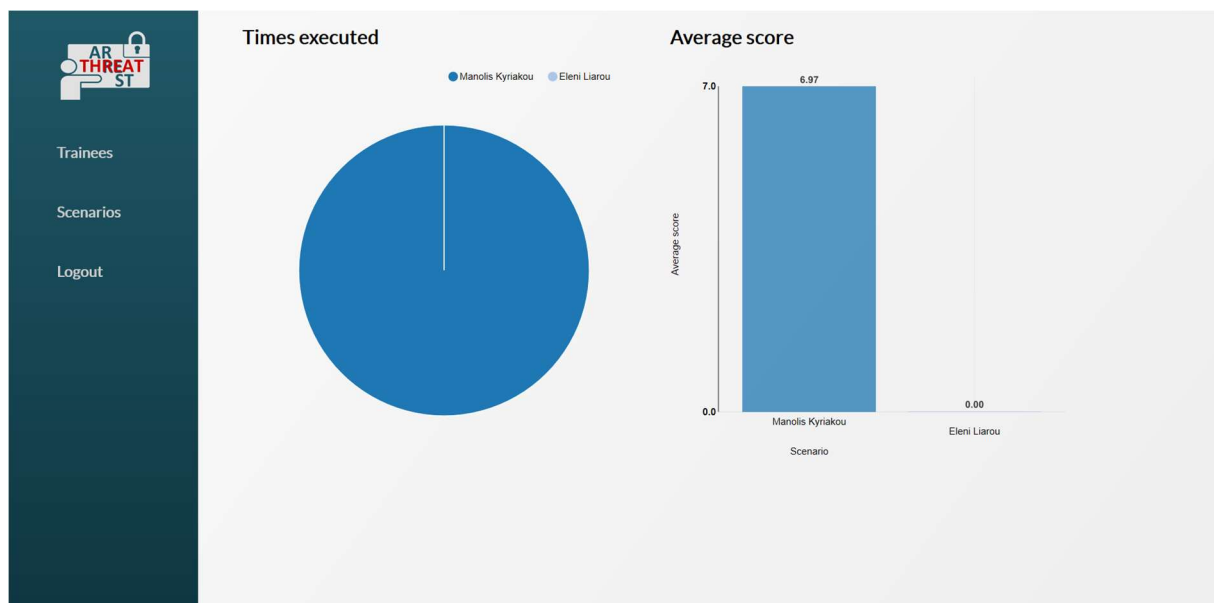


Figure 24 – Scenario Graphs

4.5 Trainee Perspective

The trainee perspective provides the trainee profile, the statistics of the trainee and the details of the scenario one wishes to utilise.

4.5.1 Profile (Trainee)

A trainee after successfully logs in to the platform, is presented with her/his Profile (Figure 25 – Trainee Profile).

Specifically, it includes the following information:

- Company Details
- Game Details
- Available Scenarios
- Completion Status
- Times Played
- Top Score
- Average Playing Time
- Total Time Played

Eleni Liarou

Company Details

Company
Microsoft

Department
Human Resources

Position in company
Head of HR

Expertise

Years of experience

Game Details

Total Score
3.93

Scenarios Completed
0/3

Times Played
5

Company Rank
1

Show entries Search:

Scenario	Completion Status	Times Played	Top Score	Avg Playing Time	Total Time Played	
Smart Shipping 1 - Vishing	87	4	9.3	19	77	View Scenario
Smart Shipping 2 - Phishing email	0	0	0.0	0	0	View Scenario
Smart Shipping 3 - GPS spoofing	43	1	2.5	7	7	View Scenario

Showing 1 to 3 of 3 entries Previous **1** Next

Figure 25 – Trainee Profile

By scrolling down there is a graphical representation of the Completion Status and Average Playing Time per scenario (Figure 26 – Statistics of Trainee).



Figure 26 – Statistics of Trainee

By clicking [View Scenario](#) on the Trainee Profile screen, a new screen appears with the Scenario Details (Figure 27 – Scenario Details).

More specifically, it includes the following information:

- Scenario Name
- Difficulty Level
- Scenario Description
- Scenario Goal
- Steps Per Module
- Hints Per Module
- Documentation Hints

THREAT-ARREST

Profile
Logout

Scenario Details

[Play Now](#)

Details

Scenario name	Difficulty level
Smart Shipping 1 - Vishing	1

Scenario description

This is a social engineering scenario for non-security experts. A vishing attack is performed to the ship's crew (USER2) or the offshore officers (USER3). The attacker makes phone calls and tries to disclose confidential or business critical information for the shipping company.

Scenario goal

The trainees answer questionnaires and try to choose the proper action that must be performed.

Steps per module	Hints per module
Emulation steps	Emulation hint
4	2
Simulation steps	Simulation hints
1	5
Gaming steps	Gaming hints
2	6

Documentation:

[Case Study \(MS Word Doc\)](#)

Figure 27 – Scenario Details

Finally, by clicking the **Play Now** button, the trainee can proceed further to play the specific scenario.

5 Conclusions

This deliverable is a report of the first version of the THREAT-ARREST real time assessment monitoring framework, that has been developed within a wider concept of the THREAT-ARREST training tool aiming to facilitate the access of the end users (trainers, trainees, administrators) in the THREAT-ARREST training modules and the efficient assessment and monitoring of the results of the training sessions.

The “THREAT-ARREST Training Tool” according to the refined THREAT-ARREST architecture is one of the core modules in the THREAT-ARREST platform and acts as the entry point for all TA users in order for them to use the provided features and functionalities of the platform. Its main goal is to provide real time assessment of the trainees’ performance while they engage with the available training scenarios. In order to facilitate this, the TT described in this document offers all required services that mainly consist of (i) Main Authentication Server for the TA Platform; (ii) Association of trainers and trainees with their sector and respective CTPP scenarios; (iii) Retrieval of the CTPP models and sub models from the CTPP DB and instantiation of the relevant TA modules; and (iv) Real time overview of the trainees’ progress while they engage in the individual modules (TT / GT / ET / ST).

Due to the fact that the relevant TA participating modules and the finalized definition of their integration in the TA platform was not fully finalized at the time of the development of this initial version of the TT, a number of proactive assumptions and steps were made to enable the demonstration of the overall TT’s functionalities. In this framework, and with respect to the trainees’ scoring and assessment, it is noted as a next step that in the final version of the tool the individual components (e.g. the GT) will be returning to the T.T. the actual trace rather than a pre-calculated score.

This deliverable forms the basis towards the 1st integrated version of the envisioned THREAT-ARREST training platform, defined as the milestone “MS4 – 1st version of Integrated training platform”. It will be used as a basis for the finalization and integration of all THREAT-ARREST modules afterwards. The next iteration of the task “T4.3 – Real time trainee performance assessment” is due at M28 and the deliverable “D4.6 – Real time trainee performance assessment v2”.

References

- [1] Fysarakis, K., et al., 2014. Embedded systems security challenges. Measurable security for Embedded Computing and Communication Systems (MeSeCCS 2014), within the 4th International Conference on Pervasive and Embedded Computing and Communication Systems (PECCS 2014), 7-9 January 2014, Lisbon, Portugal, pp. 1-10.
- [2] Fysarakis, K., et al., 2015. RT-SPDM: real-time security, privacy and dependability management of heterogeneous systems. Human Aspects of Information Security, Privacy and Trust (HCI International 2015), 2-7 August 2015, Los Angeles, CA, USA, Springer, LNCS, vol. 9190, pp. 619-630.
- [3] Hatzivasilis, G., et al., 2019a. Review of Security and Privacy for the Internet of Medical Things (IoMT). 1st International Workshop on Smart Circular Economy (SmaCE), Santorini Island, Greece, 30 May 2019, IEEE, pp. 1-8.
- [4] Hatzivasilis, G., et al., 2019b. WARDOG: Awareness detection watchdog for Botnet infection on the host device. IEEE Transactions on Sustainable Computing – Special Issue on Sustainable Information and Forensic Computing, IEEE, vol. 4, pp. 1-15.
- [5] Hatzivasilis, G., et al., 2019c. MobileTrust: Secure Knowledge Integration in VANETs. ACM Transactions on Cyber-Physical Systems – Special Issue on User-Centric Security and Safety for Cyber-Physical Systems, ACM, vol. 4, issue 3, Article no. 33, pp. 1-15.
- [6] Hatzivasilis, G., et al., 2017. SCOTRES: Secure Routing for IoT and CPS. IEEE Internet of Things Journal (IoT), IEEE, vol. 4, issue 6, pp. 2129-2141.
- [7] Manifavas, C., et al., 2014. DSAPE – Dynamic Security Awareness Program Evaluation. Human Aspects of Information Security, Privacy and Trust (HCI International 2014), 22-27 June, 2014, Creta Maris, Heraklion, Crete, Greece, Springer, LNCS, vol. 8533, pp. 258-269.

Appendix I

This appendix details the *expected trace* element of the CTTTP model that drives the automated evaluation of the trainee for the Virtual Labs with emulated and/or simulated components. The code follows the JSON format.

The next piece of code describes the instantiation of the **Evaluation Report** that is presented in the subsection 2.1.3.1, where health records were disclosed from the compromise ‘User-2’ account.

```
[{"Evaluation report": [
  "question set": [
    [ "number": "1",
      "description": "Was there any attack performed",
      "type": "radio",
      "answers": ["Yes", "No"],
      "correct option": ["Yes"],
      "successScore": 2.5,
      "hint": "The logs must be carefully examined!",
      "hintImpact": 0.5],
    [ "number": "2",
      "description": "Which was the attack",
      "type": "custom-select",
      "answers": [ ["0", "Denial of service"], ["1", "Disclosure of health records"], ["2", "Ransomware"], ["3", "Crypto-miner"], ["4", "Botnization"] ],
      "correct option": ["1", "Disclosure of health records"],
      "successScore": 2.5,
      "hint": "Check the examined logs for the nature of the attack",
      "hintImpact": 0.5],
    [ "number": "3",
      "description": "Was there any compromised user account",
      "type": "text",
      "answers": ["If yes, input compromised user account here"],
      "correct option": ["User-2"],
      "successScore": 2.5,
      "hint": "The logs must be carefully examined!",
      "hintImpact": 0.5],
    [ "number": "4",
      "description": "Which was the mitigation actions that you performed",
      "type": "checkbox",
      "answers": ["None", "Anti-virus update", "Anti-virus scan", "Restore system from a previous unaffected time-point", "Suspend compromised user's access", "Inform compromised user"],
      "correct option": ["Suspend compromised user's access", "Inform compromised user"],
      "successScore": 2.5,
      "hint": "Check the user's ID inside the log file ",
      "hintImpact": 0.5]
  ]
}]
```

The next piece of code describes the evaluation of the trainee based on **Event Captors** that are presented in the subsection 2.1.3.2.

```
[{"expected-trace": [
  [ "valueName": "scenario1.ShipMain.Destination=Piraeus",
    "successScore": 5],
  [ "valueName": "scenario1.ShipMain.Deck.GPS.suspendOperation",
    "successScore": 5]
]
```

For a successful training session, the TT will eventually receive two messages from the ST and the deployed event captors that the trainee performed these actions.

```
#Message 1
{
  "simTime":1500,
  "simTimeAbs":"2020-01-28T20:00:39.638Z",
  "wallTime":1564432617032,
  "valueName":"scenario1.ShipMain.Destination=Piraeus"
}

#Message 2
{
  "simTime":3500,
  "simTimeAbs":"2020-01-28T20:00:42.748Z",
  "wallTime":1564432883901,
  "valueName":"scenario1.ShipMain.Deck.GPS.suspendOperation"
}
```

This communication process between the TT and ST is further detailed in the deliverable “D5.4 – Simulated components network execution module v1”.

The next piece of code describes the evaluation of the trainee based on ***Simulated Attacks*** that are presented in the subsection 2.1.3.3. There, we instantiate a Virtual Lab where the Smart-Plug-2” and the ‘Device-3’ have been compromised. Thus, the trainee must restore their operation.

```
[ "expected-trace":[
  ["valueName":"scenario2.SmartHome.SmartPlug_2.restore",
  "score":5],
  ["valueName":"scenario2.SmartHome.SmartPlug_3.SmartDevice_3.restore",
  "score":5]
]]
```

For a successful training session, the TT will eventually receive two messages from the ST denoting that the trainee performed the correct actions and blocked the simulated attacks.

```
#Message 1
{
  "simTime":1500,
  "simTimeAbs":"2020-01-28T20:00:39.638Z",
  "wallTime":1564432617032,
  "valueName":"scenario2.SmartHome.SmartPlug_2.restore"
}

#Message 2
{
  "simTime":3500,
  "simTimeAbs":"2020-01-28T20:00:42.748Z",
  "wallTime":1564432883901,
  "valueName":"scenario2.SmartHome.SmartPlug_3.SmartDevice_3.restore"
}
```

This communication process between the TT and ST is similar as with the case of the Event Captors.

Appendix II

This appendix references a list of trainee evaluation methods that will be also considered for the final version of the real time trainee assessment procedures of THREAT-ARREST.

Table 1. Trainee performance references

Author	Subject – Topic	Resource details	Year
(ISC) ²	Computerized Adaptive Testing (CAT) for CISSP	https://www.isc2.org/Certifications/CISSP/CIS-SP-CAT	2020
Agne Brilingait, Linas Bukauskas, Aušrius Juozapavicius	A framework for competence development and assessment in hybrid cybersecurity exercises	Elsevier / Computers & Security 88	2020
Bilal Khan, Khaled S. Alghathbar, Syed Irfan Nabi and Muhammad Khurram Khan	Effectiveness of information security awareness methods based on psychological theories	African Journal of Business Management Vol. 5(26), pp. 10862-10868, 28 October, 2011	2011
Demitrius Fenton, Terry Traylor, Guy Hokanson & Jeremy Straub	Integrating Cyber Range Technologies and Certification Programs to Improve Cybersecurity Training Programs	Springer Nature Switzerland AG	2019
Erkan Kahraman	Evaluating IT security performance with quantifiable metrics	DSV SU/KTH Institutionen fur Data- och Systemvetenskap	2005
EU	Guidelines on Conformity Assessment – ISO / IEC 17024:2012	UNIDO	2013
GIAC	GIAC Proctor Program Overview	https://www.giac.org/exams/proctor	2020
H.A. Kruger, W.D. Kearney	A prototype for assessing information security awareness	Elsevier Science Direct Journal	2006
Irina Tal, Eva Ibarrola, Gabriel-Miro Muntean	Quality and Standardization in Technology-Enhanced Learning (TEL)	ITU Kaleidoscope 2016 – ICTs for a Sustainable World	2016
ISO/IEC 27035-1:2016	Principles of incident management	ISO/IEC	2016
Kaleel Rahman, The University of Sydney, New South Wales, Australia	Learning from Your Business Lectures: Using Stepwise Regression to Understand Course Evaluation Data	The Journal of American Academy of Business, Cambridge / Vol. 9 - Num. 2	2006
Kenji Uesugi & Toshihiro Hirayama	A Cybersecurity KPI Model	JCIC	2019
Konstantinos Rantos (1), Konstantinos Fysarakis & Charalampos Manifavas (2)	How effective is your security awareness program? – An evaluation methodology	(1) Dept. of Industrial Informatics, Kavala Institute of Technology (2) Dept. of Applied Informatics & Multimedia, Technological Educational Institute of Crete	2011
Lambert, John	Defenders think in lists. Attackers think in graphs	Microsoft Docs	2015
Mauro Andreolini, Vincenzo Giuseppe, Colacino Michele, Colajanni & Mirco Marchetti	A Framework for the Evaluation of Trainee Performance in Cyber Range Exercises	Mobile Networks and Applications · December 2019	2019
Michael Adams, CEO, NuCrest, LLC	How to Measure the Effectiveness of	NIST	2019

Author	Subject – Topic	Resource details	Year
	Cybersecurity Training and Awareness Programs		
NIST SP 800-61 rev.2	Computer Security Incident Handling Guide	NIST	2012
NIST SP.800-16 Rev.1	A Role-Based Model for Federal Information Technology / Cybersecurity Training	NIST	2014
NIST SP.800-50	Building an Information Technology Security Awareness and Training Program	NIST	2003
NIST SP.800-55 Rev.1	Performance Measurement Guide for Information Security	NIST	2008
Razvan Beuran, Ken-ichi Chinen, Yasuo Tan, Yoichi Shinoda	Towards Effective Cybersecurity Education and Training	(Japan Advanced Institute of Science and Technology)	2017
SANS	Security Awareness Metrics	https://www.sans.org/security-awareness-training/blog/security-awareness-metrics	2020
Wagenstein, H. N	A capability maturity model for training & education	https://www.pmi.org/learning/library/capability-maturity-model-training-education-8102	2006