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

D6.2: Initial installation and usage guidelines for the THREAT-ARREST platform[†]

Abstract: This document reports on the installation procedures and guidelines for the usage of the THREAT-ARREST platform first version. It overviews the installation necessary to deploy an instance of a THREAT-ARREST platform and guidelines for using the platform's GUI. The guidelines primarily address trainees, trainers, and those responsible for the creation of CTTP models. The platform training capabilities have been developed and provided *as a service* to end user (pilot) organisations.

[†] *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.*

Contractual Date of Delivery	30/04/2020
Actual Date of Delivery	30/04/2020
Deliverable Security Class	Public
Editor	Hristo Koshutanski (ATOS)
Contributors	Fulvio Frati (UMIL), Torsten Hildebrandt (SIMPLAN), George Hatzivasilis (FORTH), K. Fysarakis, M. Smyrlis, S. Spanoudaki, G. Spanoudakis (STS), Oleg Blinder (IBM), Ludger Goeke, Alejandro Quintanar, Sebastian Pape (SEA), George Tsakirakis, George Bravos (ITML)
Quality Assurance	George Hatzivasilis (FORTH), Dirk Wortmann (SIMPLAN).

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. Dirk Wortmann (SIMPLAN).

Revisions

Version	Date	By	Overview
0.8	30/04/2020	Editor	Addressed PCC & PTC review comments
0.7	29/04/2020	Editor	Addressed reviewers' comments from the quality review process.
0.6	17/04/2020	Editor	ATOS contributed to Sections 1, 2, 3.1 and 5. It includes revision of partners contribution and alignment to overall presentation.
0.5	13/04/2020	SEA	SEA contributed to Sections 3.5 and 4.2.
0.4	06/04/2020	ITML, SIMPLAN	ITML contributed to Sections 3.6 and 4.1. SIMPLAN contributed to Section 3.3.
0.3	02/04/2020	IBM	IBM contributed to Sections 3.1, 3.4.2 and 3.8.
0.2	26/03/2020	UMIL, FORTH, STS	UMIL contributed to Section 3.4, FORTH contributed to Section 3.2, and STS contributed to Sections 3.7 and 4.3.
0.1	24/03/2020	Editor	First Draft including ToC

Executive Summary

This document is “D6.2 – Initial Installation and usage guidelines for the THREAT-ARREST platform” and reports the results of task “T6.4 – Documentation and Guidelines for the usage of the THREAT-ARREST platform”.

The document presents the installation procedures and guidelines for the usage of the first version of the THREAT-ARREST platform. The platform’s training capabilities have been developed and provided as a service to end user organisations (Platform as a service – PaaS). The document overviews the hardware and software requirements necessary for the operation of the platform followed by the installation procedures necessary to deploy an instance of the platform. End-user guidelines are focused on using the platform’s Dashboard which integrates the different components’ functionalities (simulation, emulation, gamification, CTTP model editor, evaluation reports) allowing trainees/trainers to navigate through the platform’s Dashboard.

The final version of the document is “D6.6 – Final Installation and usage guidelines for the THREAT-ARREST platform” due to M36 which corresponds to the final version of the platform.

Table of Contents

List of Abbreviations

AMQP Advanced Message Queuing Protocol

CTTP Cyber Threat and Training Preparation

DFP Data Fabrication Platform

DoA Description of Action

EMon Emulated Components Monitor

ET Emulation Tool

GT Gamification Tool

I/O Input/Output

IaaS Infrastructure as a Service

IAM Identity & Access Management

IT Information Technology

JSON JavaScript Object Notation (data-interchange format)

JWT JSON Web Token

MB Message Broker

PaaS Platform as a Service

REST Representational State Transfer (cf. RESTful Web services)

SQL Structured Query Language

ST Simulation Tool

STOMP Streaming Text Oriented Messaging Protocol

TT Training Tool

UFW Uncomplicated Firewall

VM Virtual Machine

VT Visualisation Tool

List of Figures

List of Tables

1 Introduction

This document reports on the documentation and guidelines for the usage of the THREAT-ARREST platform first version. Particularly, two main points are addressed in this version of the document: i) Overview of the installation procedures necessary to deploy an instance of a THREAT-ARREST platform; and ii) end-user guidelines for using the platform's Dashboard.

For the first version of the platform, the guidelines primarily address user groups of the platform owner/administrator, trainees, trainers, and those responsible for the creation of CTTP models. These are according to the available capabilities of the platform for its first version.

The training capabilities have been developed and provided under the *Platform as a service (PaaS)* concept to end user organisations. As such, the usage guidelines are focused on how trainees/trainers can use and navigate through the platform's Dashboard.

The THREAT-ARREST platform first version has been deployed on a bare metal server in the infrastructure of the cloud provider LeaseWeb (the Netherlands), and is accessible at https://threat-arrest.org. We refer to deliverable "D6.1 – Initial Prototype of Integrated THREAT-ARREST platform" for details on the architecture of the platform, the communications and message exchange mechanisms, and for credentials to access the current version of the platform for demonstration purposes.

The rest of the document is structured as follows. Section 2 presents the hardware and software requirements for THREAT-ARREST platform operation. Particularly, the hardware requirements may vary from one platform instance to another. It depends on the training needs in each domain in terms of the number of concurrent training sessions supported and the complexity of cyber system emulation/simulation. Section 3 overviews the installation guidelines of the platform covering OpenStack installation, VM and network setup to individual components' installation procedures and software dependencies. Section 4 details the GUI of the platform's Dashboard given its central role in orchestration and integration of the different platform capabilities such as simulation, emulation, gamification, CTTP model editor, and evaluation reports. The Dashboard gives different access functionalities to different types of users – trainees, trainers and training models creators. The usage guidelines illustrate in a cascade manner the different views offered to the different types of users. Finally, Section 5 concludes the document and outlines next steps.

2 THREAT-ARREST Hardware and Software Requirements

The hardware and software requirements of the platform have been defined with respect to the scalability needs of the project. Particularly, the scalability is defined for the number of training scenarios necessary to run simultaneously and the complexity of organisations' cyber systems to be emulated for the training purposes. We note that emulation of a cyber system is the most resource demanding capability of the platform for the purposes of hands-on training. The rest of the platform capabilities, such as simulation, gamification and data fabrication, are also well estimated for the project needs with respect to the upper bound set, but the impact of emulation is the most influential to the overall estimation of hardware resources.

As such, given the three pilots of the project, we have envisaged an ***upper bound*** of platform support for ***three training scenarios*** run simultaneously each requiring up to ***ten compute nodes*** where infrastructure and services of an organisation are emulated. Each such compute/storage node can host emulation of several organisation's services such as database service, web service, SMTP service, cloud or network applications, etc. to name a few. Each such compute node is estimated an average of 2 CPU cores, 4 GB RAM, and 30 GB HDD.

We note that for the case of simpler cyber system emulation/simulation, the platform may well support the simultaneous execution of much more scenarios before a degradation of performance can be observed.

Table 1 shows the hardware requirements for the deployment of THREAT-ARREST platform supporting the upper bound of three simultaneous training scenarios with the complex infrastructure that emulation/simulation needs. For each such scenario a column under each tool is shown to indicate the resources necessary for each scenario or one column in cases the resources are seen necessary for the three scenarios.

*Table 1: Hardware requirements for deployment of THREAT-ARREST platform supporting three simultaneous training scenarios**

HW Requirements	ET			ST			GT	TT	DFP	AT	EMon	Rem Access	MB	Total (virtual)	OpenStack physical HW requirements	Total (physical)
CPU cores @ 2.4 GHz	20	20	20	2	2	2	2	2	2	2	2	2	2	80	2	**22**
RAM (GB) DDR4	40	40	40	6	6	6	8	8	12	16	8	8	8	206	6	**178**
Storage (GB) SSD	300	300	300	60	60	60	60	60	50	60	60	60	50	1480	100	**1580**
Bandwidth (Mbps)	50	50	50	50	50	50	50	50	50	50	50	50	50	50	-	**50**

**The deployment refers to complex infrastructure emulation/simulation needs, using 4:1 vCPU to pCPU ratio and 1.2:1 vRAM to pRAM ratio.*

Given some best practices and suggestions[1,2], and the fact that cyber security training, although emulating and simulating cyber system services and processes, does not represent a real production system with real traffic and production activities, we have selected the following

[1] https://communities.vmware.com/servlet/JiveServlet/previewBody/21181-102-1-28328/vsphere-oversubscription-best-practices[1].pdf

[2] https://cloudarchitectmusings.com/2012/12/21/back-to-basics-general-vsphere-sizing/

ratio for CPU and RAM oversubscription to ensure higher compute and memory scalability – *4:1 vCPU to pCPU ratio* and *1.2:1 vRAM to pRAM ratio*.

Given that, the physical hardware resources necessary to deploy and operate the THREAT-ARREST platform, for the established upper bound of training scenarios, are 22 CPU cores, 178 GB RAM, and 1600 GB HDD. We note that the number of physical CPU cores can also be addressed by logical CPU cores given the underlying CPU supports the hyper-threading technology.

Table 2: Software requirements of THREAT-ARREST platform components

SW requirements	ET	ST	GT	TT	DFP	AT	RemAccess	EMon	MB
Software	**Ubuntu 18.0.4** LTS, Git Server, MySQL Server	**Ubuntu 18.0.4** LTS, Java 8, Git	**Ubuntu 18.0.4** TLS	**Ubuntu 18**, Laravel v6.0, PHP >= 7.2.0, MySQL, Git	**Ubuntu 16**, Apache Tomcat (7), Docker Container (18.06), Java (8), Git	**Ubuntu 18 LTS**, Java version 1.8 (Oracle), Python 3.7, MySQL Server (Latest), Git	**Ubuntu 18**, Java 1.8, Guacamole server latest version, Git	**Ubuntu 18**, Java 1.8, Tomcat (latest version)	**Ubuntu 18**, RabbitMQ latest version, Web STOMP plugin, STOMP plugin.
List of TCP ports used to provide services	**80, 8080** (HTTP), **22** (SSH), **9418** (Git Server), **3306** (MySQL Server)	**22** (SSH), **8080** (HTTP)	**80** (HTTP), **443** (HTTPS/TLS), **22** (SSH)	**80**, **8080** (HTTP), **443** (HTTPS/TLS), **22** (SSH)	**80** (HTTP), **22** (SSH)	**80** (HTTP), **8080** (Tomcat), **443** (HTTPS/TLS), **3306** (MySQL), **22** (SSH), **5672** (RabbitMQ)	**80, 8080** (HTTP), **4822** (Guacamole Server), **22** (SSH), **443** (HTTPS/TLS), **3389** (RDP), **5432** (PostgreSQL)	**80, 8080, 22**	**5672** (RabbitMQ server), **5671** (RabbitMQ over TLS/SSL) **15674** (RabbitMQ Web STOMP Service), **15673** (Web STOMP Service over TLS/SSL)

Table 2 shows the software requirements necessary for each component of the platform to operate. Additionally, it also lists the port numbers and services each component requires for its operation.

3 THREAT-ARREST Installation Guidelines

3.1 OpenStack Installation and Network Setup

OpenStack provides an Infrastructure-as-a-Service (IaaS) solution through a set of interrelated services. Each service offers an application programming interface (API) that facilitates this integration.

OpenStack services are composed of several processes. All services have at least one API process, which listens for API requests, pre-processes them and passes them on to other parts of the service.

For communication between the processes of one service, an Advanced Message Queuing Protocol (AMQP) message broker is used.

In our case the **OpenStack Queens** release was deployed on a single bare metal machine. The bare metal is installed with "Ubuntu 16.04”. We use All-In-One Single Machine installation. All the services and components run on the same node:

- **Controller** with Identity service (Keystone), Image service (Glance), Dashboard (Horizon). It also includes supporting services such as an SQL database, message queue (RabbitMQ).
- **Compute** which operates instances. Compute uses the KVM hypervisor.
- **Block Storage** (Cinder) contains the disks for instance provision. The service provisions logical volumes using the LVM driver.
- **Networking** Option 2: Self-service networks. The self-service networks option augments the provider networks option with layer-3 (routing) services that enable self-service networks using overlay segmentation methods. It routes virtual networks to physical networks using NAT.
- **Orchestration** (HEAT) is an engine to launch multiple composite cloud applications based on templates.

3.1.1 Network setup and Virtual machines

There is one public network called **provider** 5.79.110.0/27:

- The subnet is Start 5.79.110.13 - End 5.79.110.16.
- IP address 5.79.110.13 is in use by DHCP.
- IP address 5.79.110.14 is in use by Router.

A private network **private1** was defined. This is Class C network: Private1 – 10.10.1.0/24 – Start 10.10.1.2 – End 10.10.1.254.

Also, few additional private networks were created in the environment. A router **router1** was defined. This router currently has multiple network interfaces and one of them is located in public network with IP address of 5.79.110.14.

There are 3 public IP addresses which were allocated as floating IPs for 3 Virtual Machines (VMs) – RemAccess (Guacamole), ET (Emulation Tool+Git+DB) and MB (Message Broker). Each one of these VMs also has private IP address.

In addition, one VM was deployed per tool in private network. Each tool VM has been associated to a specific port on the RemAccess machine by definition of iptables rules.

All VMs which are in different private networks can access the Internet, can access each other, are able to access the 3 public machines described above, and can be accessed from these public machines as well.

There are 2 basic images based on different releases of Ubuntu and Windows. A few flavours were created which are an available hardware configuration for a server and define the compute, memory, and storage capacity of Nova computing instances.

Figure 1 illustrates the network view of the THREAT-ARREST platform. Each platform component is assigned a VM with the necessary hardware and software requirements presented in Section 2.

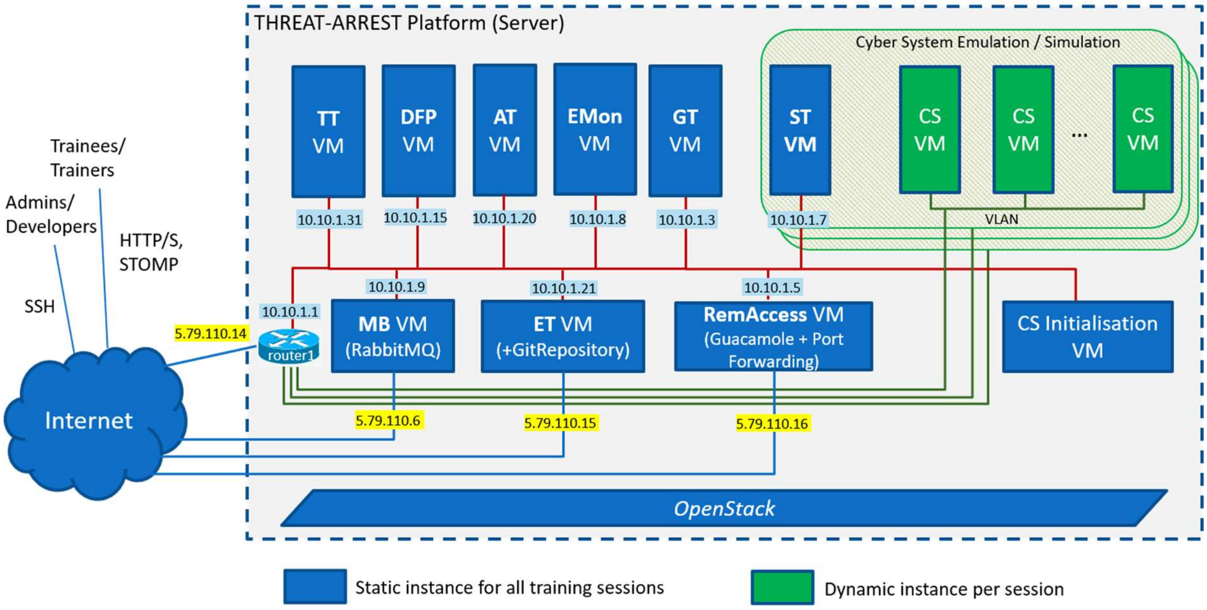


Figure 1: THREAT-ARREST Platform Network View

The yellow highlighted IP addresses are public IP addresses provided by the LeaseWeb provider. Table 3 shows the Tool VMs and the assigned local and public IP addresses.

Table 3: Tool VMs and IPv4 Addresses

Tool VM	Local IP Address	Public IP Address
TT VM	10.10.1.31	-
DFP VM	10.10.1.15	-
AT VM	10.10.1.20	-
EMon VM	10.10.1.8	-
GT VM	10.10.1.3	-
ST VM	10.10.1.7	-
MB VM	10.10.1.9	5.79.110.6
ET VM	10.10.1.21	5.79.110.15
RemAccess VM	10.10.1.5	5.79.110.16

The THREAT-ARREST platform is accessible through the RemAccess machine which serves as a gateway to the platform components and services. Port Forwarding is implemented on RemAccess (threat-arrest.org – 5.79.110.16) host. For instance, access to the THREAT-ARREST Training Tool Dashboard is at http://5.79.110.16 or https://5.79.110.16 will port forward to the Training Tool's VM at 10.10.1.31:80 or 10.10.1.31:443, respectively.

Table 4 shows the port forwarding setup in RemAccess machine for the first version of the platform.

Table 4: Port Forwarding to Platform's Components

RemAccess TCP Port	Local Tool VM and TCP Port
2022	GT port 22
2080	GT port 80
2443	GT port 443
3022	TT port 22
80	TT port 80
443	TT port 443
38080	TT port 8080
4022	DFP port 22
4080	DFP port 80
5022	AT port 22
5080	AT port 80
58080	AT port 8080
5443	AT port 443
53306	AT port 3306
5672	AT port 5672
6022	EMon port 22
6080	EMon port 80
6808	EMon port 8080
1022	ST port 22
18080	ST port 8080

The commands below should be executed with a root account or by a user having sudo permissions in the RemAccess machine.
To list the currently defined rules:

```
iptables-save
```

To create a new redirection rule, for instance for port 80 on 10.10.1.31 host:

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 10.10.1.31:80
```

To make the rule permanent and be activated after reboot:

```
iptables-save > /etc/iptables/rules.v4
```

3.2 Message Broker Installation and Setup (MB VM)

In this section, we will describe the installation of the broker that will facilitate the operation of the THREAT-ARREST platform components. We choose RabbitMQ[3] as the designated choice, as it is a widely-used broker solution and it is open source. Moreover, it supports several messaging protocols, like the Advanced Message Queuing Protocol (AMQP) and the Streaming Text Oriented Messaging Protocol (STOMP). RabbitMQ is written in the Erlang programming language and supports several client libraries and interfaces with the broker and all major programming languages, such as Java, C#, Python, and JavaScript. The initial deployment and usage of the broker is also described in the deliverable due at M12. Specifically, the communication with the Emulation Tool is presented in D2.4, the communication with the Training, Visualization, and Gamification Tools is detailed in D4.3, while the communication with the simulated components and the data fabrication platform is documented in D5.3.

Here, we will further present the installation details and provide an installation guide for the THREAT-ARREST platform operator. The broker is installed in an Ubuntu virtual machine (VM) and facilitates the internal operation within the OpenStack environment.

3.2.1 Broker VM Security

As a central communication point, we have also to take into consideration the security of this broker/server. First of all, we start by performing a series of *server hardening* policies which mainly include:

- update and upgrade the utilized packages and the operating system
- remove unnecessary packages
- detect weak passwords and update
- verify that no accounts have empty passwords
- set password rules
- disable USB devices
- secure any Apache server running in this machine
- examine which services start at boot time in order to verify that there are no malicious services starting with booting and running in the background
- delete all world-writable files
- configure *iptables* to block common attacks, like SYN flooding and spoofing
- install *Logwatch* to monitor suspicious log messages
- install and configure the Uncomplicated Firewall (UFW), which is the main solution for Ubuntu
- secure configuration of SSH
- disable telnet
- secure configuration of *sysctl* to prevent the main flooding attacks and IP spoofing
- lock user accounts after some failed login attempts
- use *netstat* and check for hidden open ports
- set root permissions for the core system files
- install *chkrootkit* and scan for rootkits
- install the open source antivirus ClamAV and scan for viruses

The text area below includes the main installation instructions for the security set up in the broker's VM.

```
#Update your package list and upgrade your OS
sudo apt-get update && apt-get upgrade

#Disable USB devices (for headless servers)
```

[3] www.rabbitmq.com/

```
/etc/modprobe.d/block_usb.conf
install usb-storage /bin/true

#Secure any Apache servers
/etc/apache2/apache2/conf
ServerTokens Prod
ServerSignature Off
Header always unset X-Powered-By
TraceEnable Off

#Install and configure UFW
apt-get install ufw
ufw enable

#Configure SSH securely
/etc/ssh/ssh_config
PermitRootLogin no # disallows root access via SSH
AllowUsers [username] # limits SSH access to the stated users
IgnoreRhosts yes # disallows SSH from trusting a host based only on its IP
HostbasedAuthentication no # as above
PermitEmptyPasswords no # prevents users from logging into SSH with an empty password, if
set as such
X11Forwarding no # stops the possibility of the server sending commands back to the client
MaxAuthTries 5 # drops the SSH connection after 5 failed authorization attempts
Ciphers aes128-ctr,aes192-ctr,aes256-ctr # disable weak ciphers
UsePAM yes # disables password authentication and defers authorization to the key-based PAM
ClientAliveInterval 900 # logs out idle users after 15 minutes
ClientAliveCountMax 0 # how many times the server checks whether the session is active
before dropping

#Disable telnet
apt-get remove telnet

#Configure sysctl securely
/etc/sysctl.conf
net.ipv4.ip_forward parameter 0 #Disable IP Forwarding by setting the net.ipv4.ip_forward
parameter to 0
net.ipv4.conf.all.send_redirects 0
net.ipv4.conf.default.send_redirects parameters 0 #Disable the Send Packet Redirects by
setting the net.ipv4.conf.all.send_redirects and net.ipv4.conf.default.send_redirects
parameters to 0
net.ipv4.conf.all.accept_redirects 0
net.ipv4.conf.default.accept_redirects parameters 0 #Disable ICMP Redirect Acceptance by
setting the net.ipv4.conf.all.accept_redirects and net.ipv4.conf.default.accept_redirects
parameters to 0
net.ipv4.icmp_ignore_bogus_error_responses parameter 1 #Enable Bad Error Message Protection
by setting the net.ipv4.icmp_ignore_bogus_error_responses parameter to 1

#Check for hidden open ports with netstat
netstat -antp

#Scan for rootkits
apt-get install chkrootkit
chkrootkit

#ClamAV
sudo apt-get install clamav
sudo freshclam
```

```
clamscan -r --bell -i /
```

3.2.2 RabbitMQ Installation

After the secure setting of the system, we will start the installation of the RabbitMQ broker and its web management console. The current version of the broker is *v. 3.6.10*. For message exchanges, most of the rest tools utilize a Java client for AMQP, which is supported by default from the broker. In order to enable the communication with the Jasima Visualization Tool that uses STOMP (see D4.3 and D5.3), we need to install two plugins: i) one for communication with STOMP[4] and ii) one for the communication with STOMP over a Websocket connection[5].

In order to enable the communication with this VM and the plugins, we have to activate the related networking ports via the UFW Firewall. Specifically, we utilize the ports:

- *15672* for the broker's web management console
- *5672* for the broker's message exchange using AMQP
- *61613* for the interaction with the STOMP plug-in
- *15674* for the interaction with the Web-STOMP plug-in

Moreover, we have to change the default passwords for the two pre-installed user accounts 'admin' and 'guest', and set strong ones. In the text area below, we detail the specific installation instructions for the deployment of the RabbitMQ message broker in the platform.

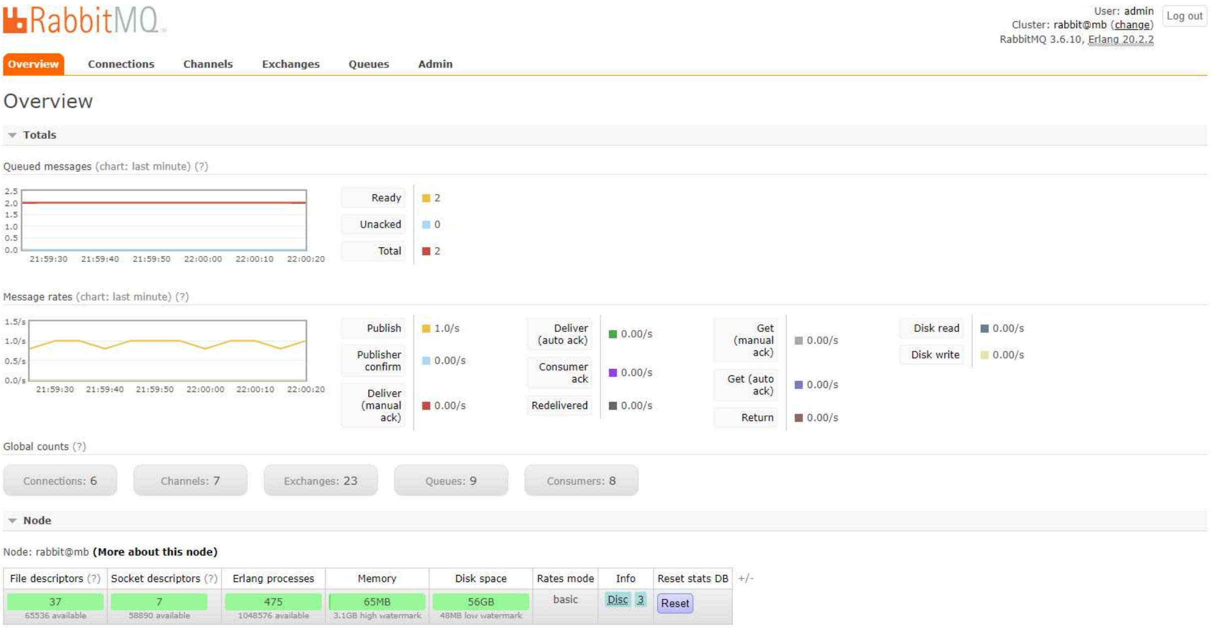
```
#Install and start the RabbitMQ broker
sudo apt install rabbitmq-server
sudo systemctl start rabbitmq-server
sudo systemctl enable rabbitmq-server
sudo systemctl status rabbitmq-server

#Change default passwords for the pre-installed users ‘admin’ and ‘guest’
rabbitmqctl add_user admin StrongPassword
rabbitmqctl set_user_tags admin administrator
rabbitmqctl list_user_permissions user

#rabbitmqctl change_password <USERNAME> <NEWPASSWORD>
rabbitmqctl change_password admin XGAqw12!!O
rabbitmqctl change_password guest k8b!PJ!E23

#Enable server and install the main plug-ins
systemctl is-enabled rabbitmq-server.service
       sudo systemctl enable rabbitmq-server #To enable if it is disabled
sudo rabbitmq-plugins enable rabbitmq_management
sudo rabbitmq-plugins enable rabbitmq_stomp
sudo rabbitmq-plugins enable rabbitmq_web_stomp

#Open the main communication ports
sudo ufw allow 15672
sudo ufw allow 5672
sudo ufw allow 61613
sudo ufw allow 15674

#Check the installation status
sudo ufw status
sudo netstat -tulpn
sudo netstat -ntlp | grep LISTEN
ss -tunelp | grep 15672
```

[4] www.rabbitmq.com/stomp.html

[5] www.rabbitmq.com/web-stomp.html

3.2.3 Exchanges and Queues Setup

Thereafter, the control panel is accessible via the URL http://5.79.110.6:15672/. From there, we can create the required users (with strong password authentication policies) and their exchanges. The next figure depicts the broker's overview, where one can see the active queues and message exchanges.



User: admin
Cluster: rabbit@mb (change)
RabbitMQ 3.6.10, Erlang 20.2.2

Overview

Totals

Queued messages (chart: last minute) (?)

Ready 2
Unacked 0
Total 2

Message rates (chart: last minute) (?)

Publish 1.0/s
Publisher confirm 0.00/s
Deliver (manual ack) 0.00/s
Deliver (auto ack) 0.00/s
Consumer ack 0.00/s
Redelivered 0.00/s
Get (manual ack) 0.00/s
Get (auto ack) 0.00/s
Return 0.00/s
Disk read 0.00/s
Disk write 0.00/s

Global counts (?)

Connections: 6
Channels: 7
Exchanges: 23
Queues: 9
Consumers: 8

Node

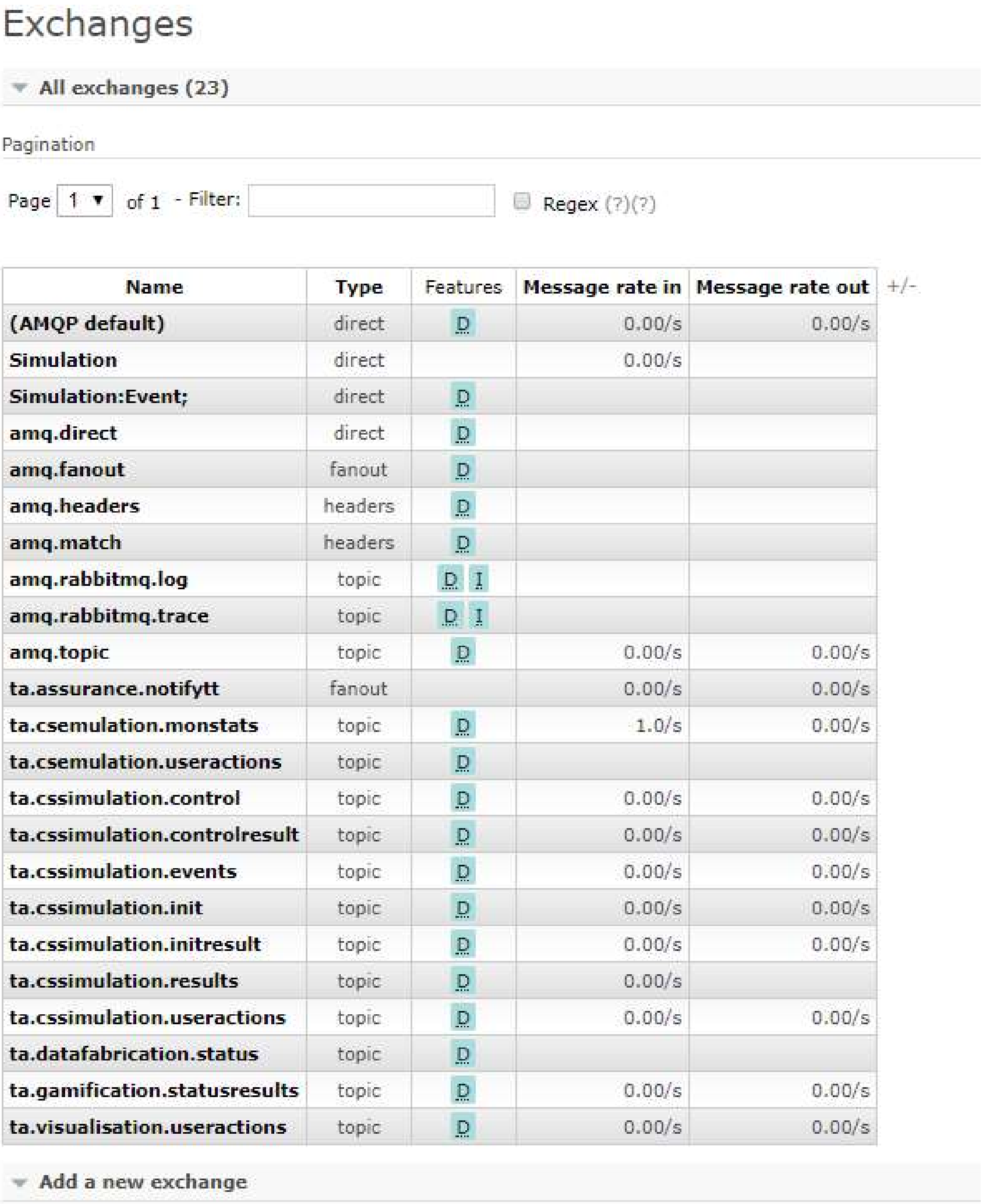
Node: rabbit@mb **(More about this node)**

File descriptors (?)	Socket descriptors (?)	Erlang processes	Memory	Disk space	Rates mode	Info	Reset stats DB
37 65536 available	7 58890 available	475 1048576 available	65MB 3.1GB high watermark	56GB 48MB low watermark	basic	Disc 3	Reset

+/-

Figure 2: RabbitMQ – Overview

Totally, we installed 23 *exchanges*, as they are depicted in the following figure.



Exchanges

All exchanges (23)

Pagination

Page 1 ▾ of 1 - Filter: □ Regex (?)(?)

Name	Type	Features	Message rate in	Message rate out
(AMQP default)	direct	D	0.00/s	0.00/s
Simulation	direct		0.00/s	
Simulation:Event;	direct	D		
amq.direct	direct	D		
amq.fanout	fanout	D		
amq.headers	headers	D		
amq.match	headers	D		
amq.rabbitmq.log	topic	D I		
amq.rabbitmq.trace	topic	D I		
amq.topic	topic	D	0.00/s	0.00/s
ta.assurance.notifytt	fanout		0.00/s	0.00/s
ta.csemulation.monstats	topic	D	1.0/s	0.00/s
ta.csemulation.useractions	topic	D		
ta.cssimulation.control	topic	D	0.00/s	0.00/s
ta.cssimulation.controlresult	topic	D	0.00/s	0.00/s
ta.cssimulation.events	topic	D	0.00/s	0.00/s
ta.cssimulation.init	topic	D	0.00/s	0.00/s
ta.cssimulation.initresult	topic	D	0.00/s	0.00/s
ta.cssimulation.results	topic	D	0.00/s	
ta.cssimulation.useractions	topic	D	0.00/s	0.00/s
ta.datafabrication.status	topic	D		
ta.gamification.statusresults	topic	D	0.00/s	0.00/s
ta.visualisation.useractions	topic	D	0.00/s	0.00/s

Figure 3: RabbitMQ – The deployed exchanges

3.3 Simulation Tool and Visualisation Tool Backend Installation (ST VM)

The Simulation Tool and Visualisation Tool backend developed by SIMPLAN are Java applications developed using Java 1.8. To deploy them in the THREAT-ARREST platform both will be packaged in a single jar file that will also contain all external Java libraries, including an embedded version of the Apache Tomcat application server required to run it. Creating this jar file is performed in a build step executed by the training developer. This build step is only necessary when major changes are required, e.g., to add a completely new type of simulated component.

The simulation is developed and tested primarily on a Windows 10 machine with a current version of Oracle's Java 1.8 JDK. The main execution environment is assumed to be a Linux machine with open-jdk 1.8 installed.

3.3.1 Server requirements:

- Ubuntu Server 18.04 with OpenJDK8 (apt package name **openjdk-8-jdk**) installed
- Server configured and security hardened as required by the execution environment following general guidelines on secure server configuration
- For configuring the firewall, the following ports will be used:
    - Incoming TCP port 8080: deliver the Visualization Tool frontend to trainees
    - Outgoing connections to the platform's message broker (TCP ports 15674 and optionally 61613)
    - Incoming TCP port 9999/UDP port 9999: used for Smart Plug simulation in the Smart Home scenario
    - Outgoing connection to the database required in the healthcare scenario

3.3.2 Installation:

Installation only consists of copying the jar-file to the server.

3.3.3 Running the software:

To run the software, it has to be started as a background task and detached from the console (so it continues running after user logs out). After a server reboot these steps have to be repeated.

The software is started using the following commands (also redirects output to a log file):

```
java -jar simulation.jar &> log.txt &
disown %1
```

3.4 Emulation Tool Installation (ET VM)

The Emulation Tool package is a Java Spring Boot[6] application that includes the core packages:

- Emulation Compiler
- Emulation Engine
- Emulation Controller

In order to be executed, the application should be included in a Linux system, preferably an Ubuntu 18.04 LTS distribution. The application is contained in a jar file (*ThreatArrestAPI.jar*) that is run by the operating system as a system service. The jar is a self-contained Spring Boot archive containing all the Tomcat routines needed to deploy the service over Internet.

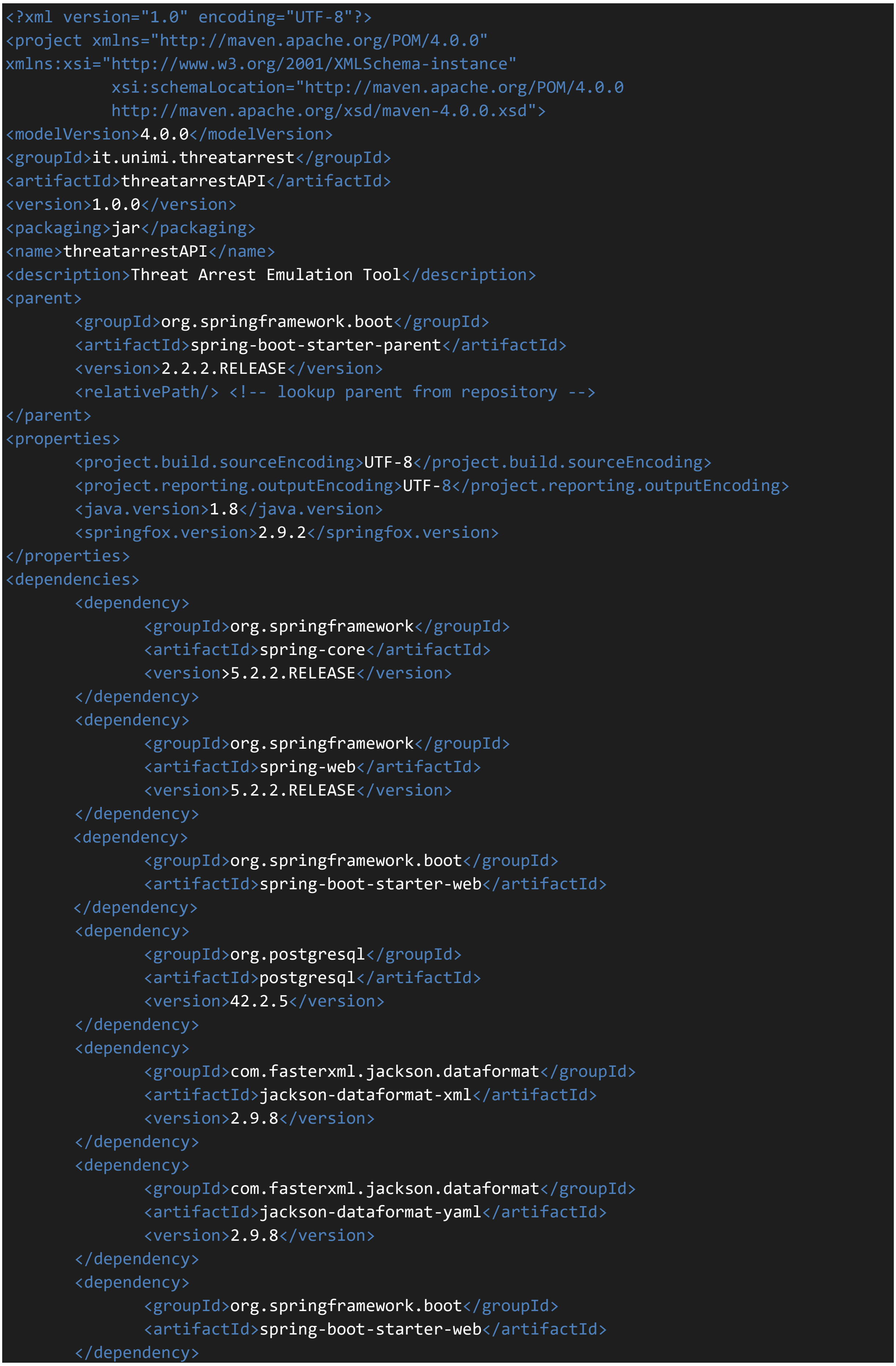
The software project management tool Apache Maven[7] is the only installation pre-requirement of the Emulation Tool. In fact, each time the tool is deployed in a new environment, or updated to a newer version, Maven will solve internal software dependencies and proceed with the source compiling. Maven has to be invoked from the folder where the source code has been copied, using the command below.

```
mvn clean package
```

Maven, in turn, will refer to the Emulation Tool Project Object Model (POM), presented below, that indicates which dependencies should be solved and how the compiling should be executed. In particular, the POM instructs Maven to resolve the following main software dependencies, without any action requested to the user:

- **Spring Boot** to provide the overall self-contained execution environment;
- **PostgreSQL** to include the libraries for the connection and update of the Guacamole database;
- **FasterXML Jackson**[8] to provide the libraries for the management of JSON and XML within a Java application;
- **Glassfish JAXB**[9] to provide the methods for binding XML schemas and Java representations;
- **Openstack4j**[10] open source Java library to allow the provisioning and control of the overall OpenStack system;
- **Apache Freemarker**[11] open source library used to generate and change data, like XML, based on templates;
- **Snakeyaml**[12] open source library to serialize Java objects to YAML documents, and vice versa.

[6] https://spring.io/projects/spring-boot
[7] https://maven.apache.org/
[8] https://github.com/FasterXML/jackson
[9] https://eclipse-ee4j.github.io/jaxb-ri/
[10] http://www.openstack4j.com/
[11] https://freemarker.apache.org/
[12] https://www.baeldung.com/java-snake-yaml



```
<?xml version="1.0" encoding="UTF-8"?>
<project xmlns="http://maven.apache.org/POM/4.0.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
           xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
           http://maven.apache.org/xsd/maven-4.0.0.xsd">
<modelVersion>4.0.0</modelVersion>
<groupId>it.unimi.threatarrest</groupId>
<artifactId>threatarrestAPI</artifactId>
<version>1.0.0</version>
<packaging>jar</packaging>
<name>threatarrestAPI</name>
<description>Threat Arrest Emulation Tool</description>
<parent>
       <groupId>org.springframework.boot</groupId>
       <artifactId>spring-boot-starter-parent</artifactId>
       <version>2.2.2.RELEASE</version>
       <relativePath/> <!-- lookup parent from repository -->
</parent>
<properties>
       <project.build.sourceEncoding>UTF-8</project.build.sourceEncoding>
       <project.reporting.outputEncoding>UTF-8</project.reporting.outputEncoding>
       <java.version>1.8</java.version>
       <springfox.version>2.9.2</springfox.version>
</properties>
<dependencies>
       <dependency>
              <groupId>org.springframework</groupId>
              <artifactId>spring-core</artifactId>
              <version>5.2.2.RELEASE</version>
       </dependency>
       <dependency>
              <groupId>org.springframework</groupId>
              <artifactId>spring-web</artifactId>
              <version>5.2.2.RELEASE</version>
       </dependency>
       <dependency>
              <groupId>org.springframework.boot</groupId>
              <artifactId>spring-boot-starter-web</artifactId>
       </dependency>
       <dependency>
              <groupId>org.postgresql</groupId>
              <artifactId>postgresql</artifactId>
              <version>42.2.5</version>
       </dependency>
       <dependency>
              <groupId>com.fasterxml.jackson.dataformat</groupId>
              <artifactId>jackson-dataformat-xml</artifactId>
              <version>2.9.8</version>
       </dependency>
       <dependency>
              <groupId>com.fasterxml.jackson.dataformat</groupId>
              <artifactId>jackson-dataformat-yaml</artifactId>
              <version>2.9.8</version>
       </dependency>
       <dependency>
              <groupId>org.springframework.boot</groupId>
              <artifactId>spring-boot-starter-web</artifactId>
       </dependency>
```

```
        <dependency>
                <groupId>io.springfox</groupId>
                <artifactId>springfox-swagger2</artifactId>
                <version>${springfox.version}</version>
        </dependency>
        <dependency>
                <groupId>io.springfox</groupId>
                <artifactId>springfox-swagger-ui</artifactId>
                <version>${springfox.version}</version>
        </dependency>
        <dependency>
                <groupId>io.springfox</groupId>
                <artifactId>springfox-bean-validators</artifactId>
                <version>${springfox.version}</version>
        </dependency>
        <dependency>
                <groupId>org.springframework.boot</groupId>
                <artifactId>spring-boot-starter-test</artifactId>
                <scope>test</scope>
        </dependency>
        <dependency>
                <groupId>org.pacesys</groupId>
                <artifactId>openstack4j</artifactId>
                <version>3.2.0</version>
                <classifier>withdeps</classifier>
        </dependency>
        <dependency>
                <groupId>org.glassfish.jaxb</groupId>
                <artifactId>jaxb-xjc</artifactId>
                <version>2.4.0-b180830.0438</version>
        </dependency>
        <dependency>
                <groupId>org.glassfish.jaxb</groupId>
                <artifactId>jaxb-runtime</artifactId>
                <version>2.4.0-b180830.0438</version>
        </dependency>
        <dependency>
                <groupId>org.freemarker</groupId>
                <artifactId>freemarker</artifactId>
                <version>2.3.28</version>
        </dependency>
        <dependency>
                <groupId>org.yaml</groupId>
                <artifactId>snakeyaml</artifactId>
                <version>1.24</version>
        </dependency>
         <dependency>
                <groupId>org.projectlombok</groupId>
                <artifactId>lombok</artifactId>
                <version>1.18.6</version>
         </dependency>
</dependencies>
<build>
        <finalName>${project.artifactId}</finalName>
        <plugins>
                <plugin>
                        <groupId>org.springframework.boot</groupId>
                        <artifactId>spring-boot-maven-plugin</artifactId>
```

```
            <configuration>
                <executable>true</executable>
            </configuration>
        </plugin>
    </plugins>
</build>
</project>
```

After the package has been built, the tool should be run as Linux service and included in the list of services triggered at system boot. The configuration file *compiler.service,* provided in the main folder and shown in the code snippet below must be copied in the system folder */etc/system/user*. The configuration file, when executed, will refer to the executable script *start.sh,* included in the main folder, which will effectively activate the Emulation Tool application.

```
[Unit]
Description=Threat-Arrest Emulation Tool
[Service]
Type=forking
User=compiler

# The configuration file application.properties should be here:
#change this to your workspace
WorkingDirectory=/home/TA/threat-arrest

# Paths to executables.
ExecStart=/home/TA/threat-arrest/start.sh start
ExecStop=/home/TA/threat-arrest/start.sh stop
ExecReload=/home/TA/threat-arrest/start.sh restart
SuccessExitStatus=143
TimeoutStopSec=10
Restart=on-failure
RestartSec=5

[Install]
WantedBy=multi-user.target
```

Finally, the specific configurations of the Emulation Tool are contained in the *application.properties* file, included in the package and shown below. In this first release of the tool, the available properties are the following:

- **openstack.endpoint, openstack.uid, openstack.domainname:** endpoint, unique id, domain name to refer the Openstack framework;
- **openstack.projectname, openstack.projectid**: name and unique id of the Openstack project that will host the emulated environment;
- **openstack.dburl, openstack.dbuser, openstack.dbpassword**: URL, username and password used to connect to the Guacamole instance database;
- **openstack.guacamole**: part of the URL used to contact the emulated components through Guacamole;
- **openstack.key, openstack.salt, openstack.keyname, openstack.keyval**: used to refer and define the key injected in the emulated components to be controlled by Openstack

- **openstack.secgroupname, openstack.secgroupval**: name and id of the default security group, defined in Openstack and used to allow Guacamole connections;
- **openstack.defaultnetwork, openstack.defaultrouter, openstack.routerip**: configurations used in the Heat template to refer the public network and the router used to connect to it;
- **openstack.curl**: default command to trigger Openstack WaitHandle objects.

```
openstack.endpoint=http://5.79.110.8:5000/v3/
openstack.uid=2b0542edcfa8423880942d4b95a49e36
openstack.pwd=***************
openstack.domainName=Default
openstack.projectName=Threatarrest
openstack.projectId=811ff0ed6828410e91bf4e0485ff2353
openstack.dburl=jdbc:postgresql://X.X.X.X:5432/guacamole_db
openstack.dbuser=guacamole_user
openstack.dbpwd=*************
openstack.guacamole=http://X.X.X.X:8080/guacamole/#/client/
openstack.key=-----BEGIN RSA PRIVATE KEY-----\r\n\
****************************************************************\r\n\
****************************************************************\r\n\
****************************************************************\r\n\
****************************************************************\r\n\
**************************************************************==\r\n\
-----END RSA PRIVATE KEY-----
openstack.salt=FE24ADC5E11E2B25288D1704ABE67A79E342ECC26064CE69C5B3177795A82264
openstack.keyname=key1
openstack.keyval=common-key
openstack.secgroupname=guacamolesecgroup
openstack.secgroupval=6f51feec-0dae-4d19-8dfd-6cd6f0fc94c3
openstack.defaultnetwork=086c28ba-03a7-430f-b1df-b7f3d8b9d990
openstack.defaultrouter=db82e035-9395-4bdf-bf58-ac23a02b6dcd
openstack.routerip=253
openstack.curl=curl -i -X POST -H "X-Auth-Token: wc_token" -H "Content-Type: 
application/json" -H "Accept: application/json" wc_endpoint --data-binary 
"{\\\\"status\\\\": \\\\"SUCCESS\\\\"}"
```

3.4.1 Apache Guacamole Installation (RemAccess VM)

The Apache Guacamole[13] clientless remote desktop gateway, which provides the direct connection to the virtual machines composing the emulated environment, is hosted in the RemAccess virtual machine within the Openstack infrastructure.

The RemAccess VM is a common Ubuntu 18.04 LTS that acts as the entry door for trainers and trainees to the THREAT-ARREST framework. The machine host specific forward rules to provide access to tools VM. Refer to Section 3.1.1 for details on the port forwarding setup.

The THREAT-ARREST framework exploits a common installation of the Guacamole Server and Client version 1.1.0.

3.4.1.1 Guacamole Server Installation

The Guacamole Server contains all the server-side components required to connect to remote machine via SSH and RDP. It is composed of a common C library, *libguac*, separate libraries

[13] https://guacamole.apache.org/

for each supported protocol (that is, RDP, SSH, and VNC), and *guacd*, the Linux service that implements Guacamole functionalities.

In particular, *guacd* is the proxy daemon that accepts users' connections and tunnels them through the Guacamole web application, connecting the remote VM. The pre-requisites to build the Guacamole Server are an updated C compiler (such as *gcc*) and the libraries that guacamole-server depends on. The main libraries that should be installed are the following:

- **Cairo**, used for graphics rendering;
- **libjpeg-turbo**, used to provide JPEG support;
- **libpng**, used by libguac to write PNG images;
- **libtool**, used to support the build process;
- **FreeRDP 2.0.0**, required for RDP support;
- **libssh2**, required for SSH support;
- **libVNCServer**, required for VNC support;
- **OpenSSL**, to provide support for SSL and TLS.

The libraries should be included in the system using the distribution-specific Linux packaging tool (for Ubuntu the tool APT). A more complete list of optional libraries is provided in the Guacamole manual[14].

The Guacamole Server sources package need to be downloaded by the project website[15], uploaded in the installation folder, and decompressed using TAR. Then, the server is built launching the following sequence of commands with root permissions, assuming that each step successfully completed all the operations without returning errors.

```
# Configure the installation and include the daemon in the init.d folder

$ ./configure --with-init-dir=/etc/init.d

# Compile the server package

$ make

# Install the components

$ make install

# Update system's cache of installed libraries

$ ldconfig

# Add guacd to the init.d folder to be executed at boot

$ update-rc.d guacd defaults
```

[14] https://guacamole.apache.org/doc/gug/

[15] https://guacamole.apache.org/releases/1.1.0/

3.4.1.2 Guacamole Client Installation

The Guacamole Client package contains all Java and JavaScript components of Guacamole to build the web application that will serve the HTML5 Guacamole Client to the VMs. This web application will then connect to *guacd*, to provide access authorization.

The pre-requisites to compile the client are Apache Maven, an updated Java JDK, a PostgreSQL database available, and a running Apache Tomcat server. As for the Guacamole Server, the sources package should be downloaded from the Guacamole website and uncompressed in the main folder.

Then, the following list of commands should be launched from the main folder with root permissions.

```
# Build the client

$ mvn package

# Deploy the WAR package in Tomcat

$ cp guacamole.war /var/lib/tomcat/webapps

# Restart Tomcat

$ /etc/init.d/tomcat8 restart

# Launch guacd

$ /etc/init.d/guacd start
```

The Guacamole configuration file can be found in the */etc/guacamole* folder as *guacamole.properties.* In the context of the Emulation Tool, only the configurations below are required.

```
# Hostname and port of guacamole proxy
guacd-hostname: localhost
guacd-port:     4822

# Auth provider class (authenticates user/pass combination, needed if using the provided
login screen)
auth-provider: net.sourceforge.guacamole.net.basic.BasicFileAuthenticationProvider

basic-user-mapping: /etc/guacamole/user-mapping.xml

postgresql-hostname: localhost
postgresql-port:     5432
postgresql-database: guacamole_db
postgresql-username: guacamole_user
postgresql-password: *************

# PostgreSQL
postgresql-default-max-connections: 10
postgresql-default-max-group-connections: 10
```

To provide the connection to the Guacamole database, the PostgreSQL JDBC driver *guacamole-auth-jdbc-postgresql-1.1.0.jar* should be uncompressed from the *guacamole-auth-*

jdbc-1.1.0.tar.gz, available in the download page, and copied in the */etc/guacamole/extensions* folder.

Finally, the Guacamole database should be created copying in the main folder the SQL scripts *001.create.schema.sql* and *002.create.admin.user.sql* from the previous JDBC package and executed as indicated below.

```
# Create the Guacamole DB

$ createdb guacamole_db

# Execute the SQL scripts

$ cat schema/*.sql | psql -d guacamole_db -f -
```

The installation of the Guacamole framework is then completed and can be accessed at the *address http://localhost:8080/guacamole* using the *gaucadmin* username and the default password (*guacadmin*, to be changed after first login).

The creation of new users and connections, as well as the release of connection URLs, are in charge of the Emulation Tool. The whole Guacamole infrastructure is hence completely transparent for trainers and trainees, that will be provided with the direct access to the specific VM, via the required protocol (RDP or SSH).

3.4.2 Emulated Components Monitoring (EMon VM)

The Emulated Components Monitor (a.k.a. Resource Monitor or just Monitor), as it is described in D2.2: "Emulated components monitoring module", is a collection of collaborative services aimed to provide accurate readings of the Platform's hardware and virtual resources and make them available for both automatic resource management tools and resource visualisation tools.

The Resource Monitor is implemented in Java and deployed as a Web Service, hosted by an Apache Tomcat Web Server, permanently running on the EMon VM (shown in Figure 1).

3.4.2.1 Prerequisites

Below is a list of prerequisites that are required to be available and installed in advance, in order to enable reliable and uninterrupted operation of the Resource Monitoring Component:

i) First, as it is shown in Figure 1, the Resource Monitor is deployed on its dedicated static EMon Virtual Machine. As it is described in Section 2 of this document and shown in the Table 1, this machine needs to have at least 2 vCPUs, 8 GB of RAM, and 60 GB of available file system storage. Linux OS is also a prerequisite. Ubuntu 18.04 or newer version needs to be installed in advance.

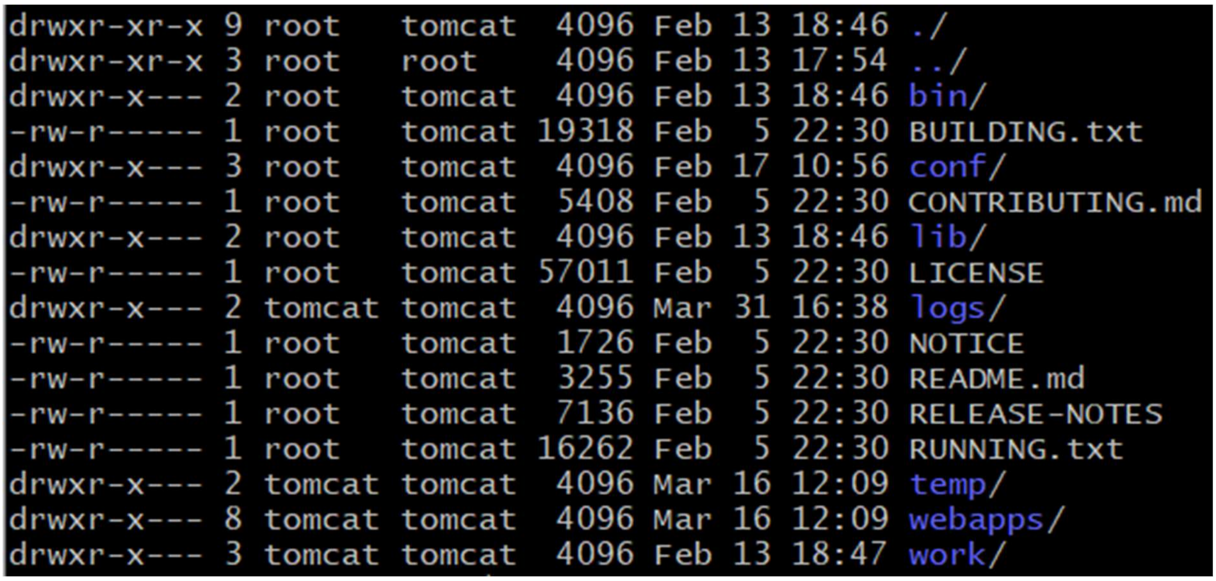
ii) Next, as it's also shown in Table 2, TCP ports 80, 8080, and 22 need to be configured and opened to enable the Monitoring Tool installation, administration, management and proper operation.

iii) In addition, as it is described in D2.2, the Resource Monitor relies on the Nova Compute API. Assuming that, THREAT-ARREST platform runs on top of the OpenStack environment, the Nova Compute Service is already available at the OpenStack Hypervisor, however it needs to be properly configured in terms of network routing, port forwarding and firewall ruling to be accessible from the EMon VM. These details are described in the section 3.1 of this document.

iv) Finally, is it's also shown in Table 2, Java 1.8 or newer needs to be installed along with the Apache Tomcat Web Server 8.5 or newer.

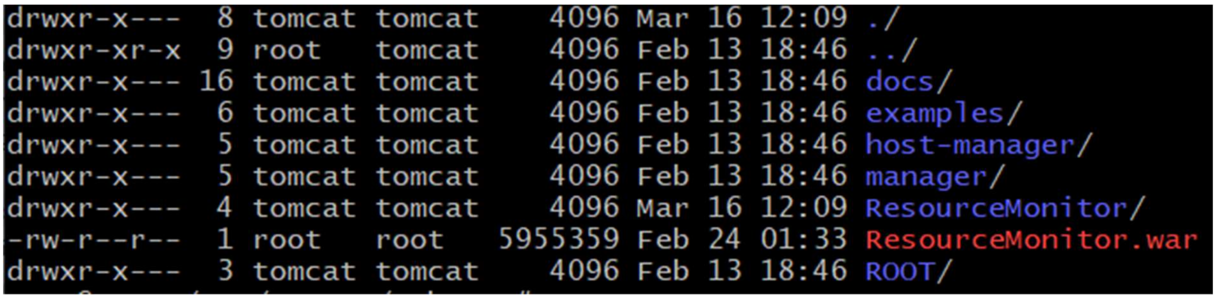
3.4.2.2 Installation and deployment

As mentioned earlier, Resource Monitor is a Web Service, hosted by an Apache Tomcat Web Server. It is deployed as a WAR file (`ResourceMonitor.war`), which should be installed in the Tomcat `webapps` folder, as it is shown below at the Figure 4 and Figure 5. After the Resource Monitor WAR is installed, the Tomcat Server should be restarted. At his point the ResourceMonitor.war will be unzipped into the `ResourceMonitor` folder, which becomes a home folder of the Resource Monitoring Service.



```
drwxr-xr-x 9 root   tomcat  4096 Feb 13 18:46 ./
drwxr-xr-x 3 root   root    4096 Feb 13 17:54 ../
drwxr-x--- 2 root   tomcat  4096 Feb 13 18:46 bin/
-rw-r----- 1 root   tomcat 19318 Feb  5 22:30 BUILDING.txt
drwxr-x--- 3 root   tomcat  4096 Feb 17 10:56 conf/
-rw-r----- 1 root   tomcat  5408 Feb  5 22:30 CONTRIBUTING.md
drwxr-x--- 2 root   tomcat  4096 Feb 13 18:46 lib/
-rw-r----- 1 root   tomcat 57011 Feb  5 22:30 LICENSE
drwxr-x--- 2 tomcat tomcat  4096 Mar 31 16:38 logs/
-rw-r----- 1 root   tomcat  1726 Feb  5 22:30 NOTICE
-rw-r----- 1 root   tomcat  3255 Feb  5 22:30 README.md
-rw-r----- 1 root   tomcat  7136 Feb  5 22:30 RELEASE-NOTES
-rw-r----- 1 root   tomcat 16262 Feb  5 22:30 RUNNING.txt
drwxr-x--- 2 tomcat tomcat  4096 Mar 16 12:09 temp/
drwxr-x--- 8 tomcat tomcat  4096 Mar 16 12:09 webapps/
drwxr-x--- 3 tomcat tomcat  4096 Feb 13 18:47 work/
```

Figure 4: Recommended Tomcat ROOT directory structure

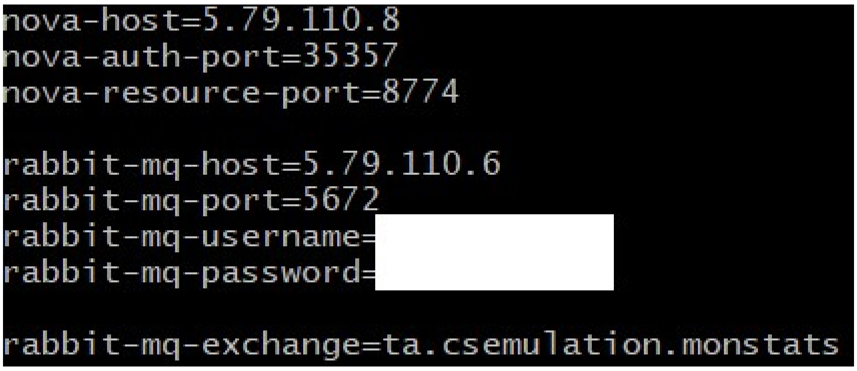


```
drwxr-x---  8 tomcat tomcat    4096 Mar 16 12:09 ./
drwxr-xr-x  9 root   tomcat    4096 Feb 13 18:46 ../
drwxr-x--- 16 tomcat tomcat    4096 Feb 13 18:46 docs/
drwxr-x---  6 tomcat tomcat    4096 Feb 13 18:46 examples/
drwxr-x---  5 tomcat tomcat    4096 Feb 13 18:46 host-manager/
drwxr-x---  5 tomcat tomcat    4096 Feb 13 18:46 manager/
drwxr-x---  4 tomcat tomcat    4096 Mar 16 12:09 ResourceMonitor/
-rw-r--r--  1 root   root   5955359 Feb 24 01:33 ResourceMonitor.war
drwxr-x---  3 tomcat tomcat    4096 Feb 13 18:46 ROOT/
```

Figure 5: Tomcat webapps directory

3.4.2.3 Configuration

Resource Monitoring Service comes up with the `app.properties` configuration file. Some properties need to be properly configured before the use. A typical config file is shown at the Figure 6, and it can be found in the `WEB-INF` directory under the Resource Monitoring home. After the Resource Monitor is properly configured, the Tomcat Server needs to be restarted once again.



```
nova-host=5.79.110.8
nova-auth-port=35357
nova-resource-port=8774

rabbit-mq-host=5.79.110.6
rabbit-mq-port=5672
rabbit-mq-username=[redacted]
rabbit-mq-password=

rabbit-mq-exchange=ta.csemulation.monstats
```

Figure 6: Resource Monitoring Service `app.properties` *config file*

At this point the Resource Monitor is up and running, and it can be operated through its REST API as it is described in D6.1 "Initial Prototype of Integrated THREAT-ARREST Platform".

3.5 Gamification Tool Installation (GT VM)

Protect (Goeke et al., 2019) comes as precompiled binary file.

i) While the binary might run on other platforms, too we only tested it with the Linux distribution Ubuntu in version 18.04 LTS.

ii) Protect provides a frontend via a webserver to communicate with the user and a backend to the system via the API. There is no package, but a protect Zip file.

iii) Installation of Protect is done via the following steps:

a. Download `protect.zip`

b. Unzip `protect.zip` in a convenient folder

c. Run the extracted binary `protect/app`

d. Ensure port 80 can be accessed by clients.

3.6 Training Tool and Dashboard Installation (TT VM)

3.6.1 Requirements

Any Linux distribution would be acceptable (preferred Ubuntu 18.04 or CentOS 7 or 8) and a Docker (version 19.03.5 at least) and docker-compose (version 1.25.3 at least) installation. No other dependencies are required to be installed system-wide as the libraries will be packaged in the Docker images.

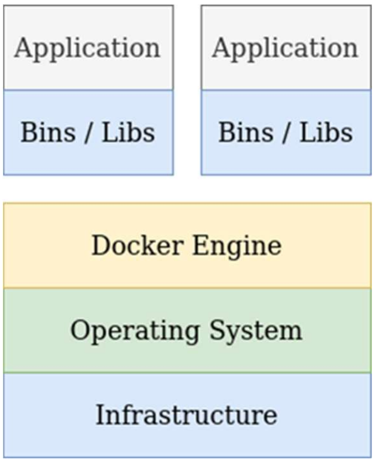


Figure 7: Docker Deployment

3.6.2 Services and software packages

Docker containers are required in order for TT to be deployed. Those contain 3 spring-boot web application and a MySQL v8 database container. No software packages are required to be installed system-wide. The Docker containers that are required to run in order for the TT to be operational are depicted below:

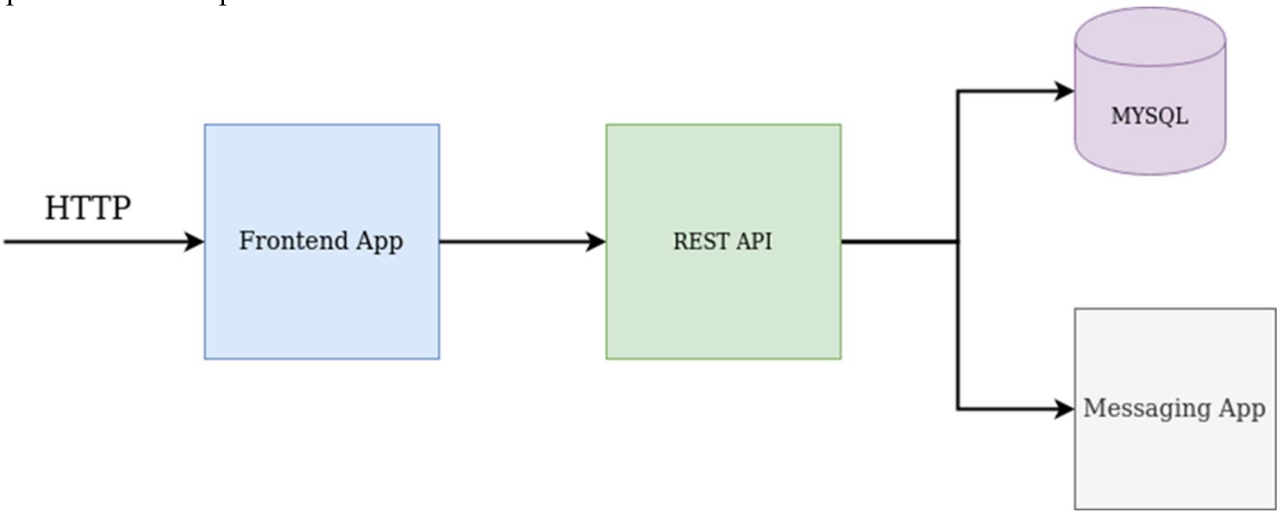


Figure 8: TT Deployment

The services executed are:

- A frontend Spring Boot web application serving the HTTP requests and presenting the UI of the TT.
- A REST API (Spring Boot) to provide an interface for the business logic on the queries performed on the database and triggering the messaging app.
- A MySQL container.

- A Spring Boot application (Messaging App) for triggering the Simulation Tool and handling the responses of the Visualization Tool.

3.6.3 Dependencies

The only dependencies are Docker and docker-compose. The standard installation from the official site is enough (not the installation with snap package manager because bugs have been observed).

3.7 Assurance Tool Installation (AT VM)

3.7.1 Overview

The Assurance Tool carries out a continuous runtime assessment of the aspects of the target cyber-system that are important for a Cyber Threat and Training Preparation (CTTP) training program. These aspects are defined by the CTTP model and sub-models and extracted via the appropriate translation mechanisms. For example, the CTTP model defines the components of the cyber-system that should be monitored, the events of these components that are of importance (e.g., operating system calls, external service calls, user actions) and the conditions that should be satisfied by them. Furthermore, each tool identified within the THREAT-ARREST platform (i.e., Emulation, Simulation, Gamification, Data Fabrication, Visualization, and Training Tools) holds its own CTTP sub-model which leads to the instantiation of the overall Training Programme.

3.7.2 Hardware and Software Requirements

The hardware and software requirements identified for the Assurance Model Virtual Machine are presented in Table 5.

Table 5: Assurance Tool Hardware and Software Requirements

CPU cores @ 2.4 GHz Architecture x86 (64-bit)	2
RAM (GB) DDR4	16
Storage (GB) SSD	60
Bandwidth (Mbps)	50
Software (and version)	Ubuntu (18 LTS), Oracle Java (1.8), MySQL Server (Latest)
Hostname	AT
List of TCP Port Numbers	80 (HTTP), 8080 (Tomcat), 443 (HTTPS/TLS), 3306 (MySQL), 22 (SSH), 5672 (RabbitMQ)

More specifically, the assurance tool runs in an Ubuntu 18 Virtual Machine. The CTTP Model editor is written in Java while the CTTP Model GUI in PHP 7, CSS, HTML and Javascript.

The editor makes use of a MySQL database located in the VM to store the CTTP models and the message broker (RabbitMQ) located in the main VM of the platform to communicate with the Training Tool in order to instantiate the Training Programme and provide the sub models to its corresponding tools.

3.7.3 Installation process

The CTTP Model editor (which is part of the Assurance tool) was packaged as a web application (.war) and deployed in a web server (Apache Tomcat/9.0.30) located inside the Assurance Tool VM.

A GUI was then created in order to facilitate the end-user with the creation, editing and view of the CTTP core model and its sub models.

The guideline for the CTTP Model Editor GUI can be found in Section 4.3.

3.8 Data Fabrication Platform Installation (DFP VM)

As it is described in "D5.1 – Real event logs statistical profiling module and synthetic event log generator v1" document, IBM's Data Fabrication Platform (DFP) (IBM, 2017) is a web-based central platform for generating high-quality data for testing, development, and training. As it is also described in D5.1, the DFP is being enhanced to support the THREAT-ARREST project requirements. The DFP has been enriched with an ability to generate sequences of simulated cyber-events in general, and synthetic security event log files in particular.

By the time when this document is written and released, the enhanced DFP is not fully integrated within the THREAT-ARREST Platform yet. It is rather deployed externally and being used off-line as a stand-alone application for fabrication of both, the static DB records as well as dynamic scenario log files. The DFP is being modified to be deployed as a Web Service, hosted under an Apache Tomcat Server. This enhancement along with other important features will be documented in the future deliverable "D5.5 – Real event logs statistical profiling module and synthetic event log generator v2". An installation procedure, deployment scheme and usage guidelines of the DFP as a Web Service will be described in the future "D6.6 – Final Installation and usage guidelines for the THREAT–ARREST platform" deliverable.

4 THREAT-ARREST Usage Guidelines

The THREAT-ARREST training is offered as a service to organizations through a Web-based GUI. The first version of the platform is released along three full-fledged training scenarios for Smart Home & IoT, Smart Shipping, and Healthcare, each addressing trainees of different knowledge and skills. The platform's Dashboard (front-end) is accessible at https://www.threat-arrest.org.

Based on the first integrated version, three training scenarios have been created for the different project use cases – Smart Home & IoT, Smart Shipping, and Healthcare, targeting trainees of different categories and skills. In the following, we list the videos of the different platform demonstrations uploaded on YouTube that can server as guidelines on how to use the platform functionality.

Table 6: THREAT-ARREST Demonstration Videos

THREAT-ARREST Demo Description	Link to Video
THREAT-ARREST Smart Energy Scenario Demo	https://youtu.be/0vGNXkne_wM
THREAT-ARREST Shipping Scenario Demo	https://youtu.be/vs8T1oZoha0
THREAT-ARREST Healthcare Scenario Demo	https://youtu.be/iFmFTBVWeio
THREAT-ARREST Training Tool Demo	https://youtu.be/DGOg1sEENCY
THREAT-ARREST CTTP Model Editor Demo	https://youtu.be/TR2jeRVLSlY
THREAT-ARREST Data Fabrication Platform (IBM) Demo	https://youtu.be/K0UiFgfWoHk

4.1 Dashboard Usage Guidelines

This section regards the usage guidelines for the Training Tool's Dashboard GUI. You can also refer to the Training Tool video in Table 6.

The implemented roles of the TT Dashboard are:

- Administrator
- Trainer
- Trainee

The administrator is solely responsible for the creation of trainers' and trainees' accounts as well as assigning both to a specific sector. Subsequently, a typical set of actions needed for a trainee to be able to commence playing a scenario is:

1. The *administrator* logs in and creates a *trainer* account and assigns it to a sector
2. The *administrator* creates a *trainee* account and assigns it to a sector
3. The *trainer* logs in and assigns Scenarios to the trainee
4. The *trainee* logs in and proceeds to play a scenario

4.1.1 User Login

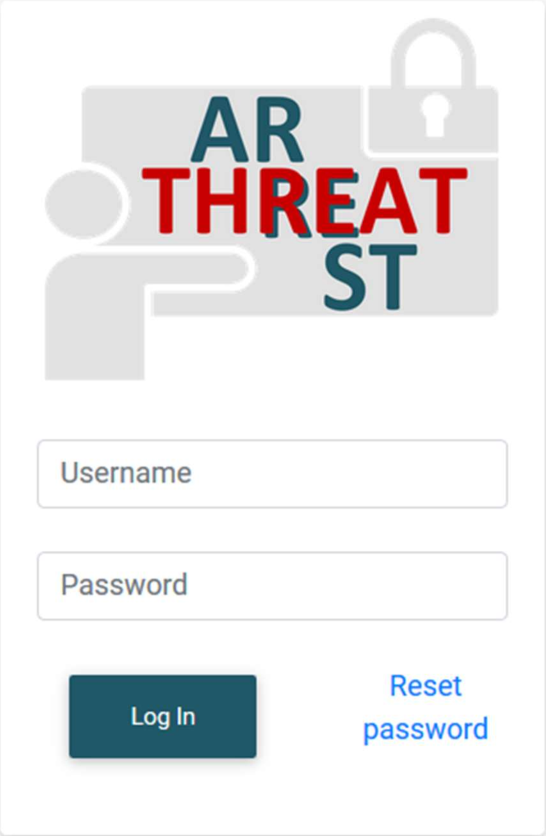


Figure 9: User Login

4.1.2 Password Recovery

By clicking the *Reset Password* option on the login screen, the users proceed to enter their email address and after submitting the form, receive an email containing a unique web link that can be used to reset their password.

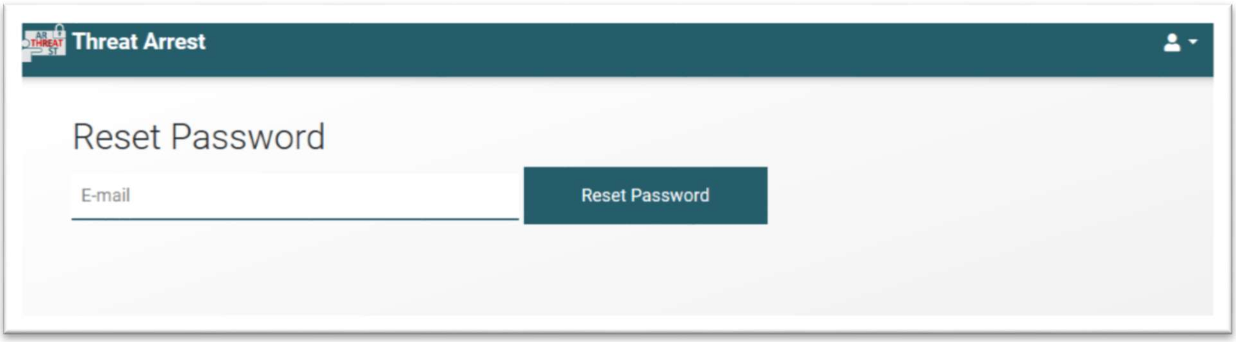
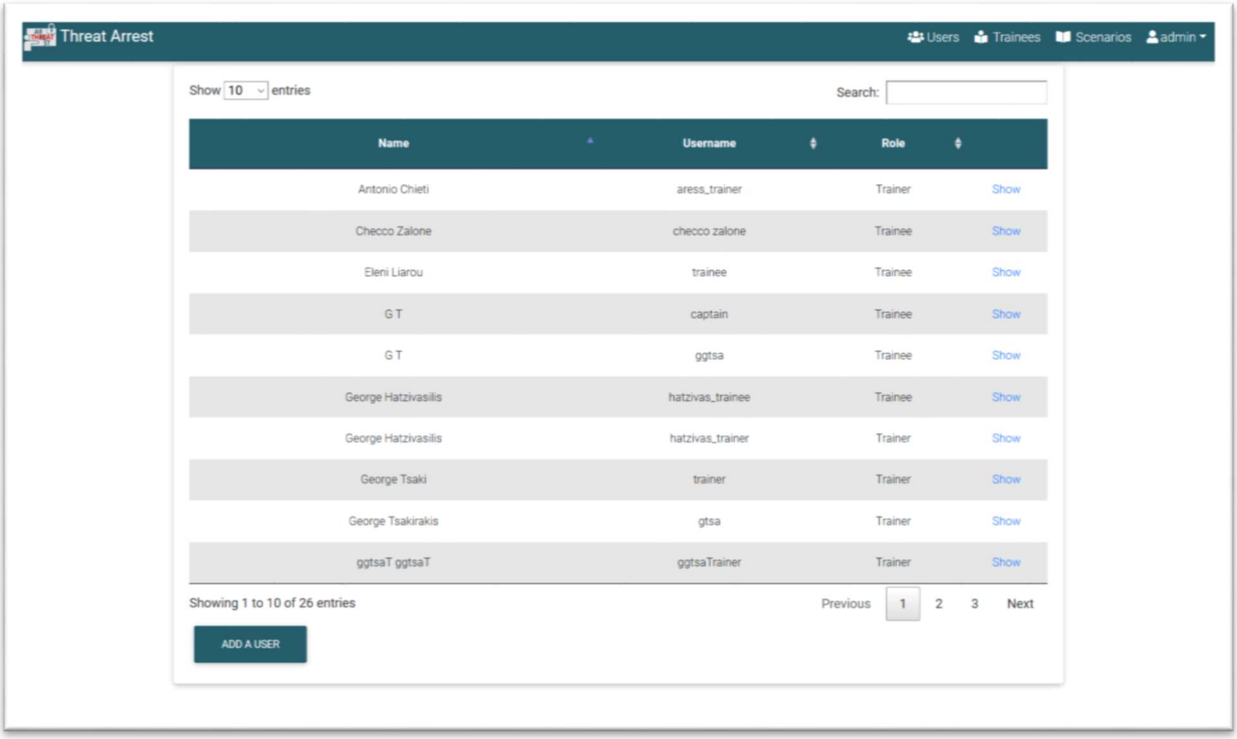


Figure 10: Password Recovery

4.1.3 Administrative Perspective

4.1.3.1 Admin Dashboard (admin)

Upon successful logon the Administrator is presented with the complete list of users.



Show 10 entries

Search:

Name	Username	Role	
Antonio Chieti	aress_trainer	Trainer	Show
Checco Zalone	checco zalone	Trainee	Show
Eleni Liarou	trainee	Trainee	Show
G T	captain	Trainee	Show
G T	ggtsa	Trainee	Show
George Hatzivasilis	hatzivas_trainee	Trainee	Show
George Hatzivasilis	hatzivas_trainer	Trainer	Show
George Tsaki	trainer	Trainer	Show
George Tsakirakis	gtsa	Trainer	Show
ggtsaT ggtsaT	ggtsaTrainer	Trainer	Show

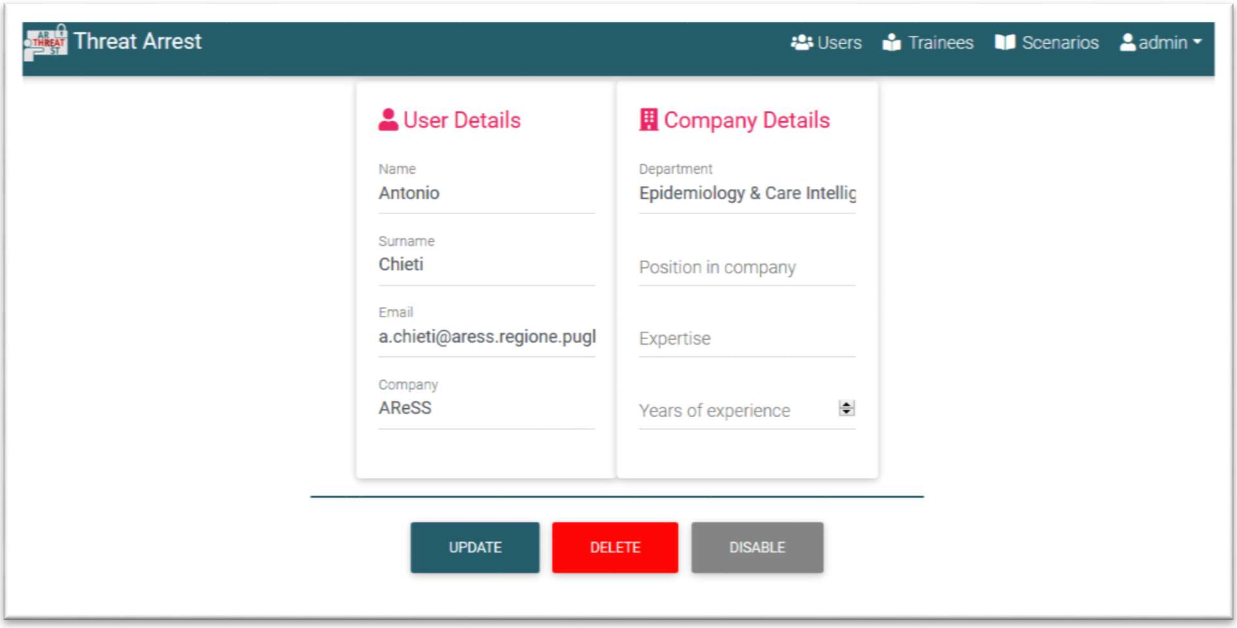
Showing 1 to 10 of 26 entries

Figure 11: Users List

4.1.3.2 Show/Edit User details (admin)

By clicking the button *Show* next to a user, the administrator can:

- Update the user's details
- Disable the user
- Delete the user



User Details

Name
Antonio

Surname
Chieti

Email
a.chieti@aress.regione.pugl

Company
AReSS

Company Details

Department
Epidemiology & Care Intellig

Position in company

Expertise

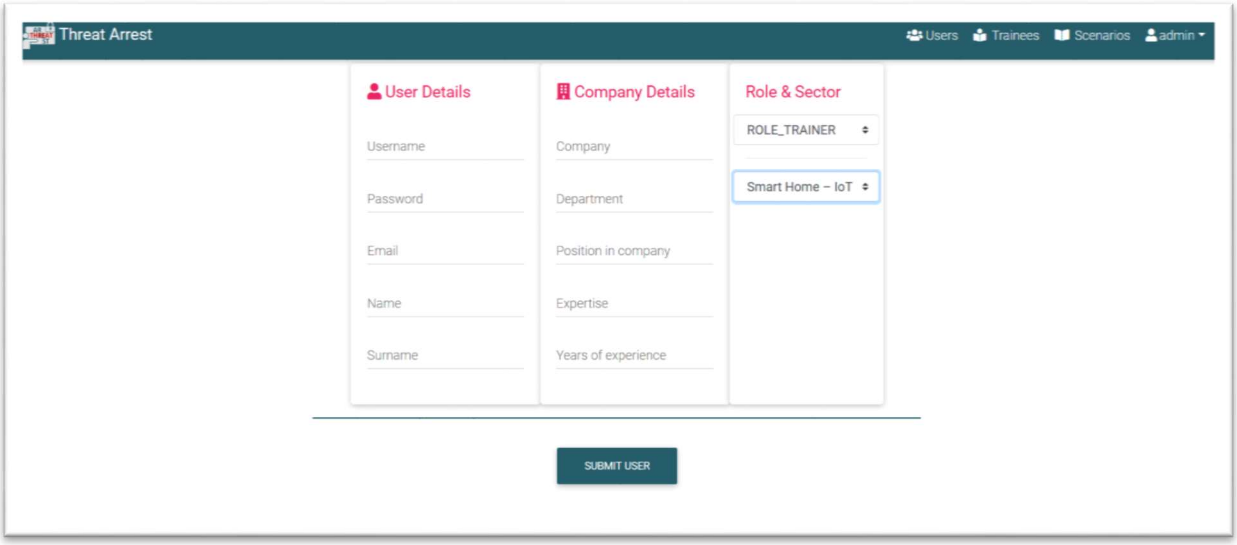
Years of experience

Figure 12: User Details & Actions

4.1.3.3 Create User (admin)

By clicking the button *Add a User* on the Admin Dashboard, the administrator can create a new user and assign them a:

- *Role* (Trainer or Trainee)
- *Sector* (Related to the different CTTP ProjectId i.e. Shipping, SmartHome & IOT etc.)



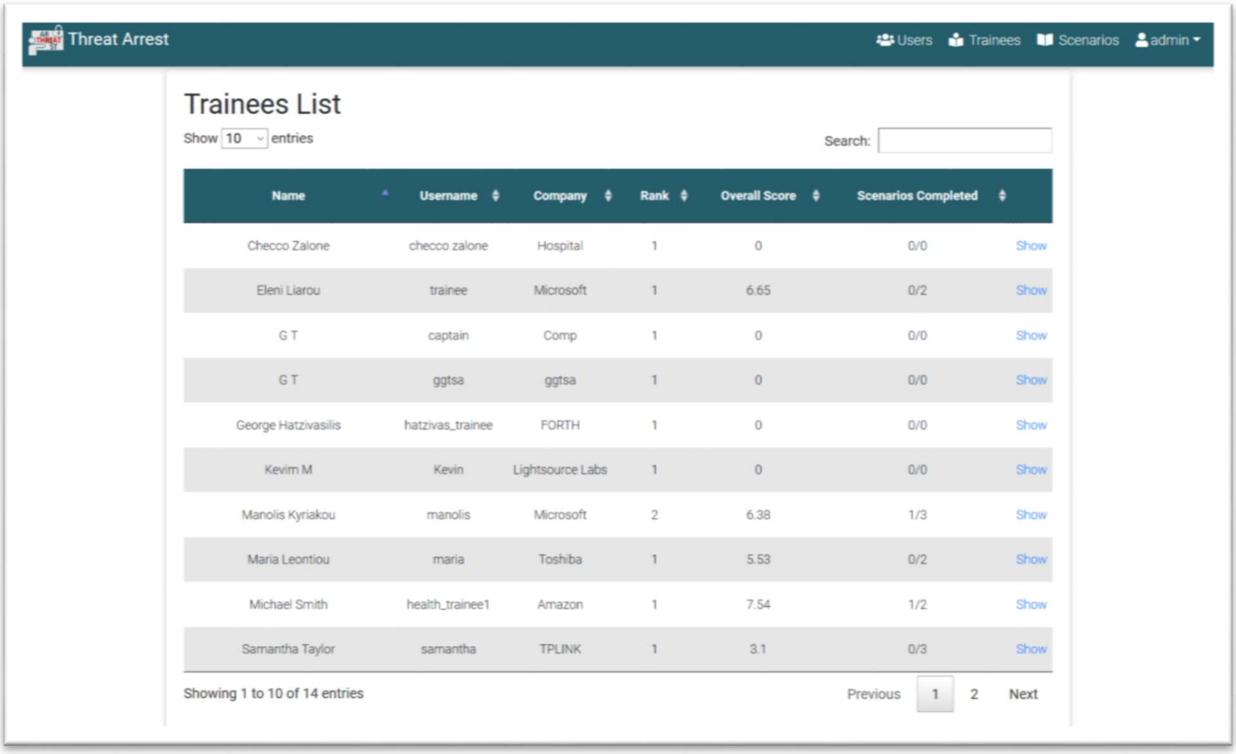
ROLE_TRAINER

Smart Home – IoT

Figure 13: User Account Creation

4.1.3.4 Trainees View (admin/trainer)

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. An administrator can access information of all trainees regardless of their sector, whereas trainers view the information of trainees belonging to the same sector.



Trainees List

Show 10 entries

Search:

Name	Username	Company	Rank	Overall Score	Scenarios Completed	
Checco Zalone	checco zalone	Hospital	1	0	0/0	Show
Eleni Liarou	trainee	Microsoft	1	6.65	0/2	Show
G T	captain	Comp	1	0	0/0	Show
G T	ggtsa	ggtsa	1	0	0/0	Show
George Hatzivasilis	hatzivas_trainee	FORTH	1	0	0/0	Show
Kevim M	Kevin	Lightsource Labs	1	0	0/0	Show
Manolis Kyriakou	manolis	Microsoft	2	6.38	1/3	Show
Maria Leontiou	maria	Toshiba	1	5.53	0/2	Show
Michael Smith	health_trainee1	Amazon	1	7.54	1/2	Show
Samantha Taylor	samantha	TPLINK	1	3.1	0/3	Show

Showing 1 to 10 of 14 entries

Figure 14: Trainees View

At the bottom of the screen there are two graphs that illustrate the Total played time per user and their overall score.

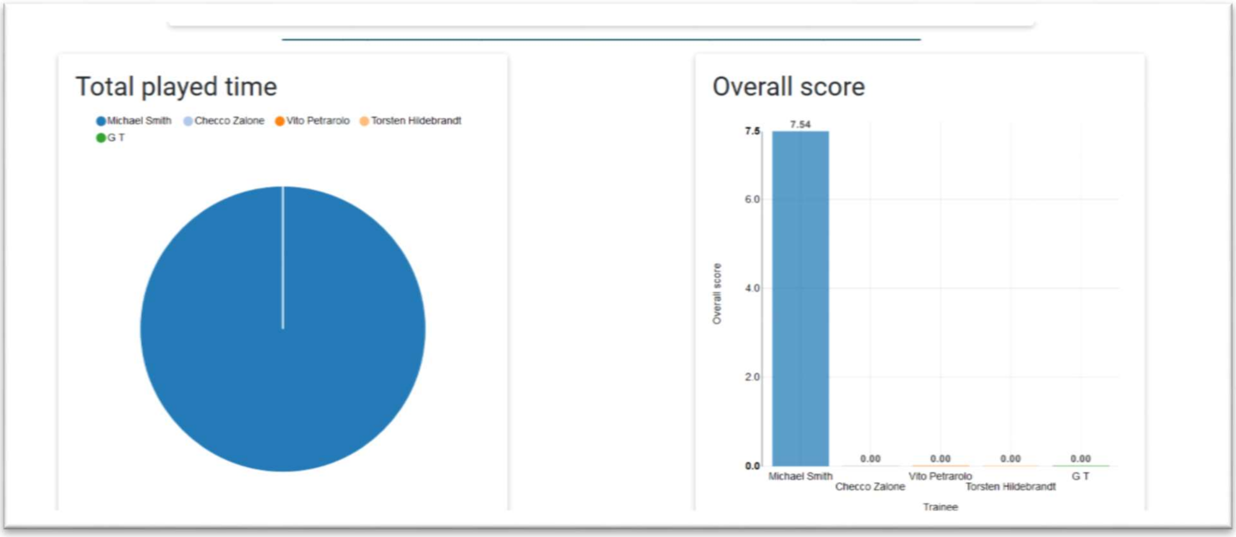
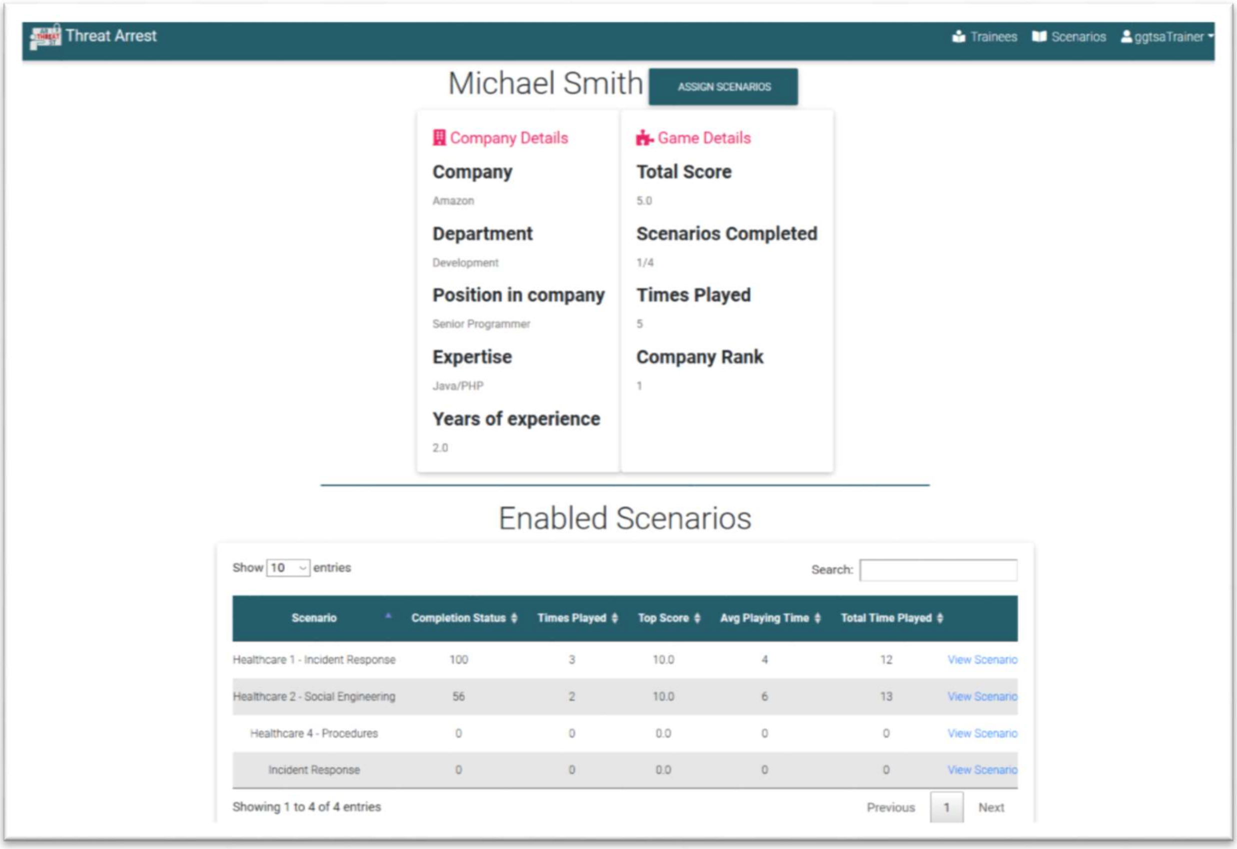


Figure 15: Graphs User's Total Played Time and Overall Score

By clicking the *Show* button next to a trainee, the users' details are presented together with their enabled scenarios and related information per scenario (Completion Status, Times Played etc.)



Michael Smith

Company Details

Company
Amazon

Department
Development

Position in company
Senior Programmer

Expertise
Java/PHP

Years of experience
2.0

Game Details

Total Score
5.0

Scenarios Completed
1/4

Times Played
5

Company Rank
1

Enabled Scenarios

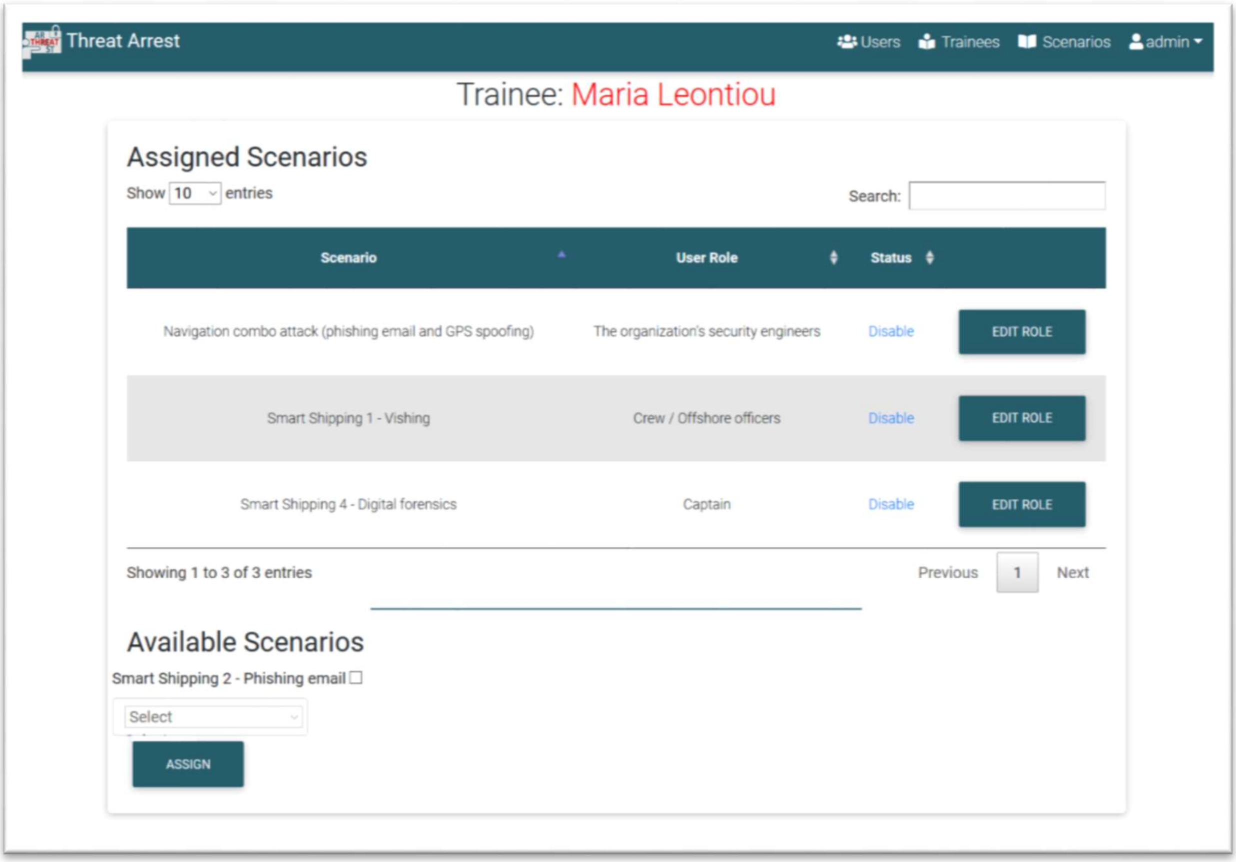
Show 10 entries Search:

Scenario	Completion Status	Times Played	Top Score	Avg Playing Time	Total Time Played	
Healthcare 1 - Incident Response	100	3	10.0	4	12	View Scenario
Healthcare 2 - Social Engineering	56	2	10.0	6	13	View Scenario
Healthcare 4 - Procedures	0	0	0.0	0	0	View Scenario
Incident Response	0	0	0.0	0	0	View Scenario

Showing 1 to 4 of 4 entries

Figure 16: User's Training Details

Furthermore, by clicking the *Assign Scenarios* a new scenario can be enabled for a trainee and assign him/her a scenario specific role. For the scenarios already enabled for the trainee there is an enable/disable as well as an option to change the trainee's scenario role.



Trainee: Maria Leontiou

Assigned Scenarios

Show 10 entries Search:

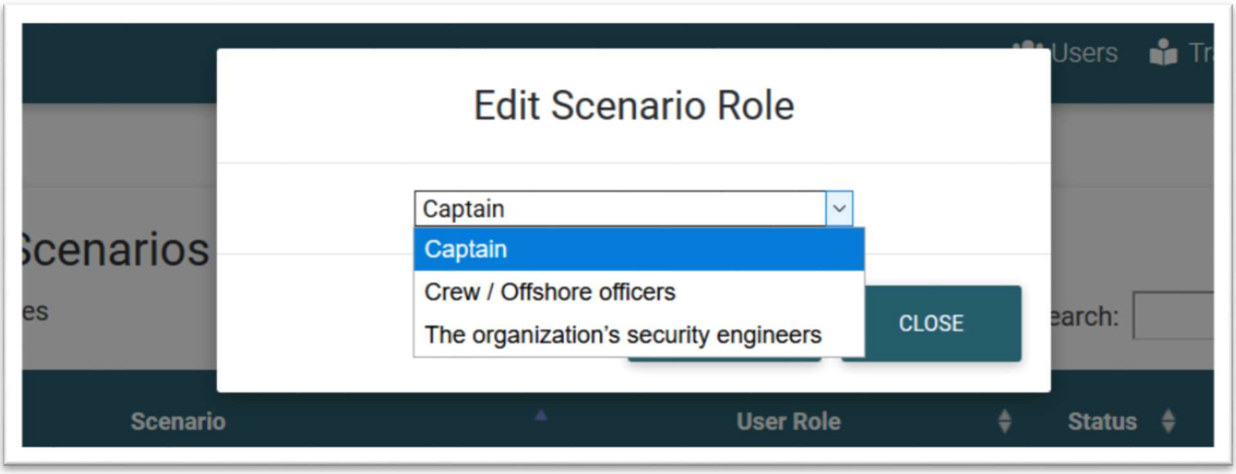
Scenario	User Role	Status	
Navigation combo attack (phishing email and GPS spoofing)	The organization's security engineers	Disable	EDIT ROLE
Smart Shipping 1 - Vishing	Crew / Offshore officers	Disable	EDIT ROLE
Smart Shipping 4 - Digital forensics	Captain	Disable	EDIT ROLE

Showing 1 to 3 of 3 entries

Available Scenarios

Smart Shipping 2 - Phishing email □

Figure 17: Scenario Assignment



Edit Scenario Role

Captain

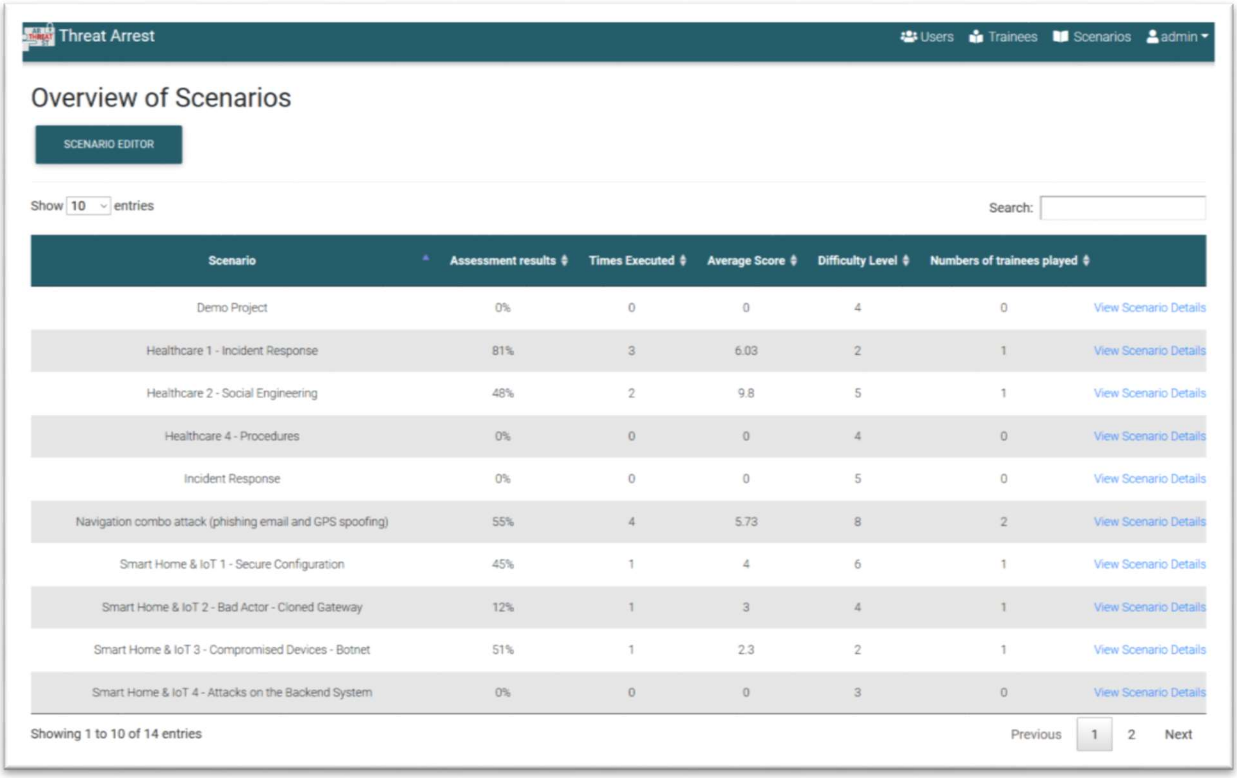
- Captain
- Crew / Offshore officers
- The organization's security engineers

Figure 18: Scenario Role

4.1.3.5 Scenarios View (admin/trainer)

The scenario views are accessible for both admins and trainers, with the only difference being that trainers can only access scenarios that belong to their sector whereas the admin has access to all scenarios regardless of their sector.

Additionally, only an administrator is presented with the button "Scenario Editor" which leads to the Assurance Tool Scenario Editor interface.



Overview of Scenarios

SCENARIO EDITOR

Show 10 entries

Search:

Scenario	Assessment results	Times Executed	Average Score	Difficulty Level	Numbers of trainees played	
Demo Project	0%	0	0	4	0	View Scenario Details
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 4 - Procedures	0%	0	0	4	0	View Scenario Details
Incident Response	0%	0	0	5	0	View Scenario Details
Navigation combo attack (phishing email and GPS spoofing)	55%	4	5.73	8	2	View Scenario Details
Smart Home & IoT 1 - Secure Configuration	45%	1	4	6	1	View Scenario Details
Smart Home & IoT 2 - Bad Actor - Cloned Gateway	12%	1	3	4	1	View Scenario Details
Smart Home & IoT 3 - Compromised Devices - Botnet	51%	1	2.3	2	1	View Scenario Details
Smart Home & IoT 4 - Attacks on the Backend System	0%	0	0	3	0	View Scenario Details

Showing 1 to 10 of 14 entries

Previous 1 2 Next

Figure 19: Scenarios View

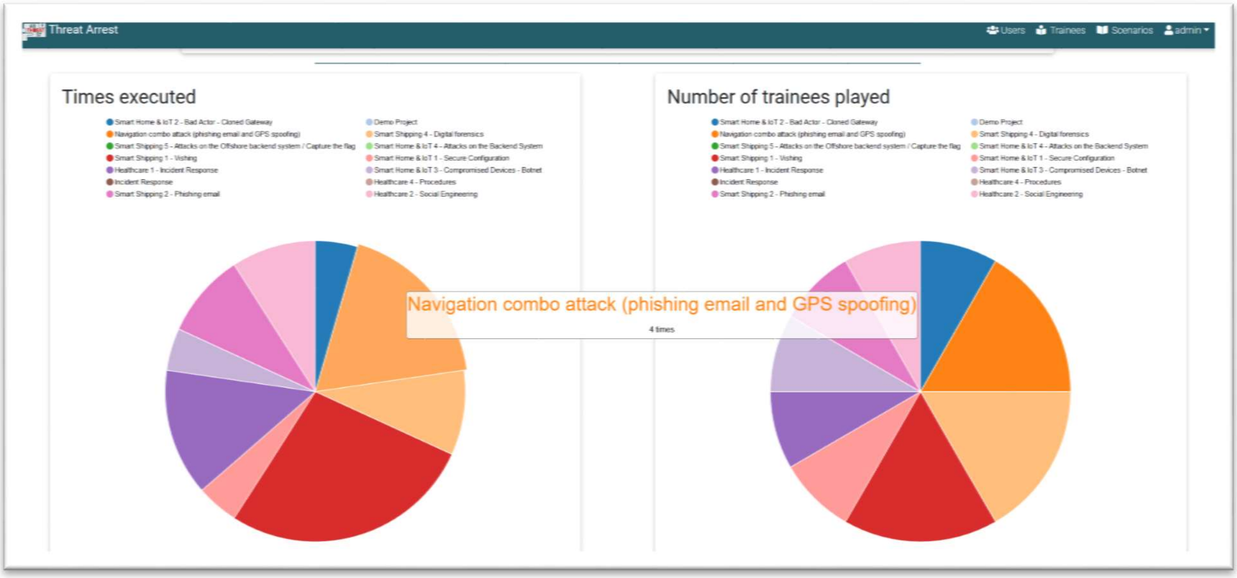
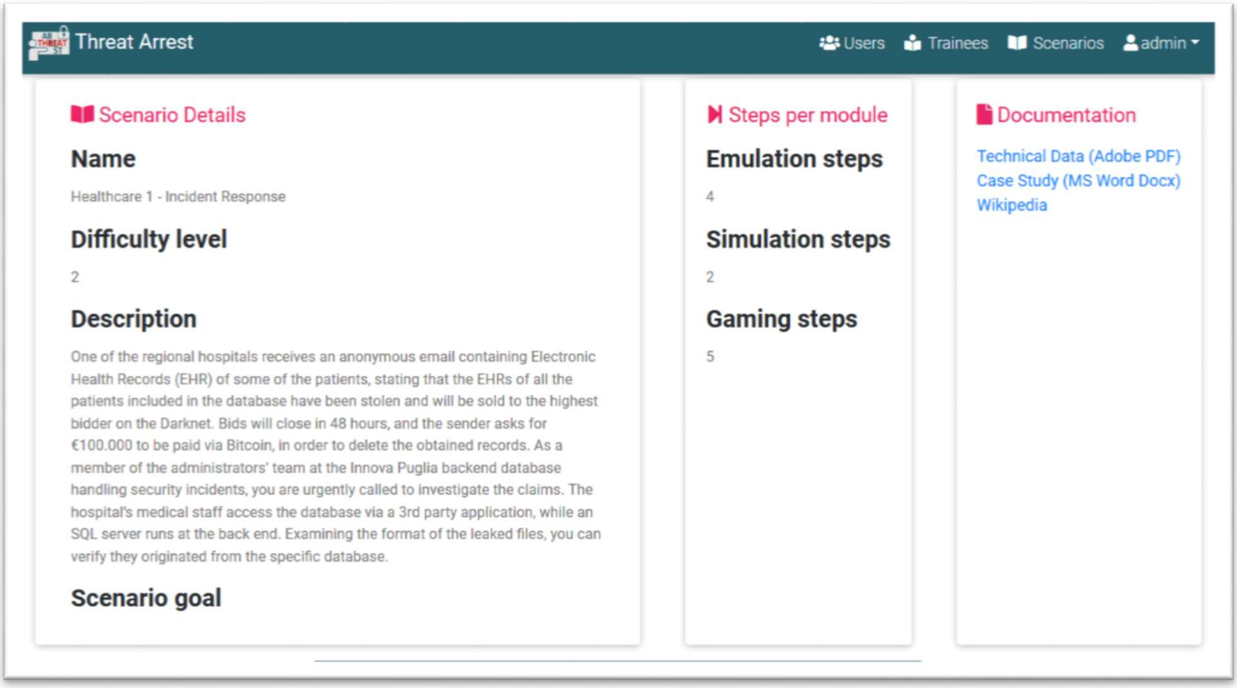

Threat Arrest
Users
Trainees
Scenarios
admin
Times executed
Smart Home & IoT 2 - Bad Actor - Cloned Gateway
Navigation combo attack (phishing email and GPS spoofing)
Smart Shipping 5 - Attacks on the Offshore backend system / Capture the flag
Smart Shipping 1 - Vishing
Healthcare 1 - Incident Response
Incident Response
Smart Shipping 2 - Phishing email
Demo Project
Smart Shipping 4 - Digital forensics
Smart Home & IoT 4 - Attacks on the Backend System
Smart Home & IoT 1 - Secure Configuration
Smart Home & IoT 3 - Compromised Devices - Botnet
Healthcare 4 - Procedures
Healthcare 2 - Social Engineering
Navigation combo attack (phishing email and GPS spoofing)
4 times
Number of trainees played
Smart Home & IoT 2 - Bad Actor - Cloned Gateway
Navigation combo attack (phishing email and GPS spoofing)
Smart Shipping 5 - Attacks on the Offshore backend system / Capture the flag
Smart Shipping 1 - Vishing
Healthcare 1 - Incident Response
Incident Response
Smart Shipping 2 - Phishing email
Demo Project
Smart Shipping 4 - Digital forensics
Smart Home & IoT 4 - Attacks on the Backend System
Smart Home & IoT 1 - Secure Configuration
Smart Home & IoT 3 - Compromised Devices - Botnet
Healthcare 4 - Procedures
Healthcare 2 - Social Engineering

Figure 20: Scenarios View Graphs

By clicking on *View Scenario Details* further information about a specific scenario is presented accompanied by statistical information and graphs.



Scenario Details

Name

Healthcare 1 - Incident Response

Difficulty level

2

Description

One of the regional hospitals receives an anonymous email containing Electronic Health Records (EHR) of some of the patients, stating that the EHRs of all the patients included in the database have been stolen and will be sold to the highest bidder on the Darknet. Bids will close in 48 hours, and the sender asks for €100.000 to be paid via Bitcoin, in order to delete the obtained records. As a member of the administrators' team at the Innova Puglia backend database handling security incidents, you are urgently called to investigate the claims. The hospital's medical staff access the database via a 3rd party application, while an SQL server runs at the back end. Examining the format of the leaked files, you can verify they originated from the specific database.

Scenario goal

Steps per module

Emulation steps

4

Simulation steps

2

Gaming steps

5

Documentation

Technical Data (Adobe PDF)
Case Study (MS Word Docx)
Wikipedia

Figure 21: Scenario Details

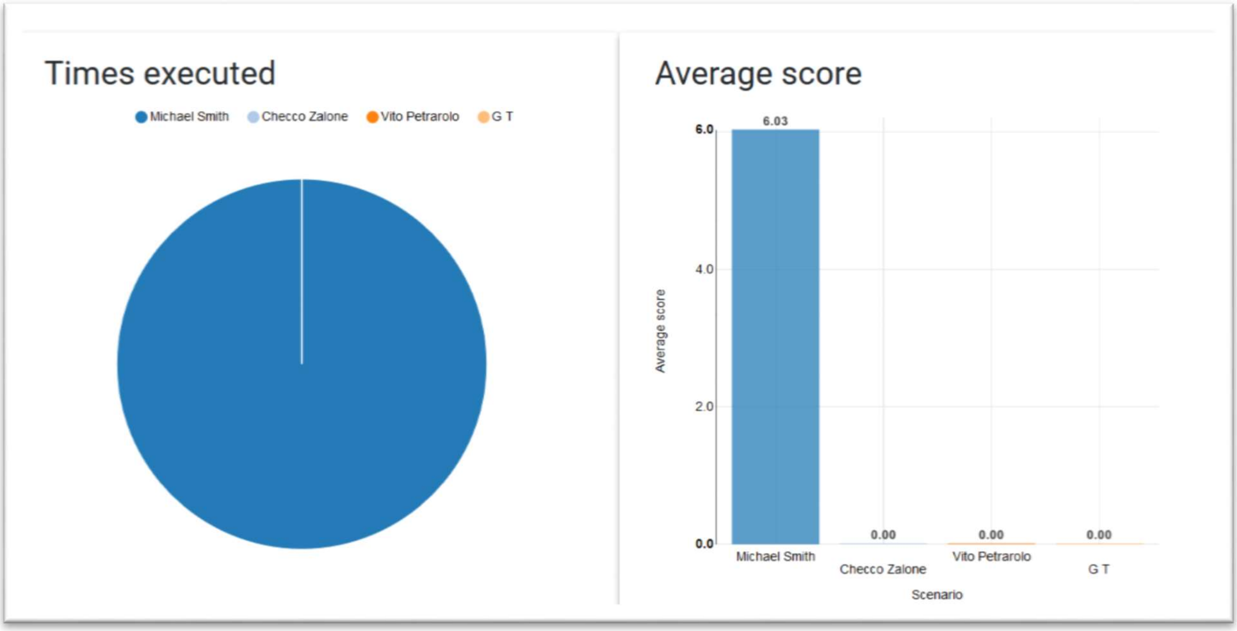
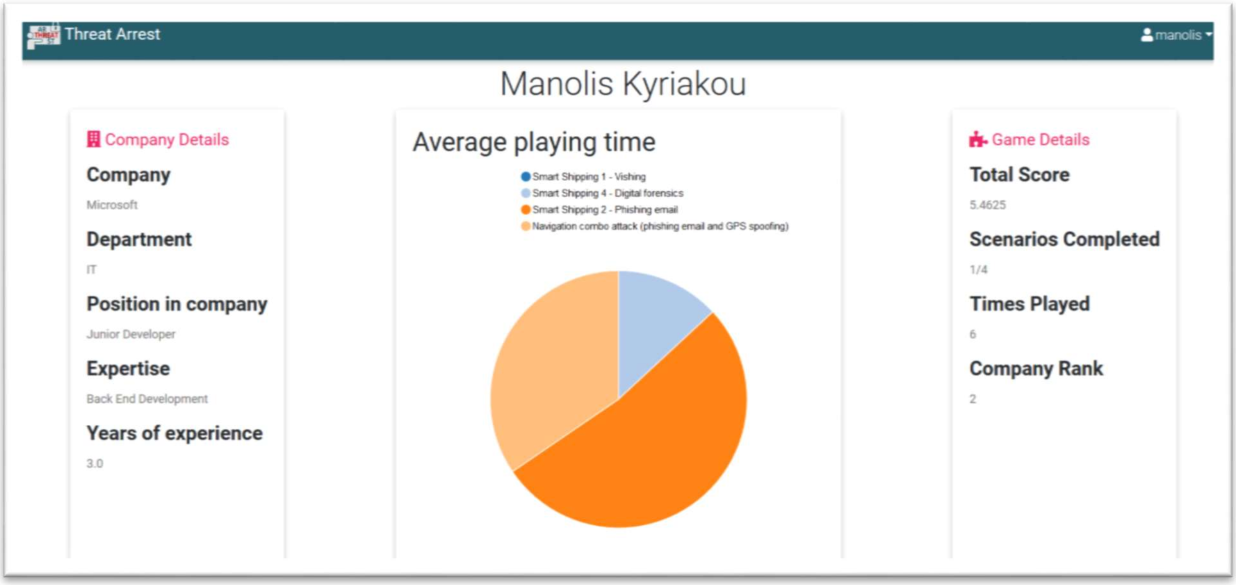


Figure 22: Scenario Graphs

4.1.4 Trainee Perspective

Upon successful login, trainees are presented with their profile's details, accompanied by information and graphs regarding their enabled scenario and past gameplays.


Threat Arrest
manolis
Average playing time
● Smart Shipping 1 - Vishing
● Smart Shipping 4 - Digital forensics
● Smart Shipping 2 - Phishing email
● Navigation combo attack (phishing email and GPS spoofing)

Manolis Kyriakou

Company Details

Company

Microsoft

Department

IT

Position in company

Junior Developer

Expertise

Back End Development

Years of experience

3.0

Game Details

Total Score

5.4625

Scenarios Completed

1/4

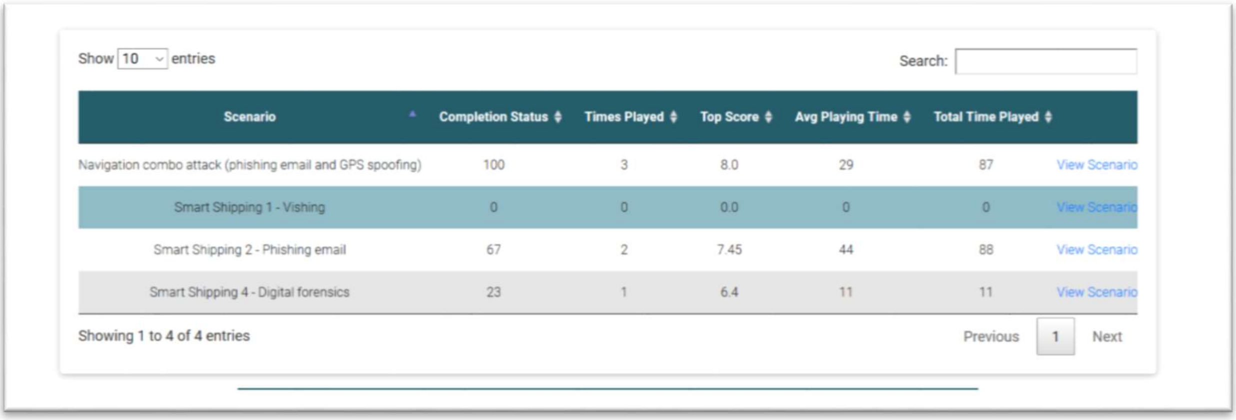
Times Played

6

Company Rank

2

Figure 23: Trainee's View



Show 10 entries

Search:

Scenario	Completion Status	Times Played	Top Score	Avg Playing Time	Total Time Played	
Navigation combo attack (phishing email and GPS spoofing)	100	3	8.0	29	87	View Scenario
Smart Shipping 1 - Vishing	0	0	0.0	0	0	View Scenario
Smart Shipping 2 - Phishing email	67	2	7.45	44	88	View Scenario
Smart Shipping 4 - Digital forensics	23	1	6.4	11	11	View Scenario

Showing 1 to 4 of 4 entries

Figure 24: Trainee's Scenario Info

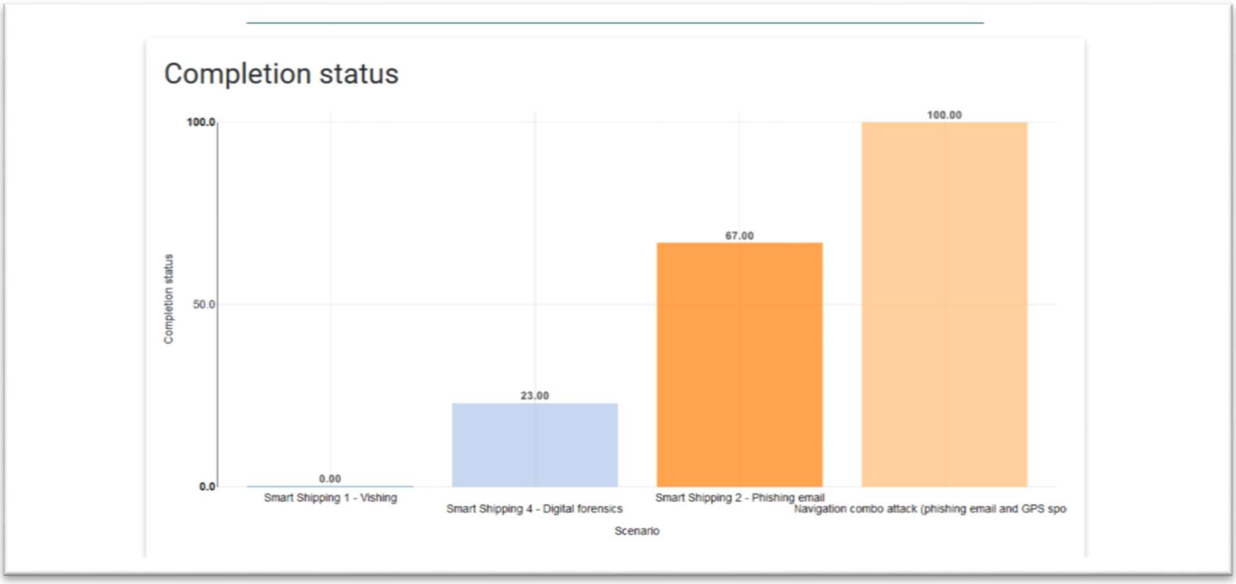
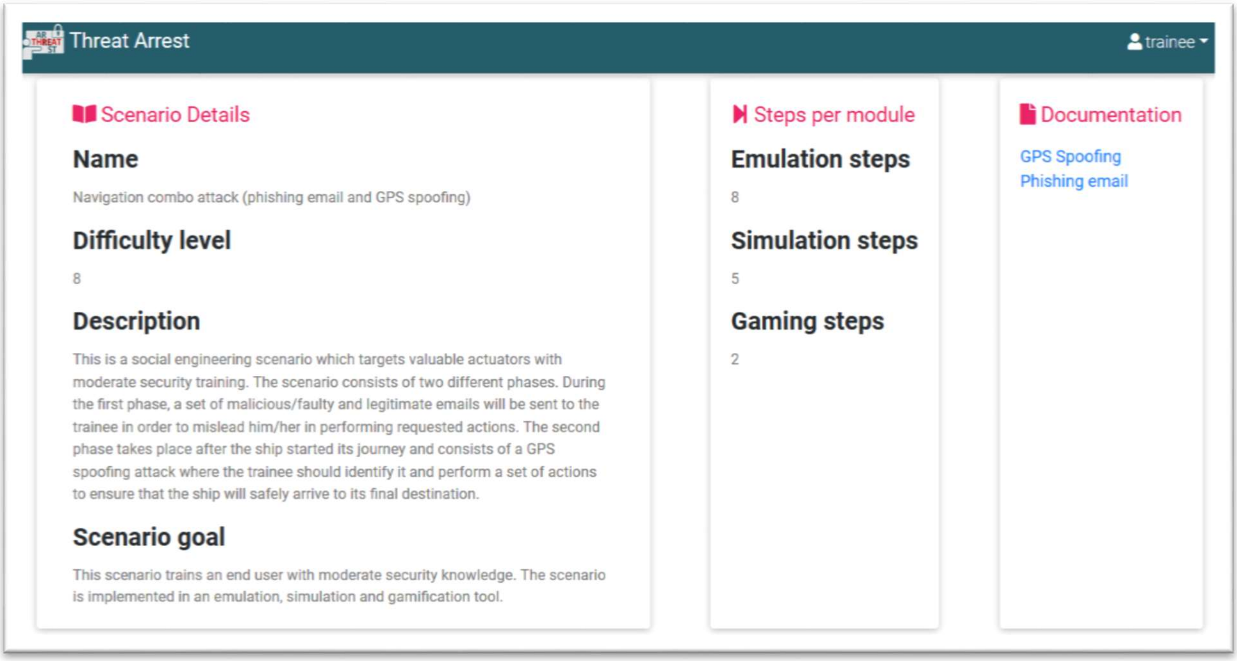


Figure 25: Trainee's Scenarios Graphs

4.1.4.1 Playing a Scenario

By selecting an individual scenario, trainees can view the scenario's detailed information, such as the scenario's Description, Difficulty Level, Goal, the number of steps per tool as well as relative documentation.



Scenario Details

Name

Navigation combo attack (phishing email and GPS spoofing)

Difficulty level

8

Description

This is a social engineering scenario which targets valuable actuators with moderate security training. The scenario consists of two different phases. During the first phase, a set of malicious/faulty and legitimate emails will be sent to the trainee in order to mislead him/her in performing requested actions. The second phase takes place after the ship started its journey and consists of a GPS spoofing attack where the trainee should identify it and perform a set of actions to ensure that the ship will safely arrive to its final destination.

Scenario goal

This scenario trains an end user with moderate security knowledge. The scenario is implemented in an emulation, simulation and gamification tool.

Steps per module

Emulation steps

8

Simulation steps

5

Gaming steps

2

Documentation

GPS Spoofing
Phishing email

Figure 26: Scenario View

At the bottom of the screen the trainees are presented with buttons to engage the individual tools.

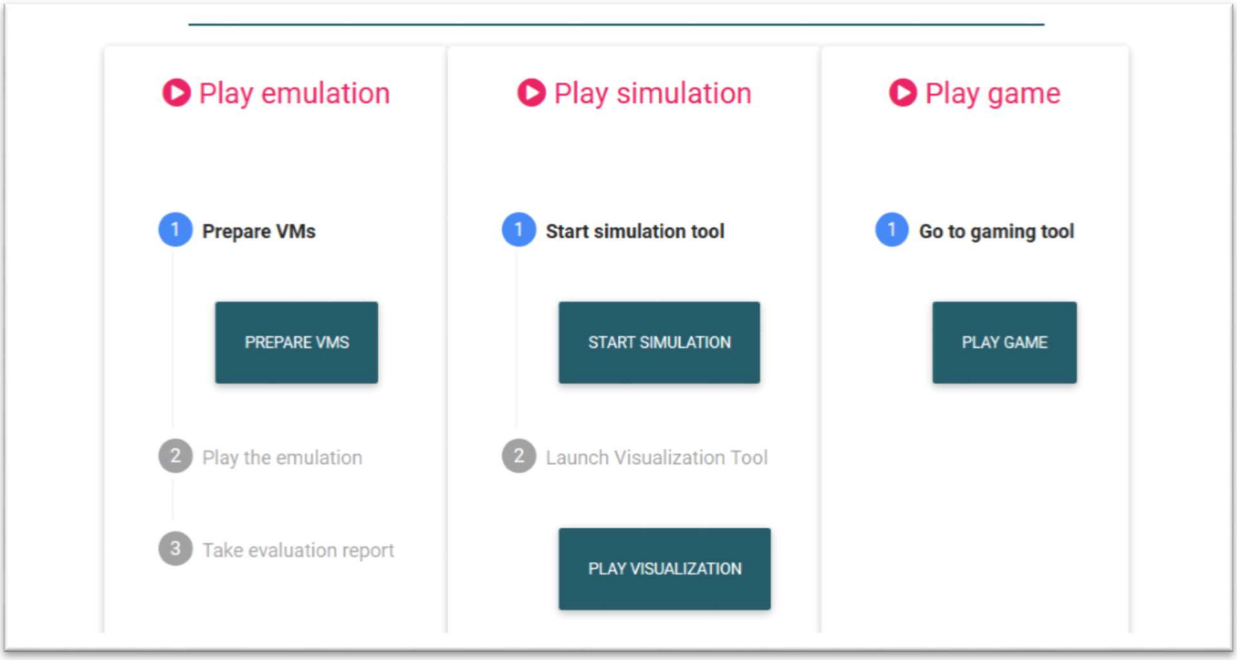


Figure 27: Individual Training Modalities View

4.1.4.2 Emulation Gameplay

To initialize the Emulation Tool environment, the trainees click on the *PREPARE VMS* button. After the environment has been prepared, the users are presented with button(s) to connect to the virtual machines, as well as a button *CLEAR ENVIRONMENT* to terminate the VMs to free resources again. Figure 28 shows the play emulation modality.

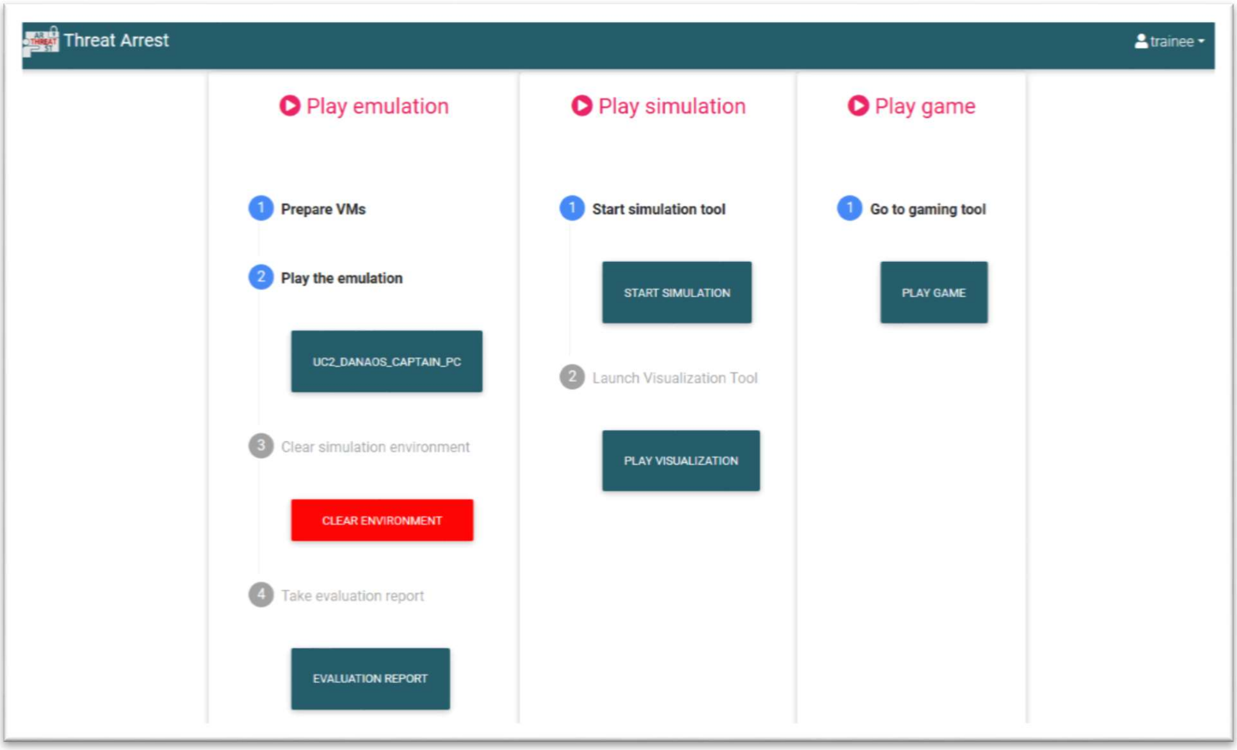
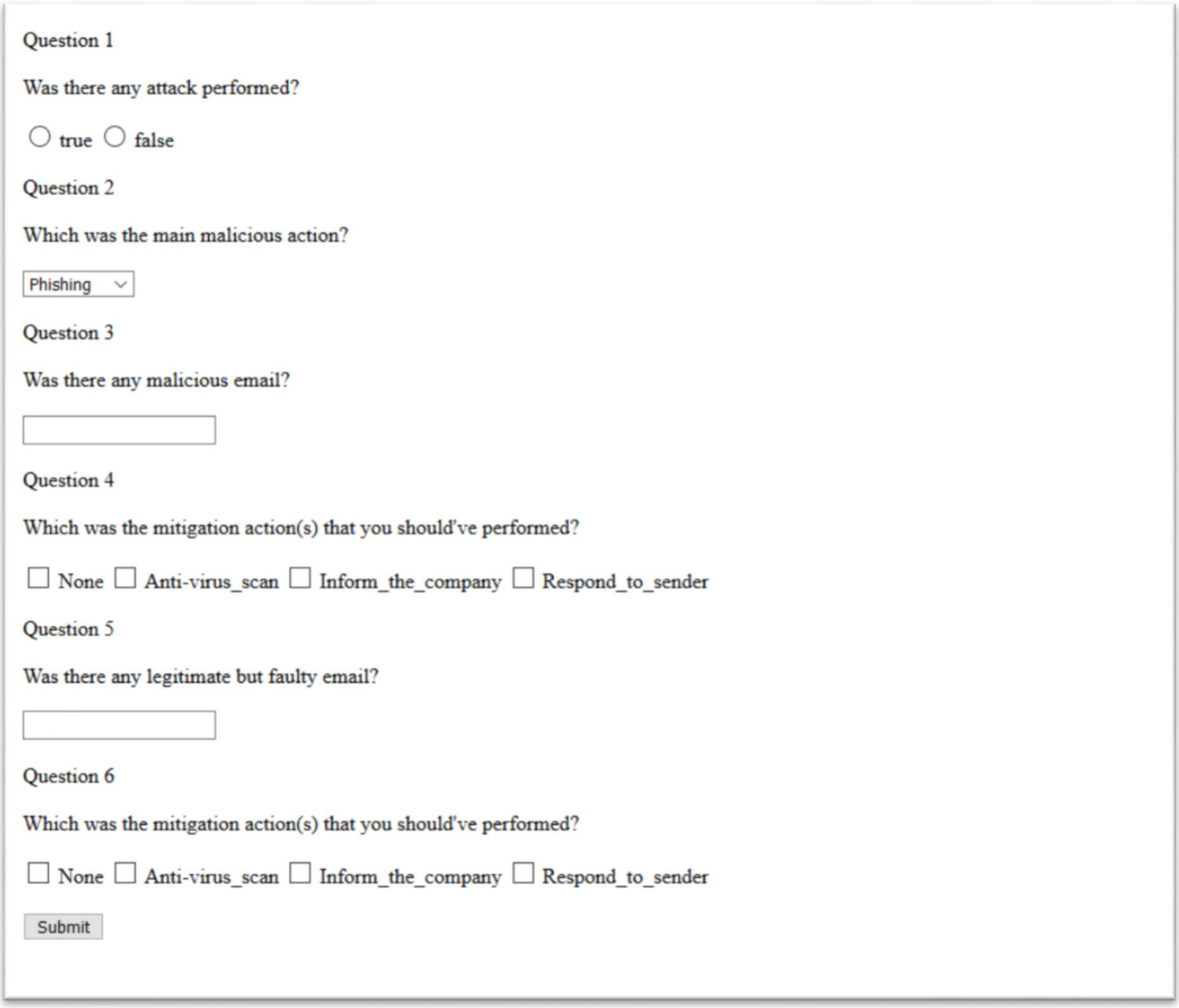


Figure 28: Play Emulation Training Modality View

After completing the Emulation part of the scenario, the users click on the *EVALUATION REPORT* and proceed to answer the respective questionnaire.



Question 1

Was there any attack performed?

○ true ○ false

Question 2

Which was the main malicious action?

Phishing

Question 3

Was there any malicious email?

Question 4

Which was the mitigation action(s) that you should've performed?

□ None □ Anti-virus_scan □ Inform_the_company □ Respond_to_sender

Question 5

Was there any legitimate but faulty email?

Question 6

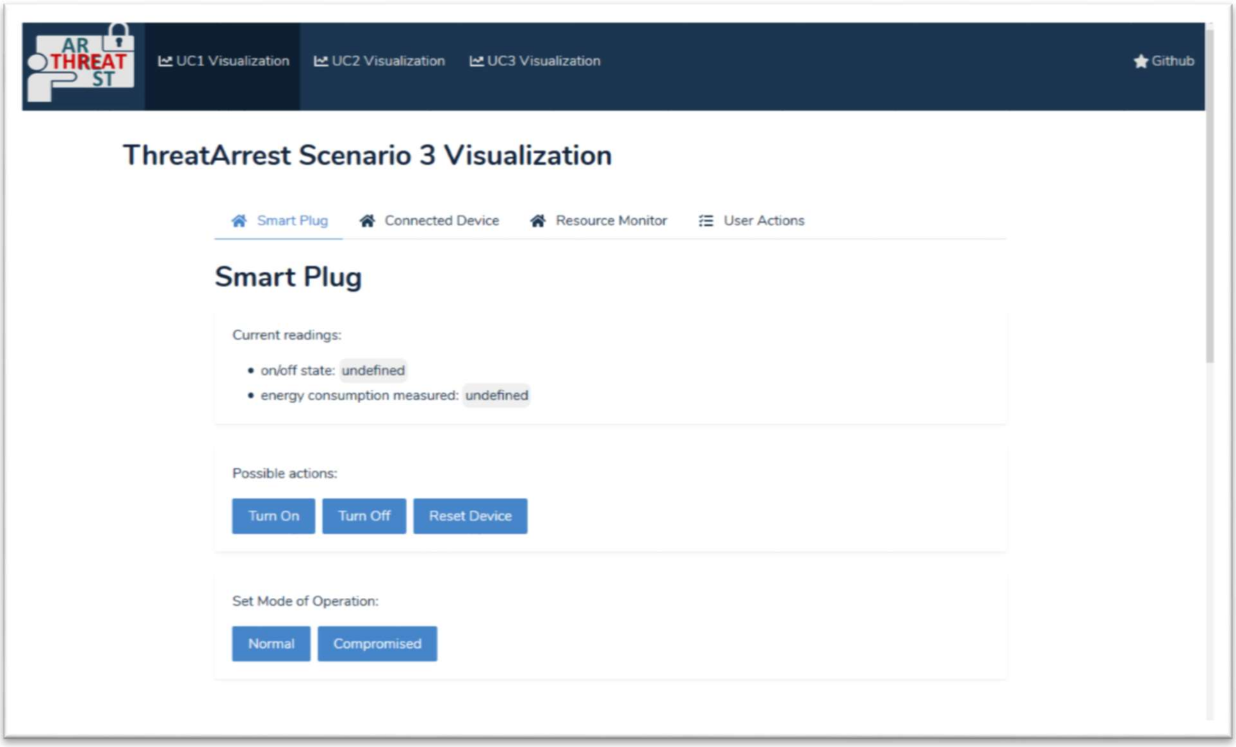
Which was the mitigation action(s) that you should've performed?

□ None □ Anti-virus_scan □ Inform_the_company □ Respond_to_sender

Figure 29: Emulation Tool Evaluation Report

4.1.4.3 Simulation Gameplay

To initialize the Simulation environment, trainees click on the *START SIMULATION* button and continue to access the Visualization Tool by clicking on the *PLAY VISUALIZATION* button.



ThreatArrest Scenario 3 Visualization

Smart Plug

Current readings:

- on/off state: undefined
- energy consumption measured: undefined

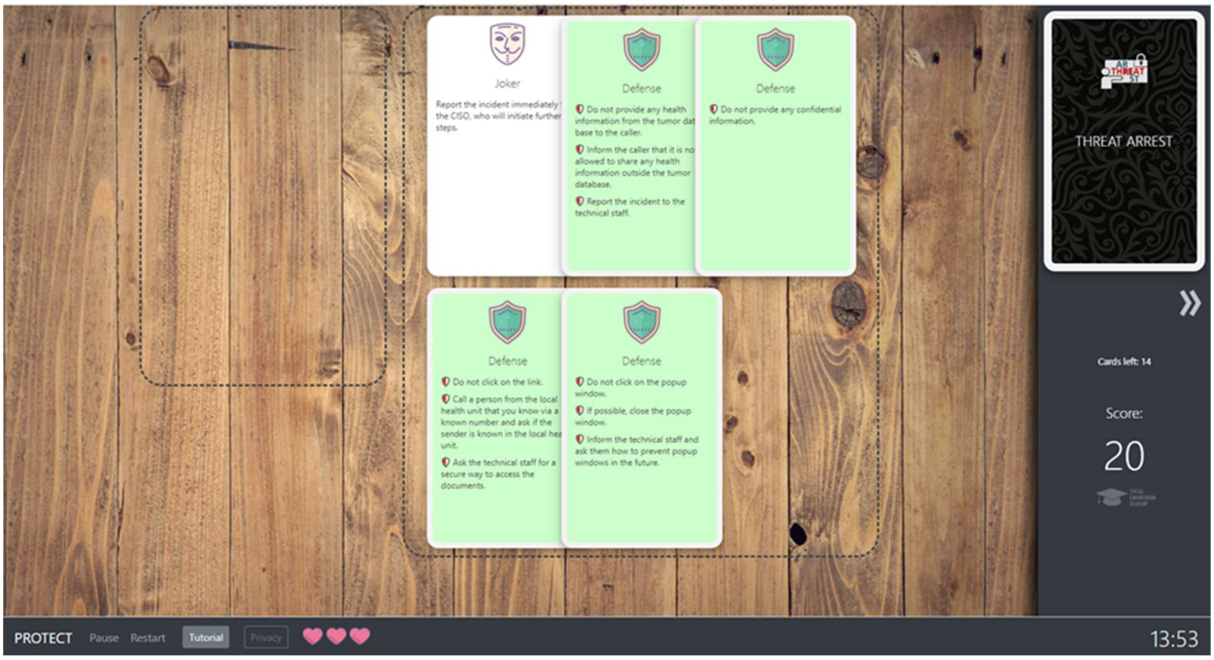
Possible actions:

Set Mode of Operation:

Figure 30: Visualization

4.1.4.4 Game Tool Gameplay

The user commences a Gaming section of a scenario by clicking on the *PLAY GAME* button after which a new tab is opened containing the Gaming Tool environment.



Joker

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

Defense

- Do not provide any health information from the tumor dat base to the caller.
- Inform the caller that it is no allowed to share any health information outside the tumor database.
- Report the incident to the technical staff.

Defense

- Do not provide any confidential information.

Defense

- Do not click on the link.
- Call a person from the local health unit that you know via a known number and ask if the sender is known in the local hea unit.
- Ask the technical staff for a secure way to access the documents.

Defense

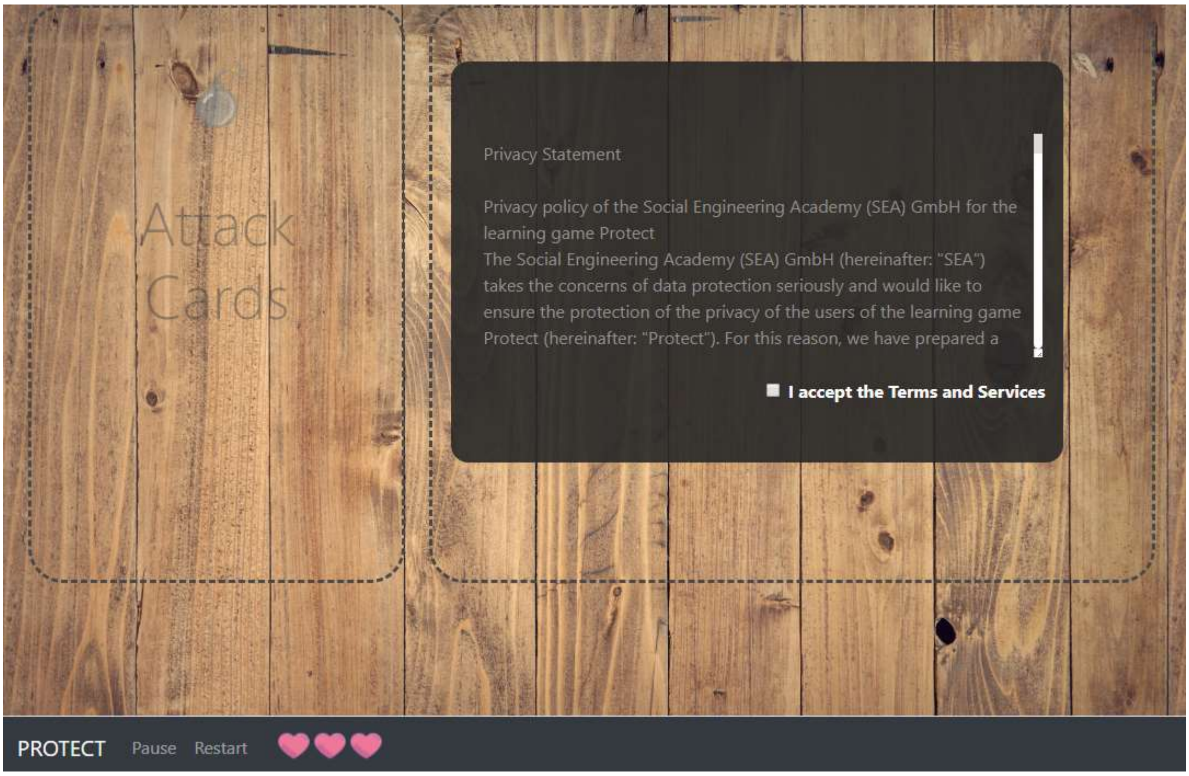
- Do not click on the popup window.
- If possible, close the popup window.
- Inform the technical staff and ask them how to prevent popup windows in the future.

Figure 31: Gaming Tool Environment

4.2 Gamification Tool Usage Guidelines

This section describes the usage regarding the user interface of the serious game PROTECT which is a part of the Gamification Tool. A detailed description of the concepts and rules of PROTECT is provided in the project deliverable “D4.2 THREAT-ARREST serious games v1”. A video of the Smart Home IoT use case in Table 6 can be used as guidelines of how to play the PROTECT game.

An instance of PROTECT is invoked in the Gamification Tool form the Training Tool. If the game is started by a certain trainee for the first time, he/she must accept the terms and services before the game starts (see Figure 32). The terms and services can be re-opened during a game by using the *Privacy* button in the bottom menu of the user interface (see Figure 33).



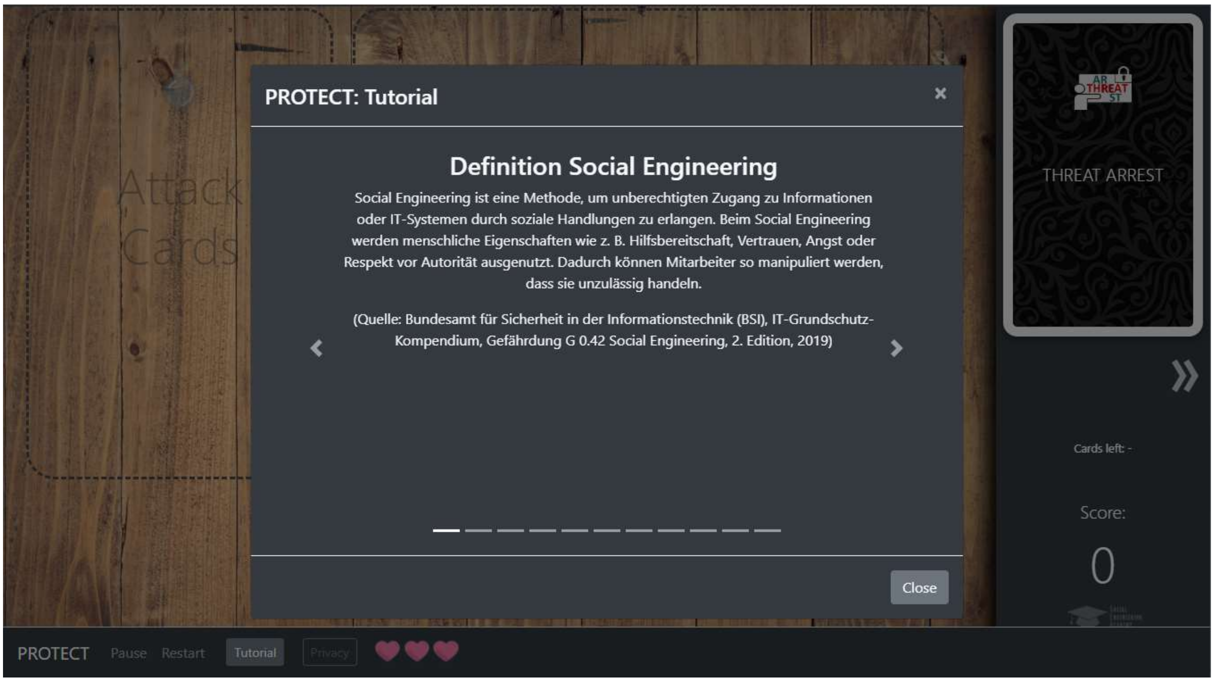
Privacy Statement

Privacy policy of the Social Engineering Academy (SEA) GmbH for the learning game Protect
The Social Engineering Academy (SEA) GmbH (hereinafter: "SEA") takes the concerns of data protection seriously and would like to ensure the protection of the privacy of the users of the learning game Protect (hereinafter: "Protect"). For this reason, we have prepared a

□ I accept the Terms and Services

Figure 32: Acceptance of terms and services

After the acceptance of the terms and services, a tutorial opens which explains the basics of social engineering and the rules of PROTECT (see Figure 33). The user can skip back and forth between the different pages by clicking on the corresponding arrows. The tutorial is closed by pressing the *Close* button. It can be reopened by the user during the game with help of the *Tutorial* button in the bottom menu (see Figure 33).



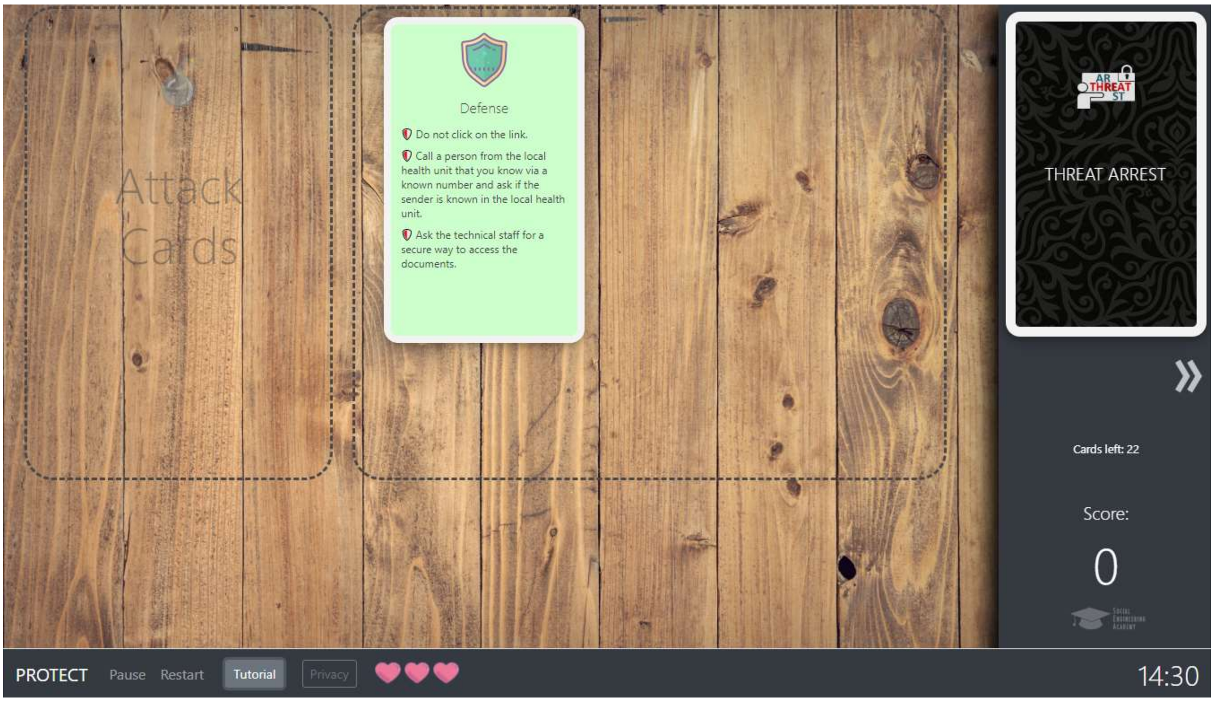
Definition Social Engineering

Social Engineering ist eine Methode, um unberechtigten Zugang zu Informationen oder IT-Systemen durch soziale Handlungen zu erlangen. Beim Social Engineering werden menschliche Eigenschaften wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt. Dadurch können Mitarbeiter so manipuliert werden, dass sie unzulässig handeln.

(Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutz-Kompendium, Gefährdung G 0.42 Social Engineering, 2. Edition, 2019)

Figure 33: Tutorial explaining PROTECT

After the tutorial has been closed, the game starts by drawing the first card automatically from the top of the card deck (see Figure 34). In subsequent games the trainee starts a game by drawing the first card manually. A card is drawn manually by clicking on the card deck in the top right corner of the user interface.



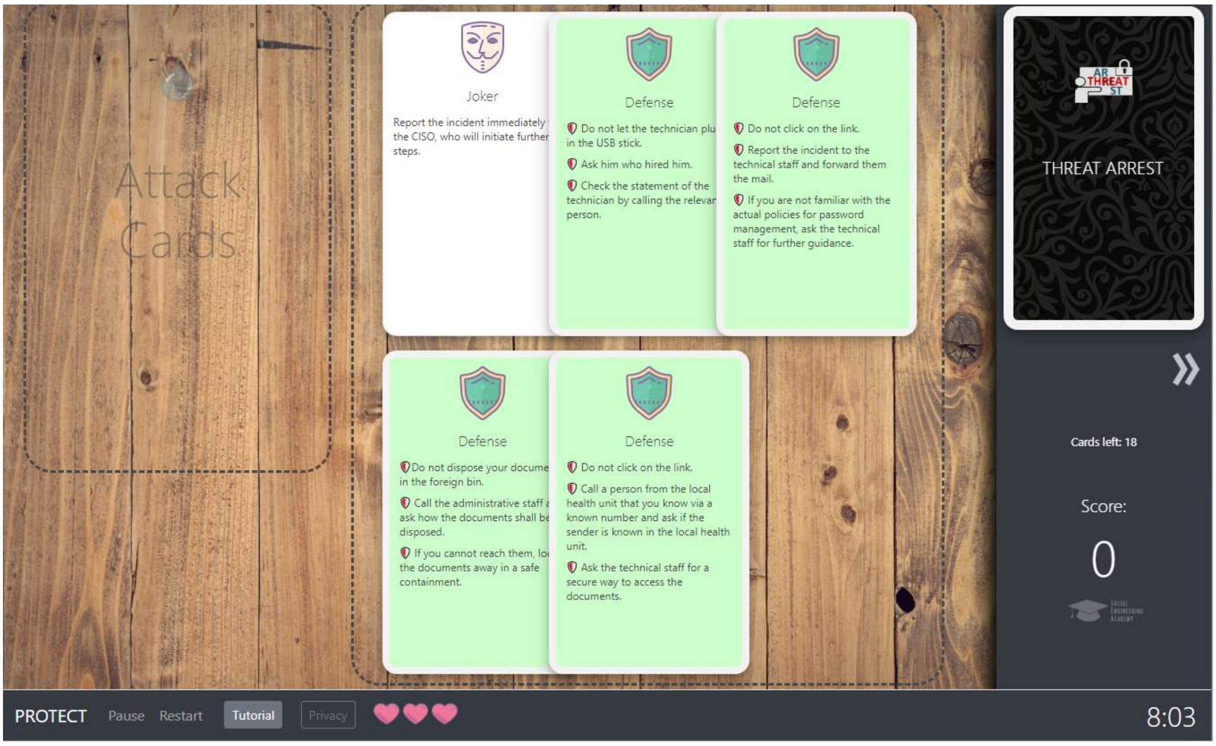
Do not click on the link.

Call a person from the local health unit that you know via a known number and ask if the sender is known in the local health unit.

Ask the technical staff for a secure way to access the documents.

Figure 34: Start of a game of PROTECT by drawing the first card

Now, the trainee draws further cards from the top of the card deck until an *Attack card* is drawn. Defense cards and Special action cards (Joker *cards, See-the-future cards, Skip-turn cards*) that have been drawn are placed on the hand of the user (see Figure 35). The hand of the trainee is represented by the area which is marked by a dotted line in the centre of the user interface.



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

- Do not let the technician plu in the USB stick.
- Ask him who hired him.
- Check the statement of the technician by calling the relevar person.

- Do not click on the link.
- Report the incident to the technical staff and forward them the mail.
- If you are not familiar with the actual policies for password management, ask the technical staff for further guidance.

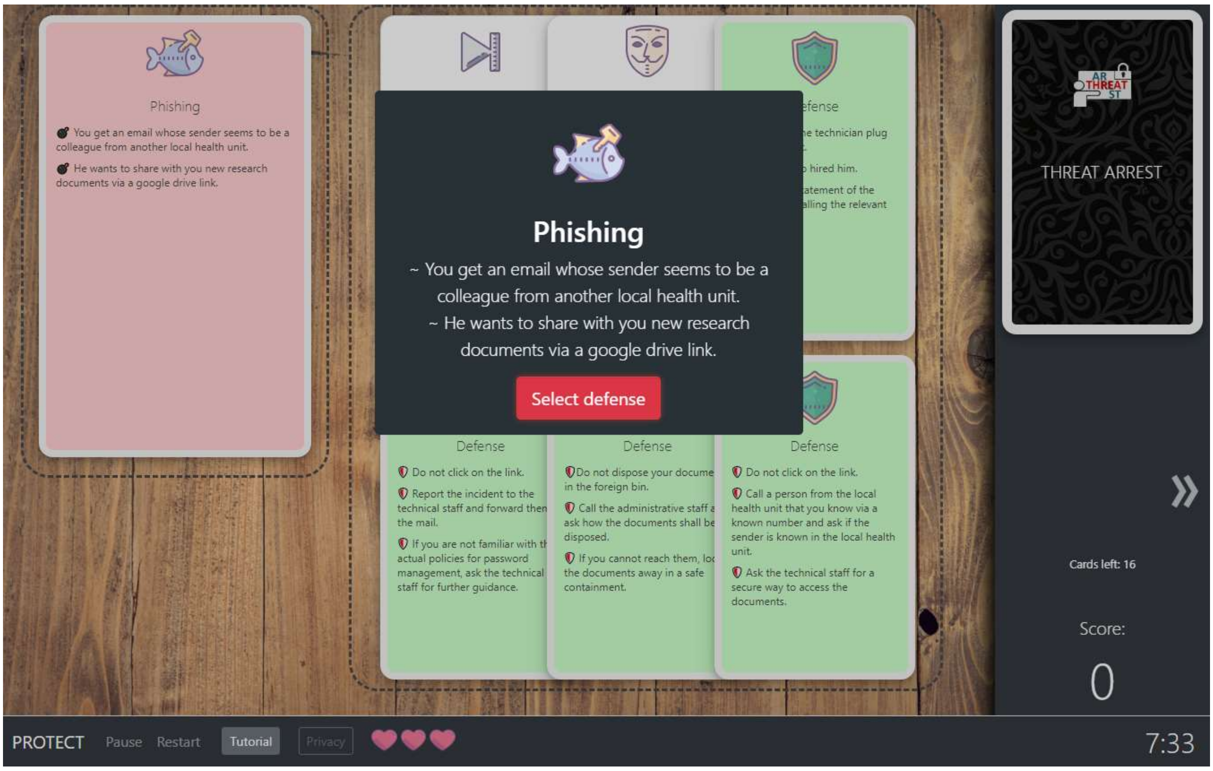
- Do not dispose your docume in the foreign bin.
- Call the administrative staff a ask how the documents shall be disposed.
- If you cannot reach them, lo the documents away in a safe containment.

- Do not click on the link.
- Call a person from the local health unit that you know via a known number and ask if the sender is known in the local health unit.
- Ask the technical staff for a secure way to access the documents.

Figure 35: Defense and Special action cards are placed on the hand of the user

If an *Attack card* is drawn, it is placed on the designated area top left in the user interface (see Figure 36). Additionally, a dialog opens which shows the content of the *Attack card*. After pressing the *Select defense* button the user has to select the correct *Defense card* from his/her hand which repeals the attack. If the trainee has a Joker card on the hand, he/she could also play this card to defend any Attack card. A card is selected by clicking on the designated card. The currently selected card is marked by a slightly tilted presentation in the user interface.

The selection of the correct *Defense card* or the playing of a *Joker card* is displayed by an appropriate dialog (see Figure 37). The game continues after the *Continue* button is clicked. If an attack has been defended correctly, the score which is displayed in the bottom right of the user interface is increased (see Figure 38).



Phishing

You get an email whose sender seems to be a colleague from another local health unit.

He wants to share with you new research documents via a google drive link.

Phishing

~ You get an email whose sender seems to be a colleague from another local health unit.
~ He wants to share with you new research documents via a google drive link.

Defense

Do not click on the link.
Report the incident to the technical staff and forward then the mail.
If you are not familiar with th actual policies for password management, ask the technical staff for further guidance.

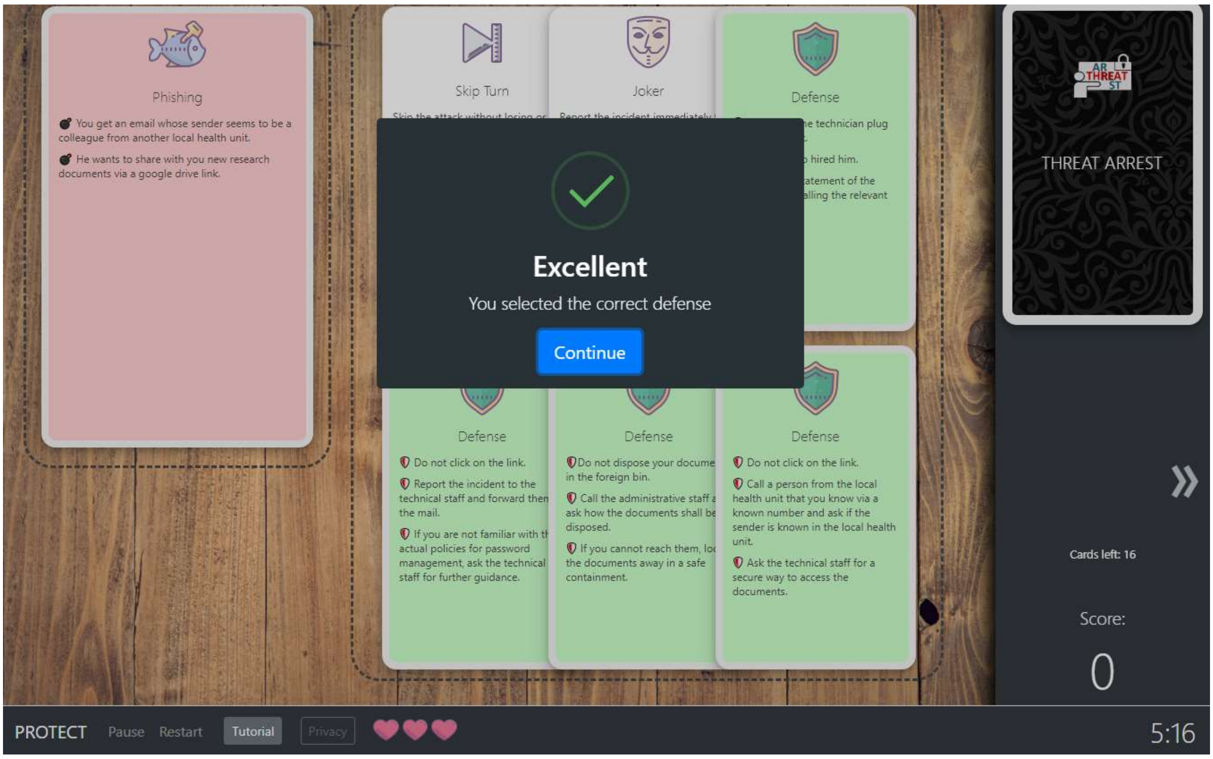
Defense

Do not dispose your docume in the foreign bin.
Call the administrative staff a ask how the documents shall be disposed.
If you cannot reach them, loc the documents away in a safe containment.

Defense

Do not click on the link.
Call a person from the local health unit that you know via a known number and ask if the sender is known in the local health unit.
Ask the technical staff for a secure way to access the documents.

Figure 36: Drawing of an Attack card

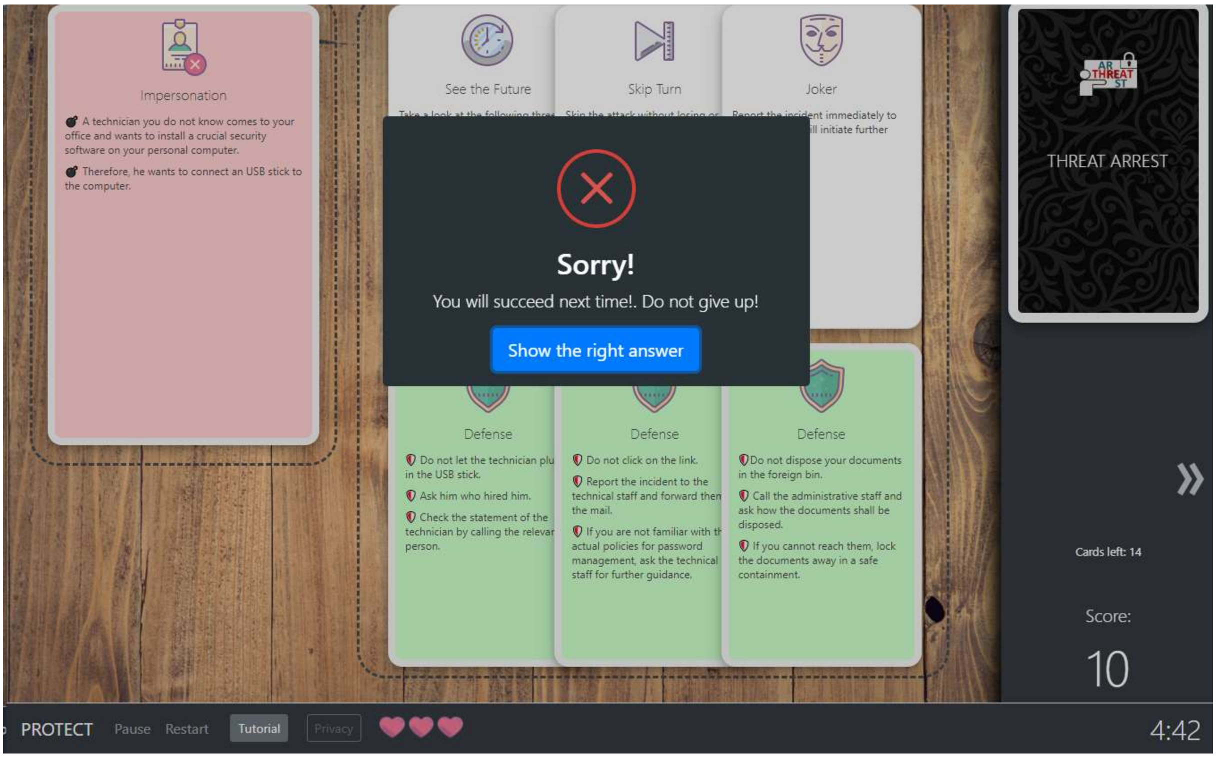


Excellent

You selected the correct defense

Figure 37: Dialog after a successful defense of an Attack card

The selection of an incorrect *Defense card* for an *Attack card* is displayed by a corresponding dialog (see Figure 38). After pressing the *Show the right answer*button another dialog shows the correct defense (see Figure 39). The game continues when the *Continue*button is pressed.



Impersonation

A technician you do not know comes to your office and wants to install a crucial security software on your personal computer.

Therefore, he wants to connect an USB stick to the computer.

See the Future

Take a look at the following three

Skip Turn

Skip the attack without losing or

Joker

Report the incident immediately to ... ill initiate further

Sorry!

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

Defense

Do not let the technician plu in the USB stick.

Ask him who hired him.

Check the statement of the technician by calling the relevar person.

Defense

Do not click on the link.

Report the incident to the technical staff and forward then the mail.

If you are not familiar with th actual policies for password management, ask the technical staff for further guidance.

Defense

Do not dispose your documents in the foreign bin.

Call the administrative staff and ask how the documents shall be disposed.

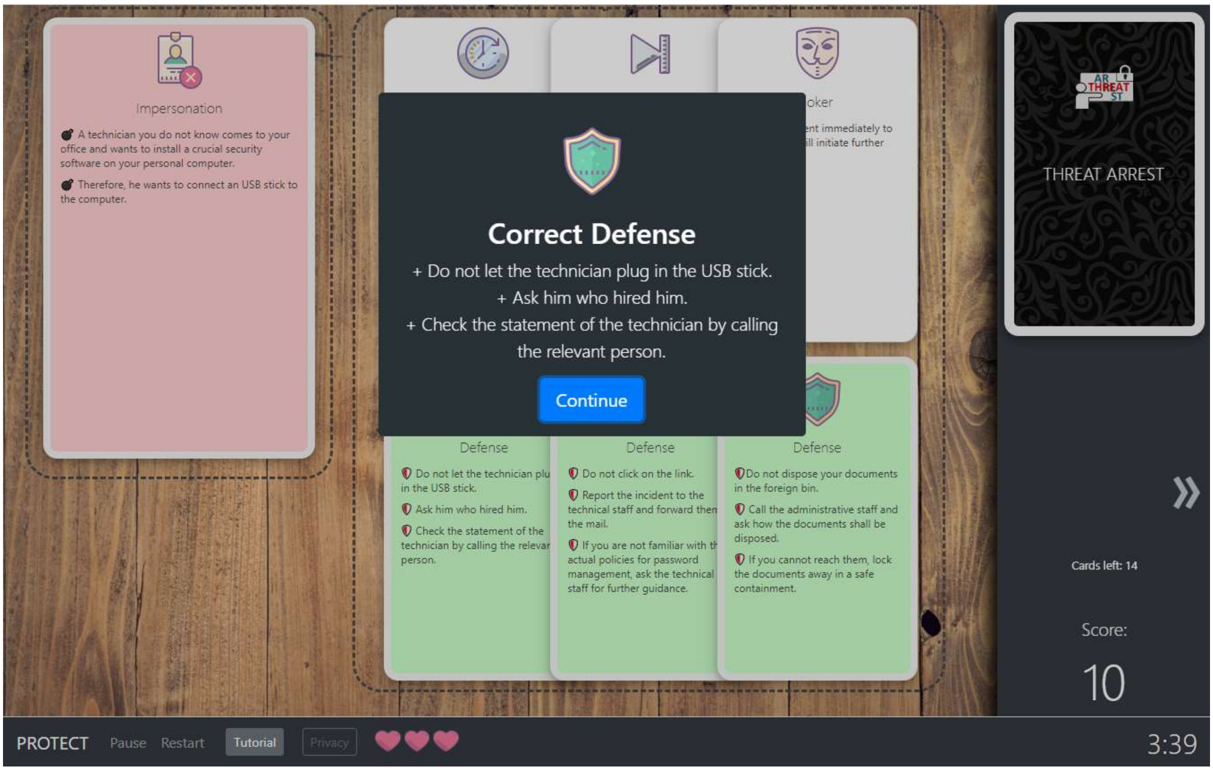
If you cannot reach them, lock the documents away in a safe containment.

Cards left: 14

Score:

10

Figure 38: Dialog after a selection of an incorrect Defense card



Impersonation

A technician you do not know comes to your office and wants to install a crucial security software on your personal computer.

Therefore, he wants to connect an USB stick to the computer.

oker

ent immediately to ... ill initiate further

Correct Defense

+ Do not let the technician plug in the USB stick.
+ Ask him who hired him.
+ Check the statement of the technician by calling the relevant person.

Defense

Do not let the technician plu in the USB stick.

Ask him who hired him.

Check the statement of the technician by calling the relevar person.

Defense

Do not click on the link.

Report the incident to the technical staff and forward then the mail.

If you are not familiar with th actual policies for password management, ask the technical staff for further guidance.

Defense

Do not dispose your documents in the foreign bin.

Call the administrative staff and ask how the documents shall be disposed.

If you cannot reach them, lock the documents away in a safe containment.

Cards left: 14

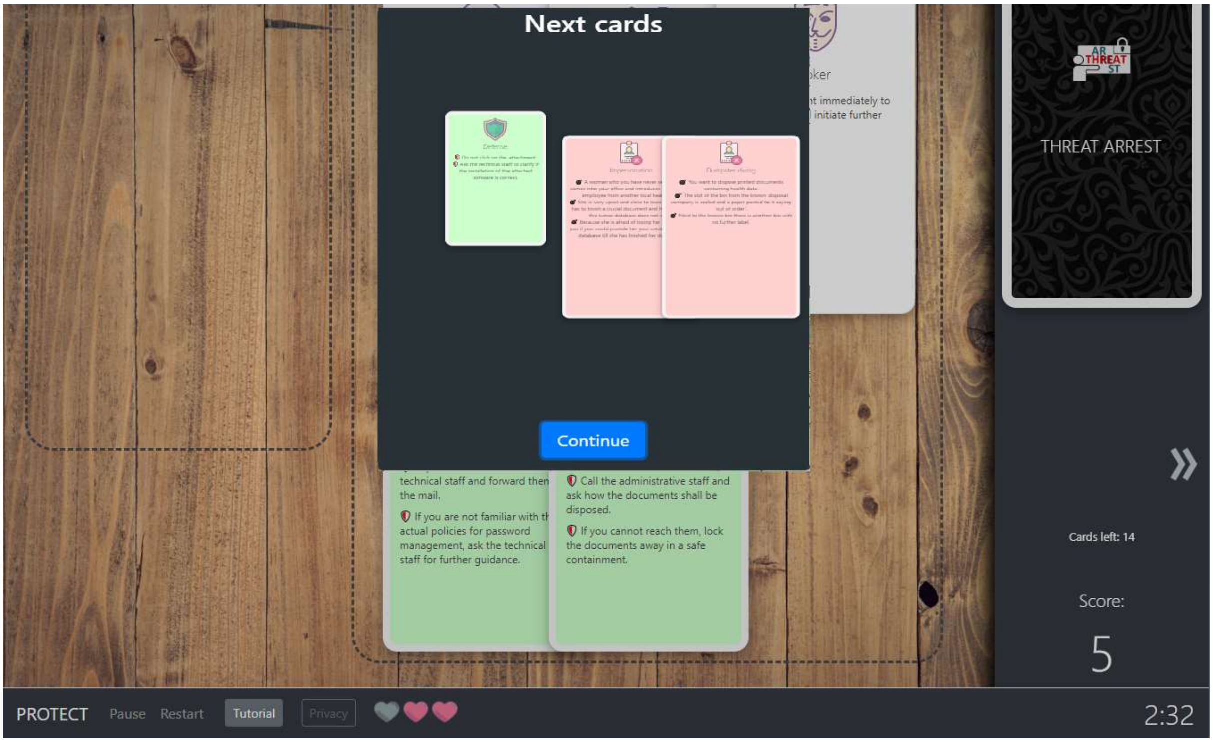
Score:

10

Figure 39: Dialog displays the correct defense after the selection of an incorrect Defense card

After an incorrect defense, the score displayed in the bottom right in the user interface is decreased (see Figure 40). Additionally, the trainee loses one life. The lives are represented by the heart symbols in the bottom menu (see Figure 40).

The playing of a *See-the-future card* from the trainee’s hand opens a dialog which displays the next three cards on the top of the deck (see Figure 40). If these cards should contain an *Attack* *card* for which the user cannot associate the appropriate *Defense card*, the trainee could play a *Skip-turn card* in the corresponding turn (see Figure 41). By this, he/she could skip the *Attack card* from the card deck and prevent the loss of a life. The game continues after the *Continue* button is pressed.



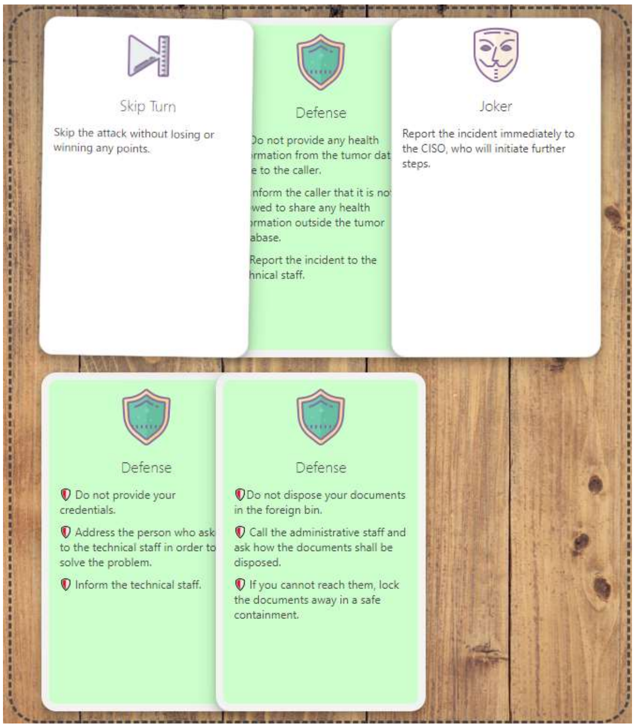
technical staff and forward then the mail.

If you are not familiar with th actual policies for password management, ask the technical staff for further guidance.

Call the administrative staff and ask how the documents shall be disposed.

If you cannot reach them, lock the documents away in a safe containment.

Figure 40: Playing of a See-the-future card



Skip the attack without losing or winning any points.

Do not provide any health rmation from the tumor dat e to the caller.

nform the caller that it is no wed to share any health rmation outside the tumor abase.

Report the incident to the hnical staff.

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

Do not provide your credentials.

Address the person who ask to the technical staff in order to solve the problem.

Inform the technical staff.

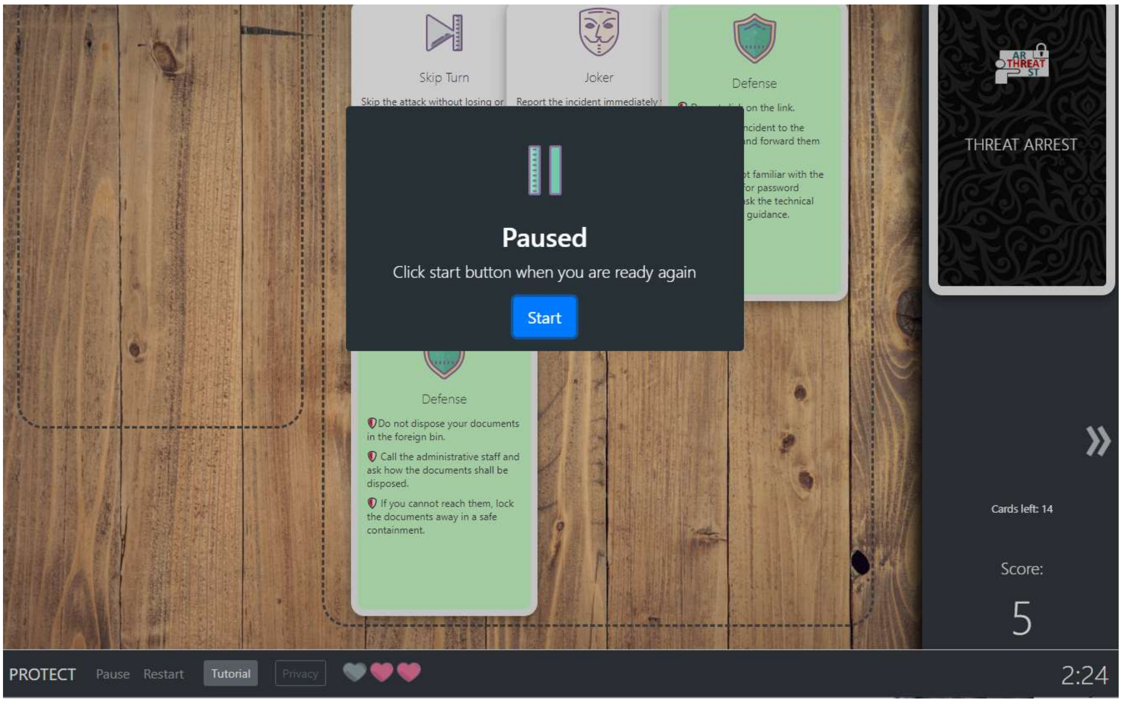
Do not dispose your documents in the foreign bin.

Call the administrative staff and ask how the documents shall be disposed.

If you cannot reach them, lock the documents away in a safe containment.

Figure 41: Playing of a Skip-turn card to skip the top card on the card deck

A game can also be paused by a trainee with the help of the *Pause* button in the bottom menu (see Figure 42). After this button has been pressed, a corresponding dialog is displayed (see Figure 42). The user can continue the game by clicking on the *Start* button.



Paused

Click start button when you are ready again

Defense

Do not dispose your documents in the foreign bin.

Call the administrative staff and ask how the documents shall be disposed.

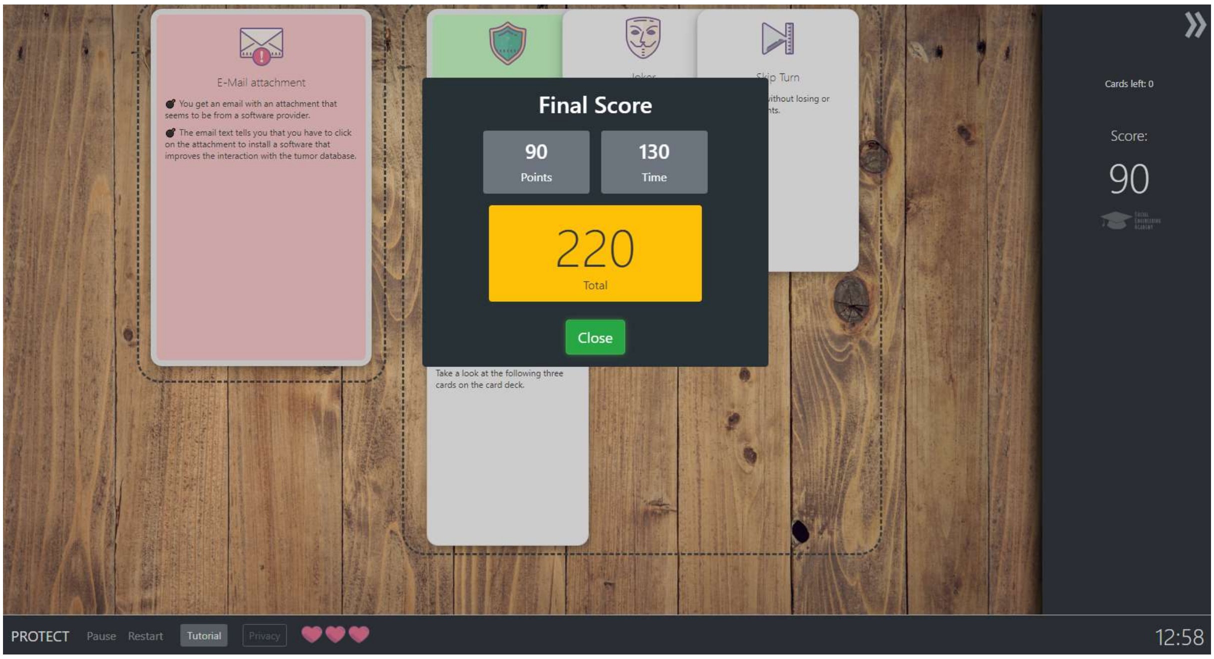
If you cannot reach them, lock the documents away in a safe containment.

Cards left: 14

Score: 5

Figure 42: Pausing of the game

A game of PROTECT is won if the trainee empties the card deck in the predetermined time. After a successful game, a dialog displays the final score (see Figure 43). The clicking of the *Close* button entails the closing of the Gamification Tool and the direction of the trainee back to the Training Tool.



E-Mail attachment

You get an email with an attachment that seems to be from a software provider.

The email text tells you that you have to click on the attachment to install a software that improves the interaction with the tumor database.

Final Score

90 Points

130 Time

220 Total

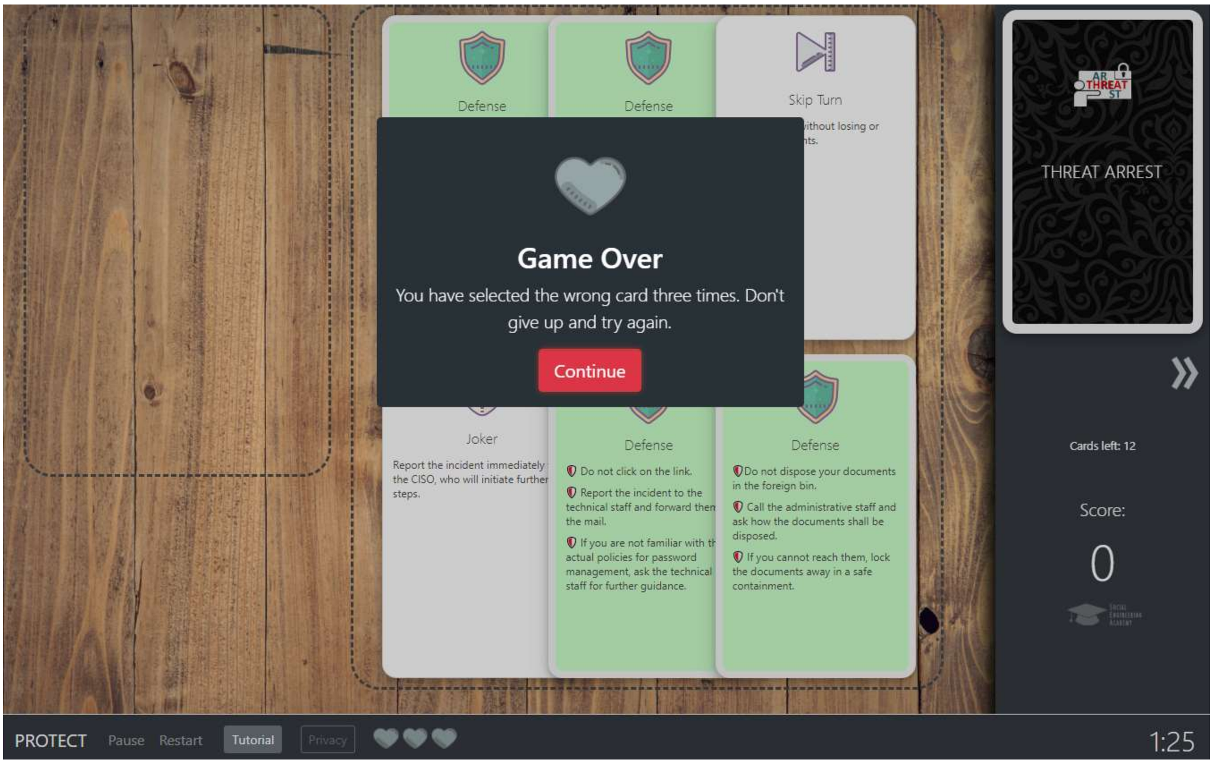
Take a look at the following three cards on the card deck.

Cards left: 0

Score: 90

Figure 43: Representation of the final score after a game has been won

If the trainee has lost all his/her lives or the time has been expired before the card deck was emptied, the trainee has lost the game. This situation is displayed by a corresponding dialog (see Figure 44 and Figure 45). After clicking on the *Continue* button the Gamification Tool is closed and the user is directed back to the Training Tool.



Game Over

You have selected the wrong card three times. Don't give up and try again.

Continue

Joker

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

Defense

- Do not click on the link.
- Report the incident to the technical staff and forward then the mail.
- If you are not familiar with th actual policies for password management, ask the technical staff for further guidance.

Defense

- Do not dispose your documents in the foreign bin.
- Call the administrative staff and ask how the documents shall be disposed.
- If you cannot reach them, lock the documents away in a safe containment.

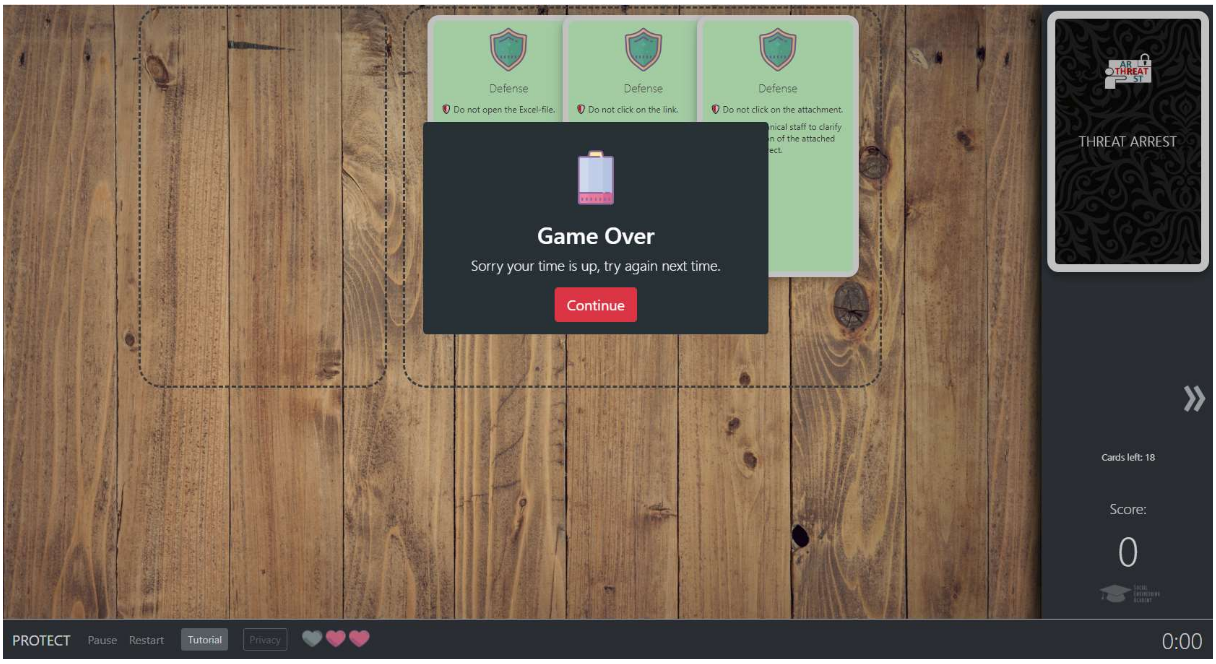
Cards left: 12

Score:

0

1:25

Figure 44: "Game Over"-Dialog after a game has been lost because the loss of all lives



Defense

- Do not open the Excel-file.

Defense

- Do not click on the link.

Defense

- Do not click on the attachment.

Game Over

Sorry your time is up, try again next time.

Continue

Cards left: 18

Score:

0

0:00

Figure 45: Dialog after losing a game because the time has been expired

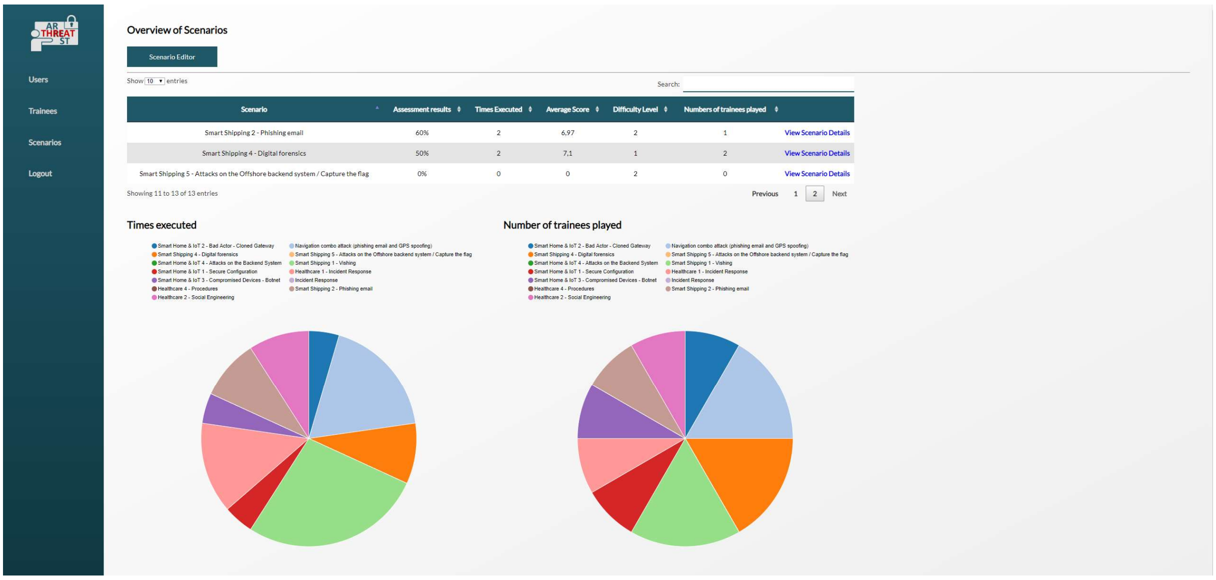
4.3 CTTP Model Editor Usage Guidelines

The video of the CTTP model editor in Table 6 can be used as guidelines of how to use the GUI of the editor. In the following, we present the main functionality of the editor.

4.3.1 Main Components

In order to utilise the CTTP Model Editor, a THREAT-ARREST user will first need to login to the Training Tool.

Following the successful login, the user will be presented with a button that will redirect him/her to the CTTP Model Editor GUI (see Figure 46).

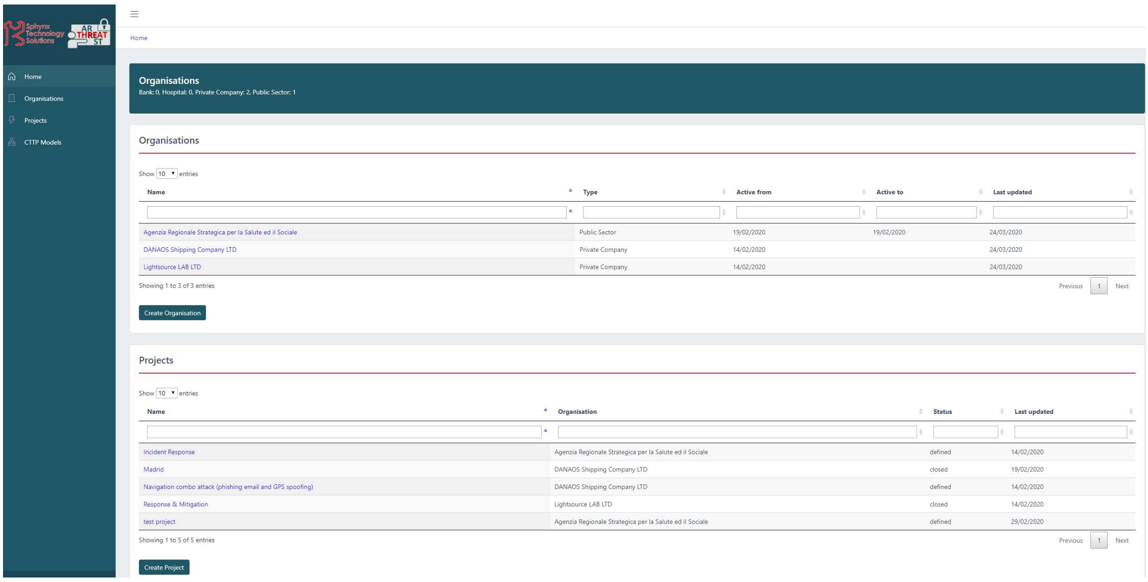

Users
Trainees
Scenarios
Logout
Overview of Scenarios
Scenario Editor
Show 10 entries
Search:
Times executed
Number of trainees played
Smart Home & IoT 2 - Bad Actor - Cloned Gateway
Smart Shipping 4 - Digital forensics
Smart Home & IoT 4 - Attacks on the Backend System
Smart Home & IoT 1 - Secure Configuration
Smart Home & IoT 3 - Compromised Devices - Botnet
Healthcare 4 - Procedures
Healthcare 2 - Social Engineering
Navigation combo attack (phishing email and GPS spoofing)
Smart Shipping 5 - Attacks on the Offshore backend system / Capture the flag
Smart Shipping 1 - Vishing
Healthcare 1 - Incident Response
Incident Response
Smart Shipping 2 - Phishing email

Scenario	Assessment results	Times Executed	Average Score	Difficulty Level	Numbers of trainees played	
Smart Shipping 2 - Phishing email	60%	2	6,97	2	1	View Scenario Details
Smart Shipping 4 - Digital forensics	50%	2	7,1	1	2	View Scenario Details
Smart Shipping 5 - Attacks on the Offshore backend system / Capture the flag	0%	0	0	2	0	View Scenario Details

Showing 11 to 13 of 13 entries

Figure 46: Scenario Editor

The welcome screen of the Editor provides the aggregated information (see Figure 47) regarding the existing organisations and projects (if any).



Organisations
Bank: 0, Hospital: 0, Private Company: 2, Public Sector: 1

Organisations

Name	Type	Active from	Active to	Last updated
Agenzia Regionale Strategica per la Salute ed il Sociale	Public Sector	19/02/2020	19/02/2020	24/03/2020
DANAOS Shipping Company LTD	Private Company	14/02/2020		24/03/2020
Lightsource LAB LTD	Private Company	14/02/2020		24/03/2020

Showing 1 to 3 of 3 entries

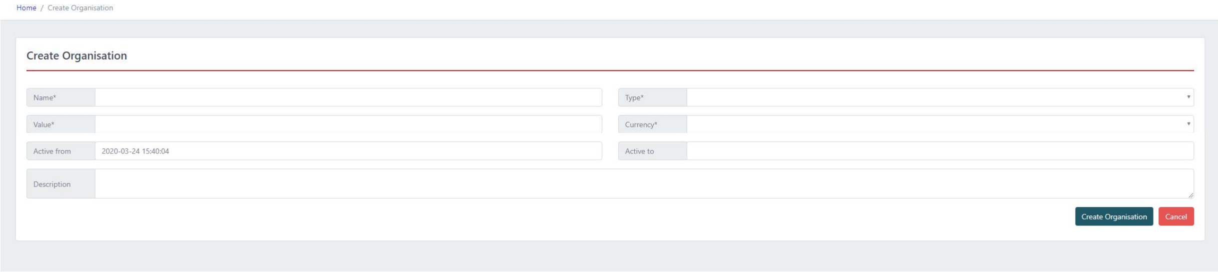
Projects

Name	Organisation	Status	Last updated
Incident Response	Agenzia Regionale Strategica per la Salute ed il Sociale	defined	14/02/2020
Madrid	DANAOS Shipping Company LTD	closed	19/02/2020
Navigation combo attack (phishing email and GPS spoofing)	DANAOS Shipping Company LTD	defined	14/02/2020
Response & Mitigation	Lightsource LAB LTD	closed	14/02/2020
test project	Agenzia Regionale Strategica per la Salute ed il Sociale	defined	29/02/2020

Showing 1 to 5 of 5 entries

Figure 47: Aggregated Information

The administrator can choose to create a new organization (see Figure 48) or edit/view an existing one (see Figure 49).

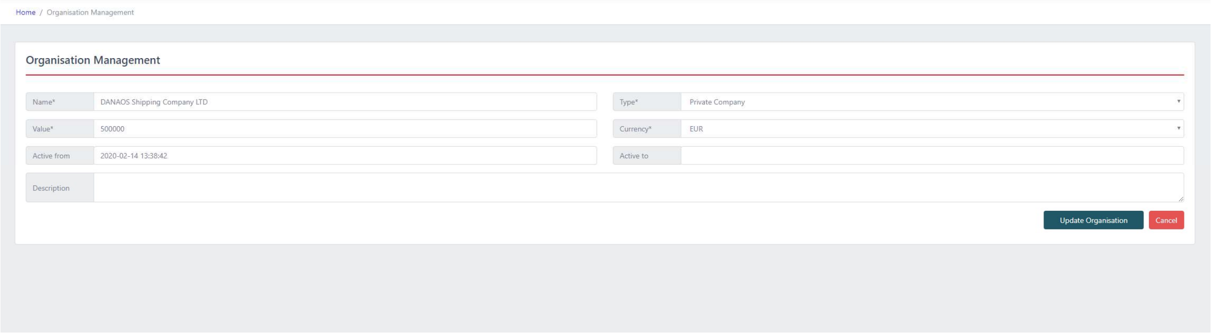


Home / Create Organisation

Create Organisation

Name*		Type*	
Value*		Currency*	
Active from	2020-03-24 15:40:04	Active to	
Description			

Figure 48 Create a new organisation



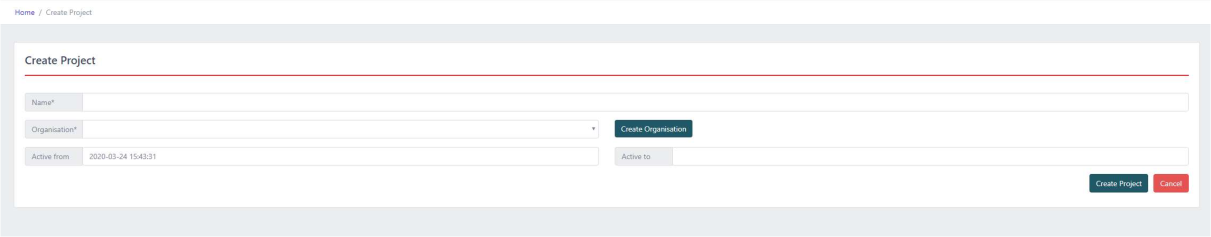
Home / Organisation Management

Organisation Management

Name*	DANAOS Shipping Company LTD	Type*	Private Company
Value*	500000	Currency*	EUR
Active from	2020-02-14 13:38:42	Active to	
Description			

Figure 49: Edit/View an existing organization

Each organisation is correlated with a number of projects. The administrator can choose to create a new project and assign it to an existing organisation (see Figure 50) or edit/view an existing one (see Figure 51).

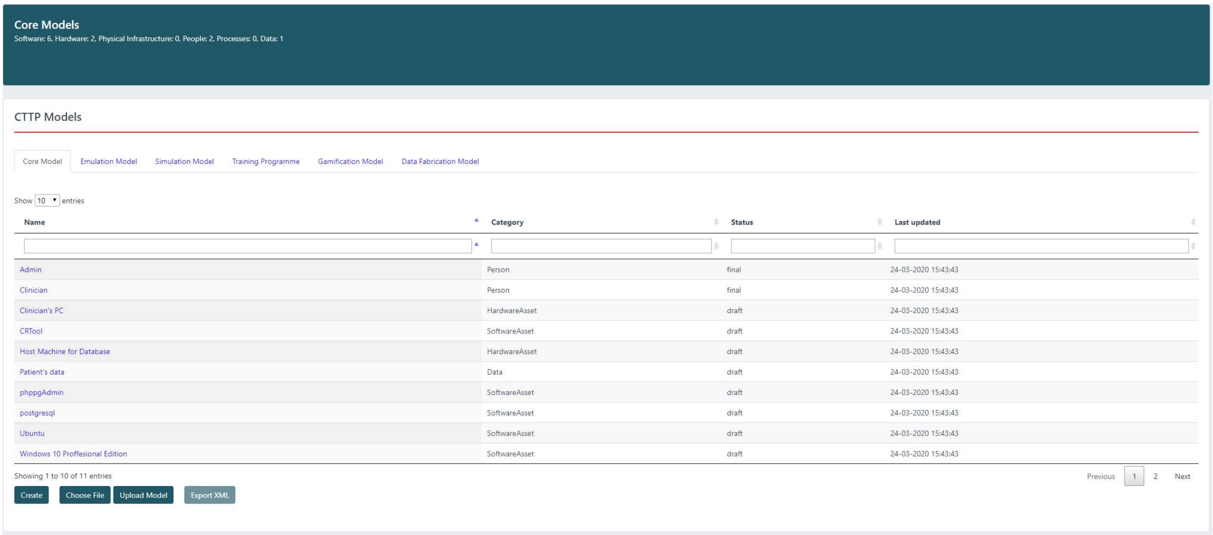


Home / Create Project

Create Project

Name*			
Organisation*			
Active from	2020-03-24 15:43:31	Active to	

Figure 50: Create new project



Core Models

Software: 6, Hardware: 2, Physical Infrastructure: 0, People: 2, Processes: 0, Data: 1

CTTP Models

Show 10 entries

Name	Category	Status	Last updated
Admin	Person	final	24-03-2020 15:43:43
Clinician	Person	final	24-03-2020 15:43:43
Clinician's PC	HardwareAsset	draft	24-03-2020 15:43:43
CRTool	SoftwareAsset	draft	24-03-2020 15:43:43
Host Machine for Database	HardwareAsset	draft	24-03-2020 15:43:43
Patient's data	Data	draft	24-03-2020 15:43:43
phppgAdmin	SoftwareAsset	draft	24-03-2020 15:43:43
postgresql	SoftwareAsset	draft	24-03-2020 15:43:43
Ubuntu	SoftwareAsset	draft	24-03-2020 15:43:43
Windows 10 Proffesional Edition	SoftwareAsset	draft	24-03-2020 15:43:43

Showing 1 to 10 of 11 entries

Figure 51: Edit/View an existing project

Inside a project, the administrator can create a new instance of the CTTP Models and sub-models or edit/view the existing one.

More specifically, each project, has the following elements:

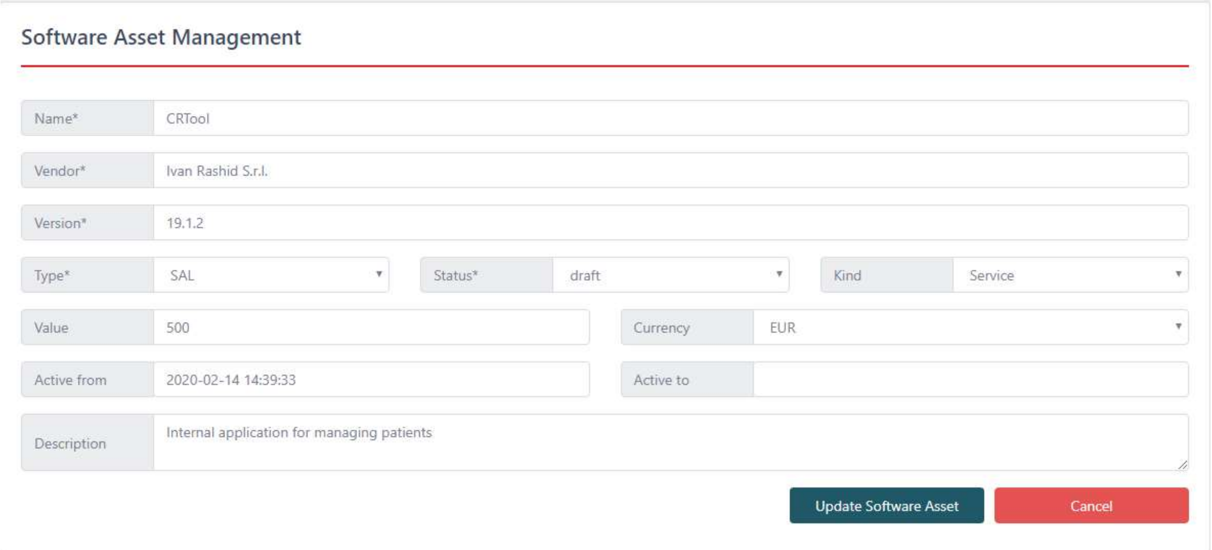
1. The Core CTTP model which includes the assets of the organisation.
2. The Emulation model which includes the model that initializes the Emulation Tool.
3. The Simulation model which includes the model that initializes the Simulation Tool.
4. The Training Programme which includes the model that initializes the Training.
5. The Gamification model which includes the model that initializes the Gamification Tool.
6. The Data Fabrication model which includes the model that initializes the Data Fabrication Tool.

4.4 Core CTTP Model

The user can choose to edit/view existing assets or add a new one.

4.4.1 Edit/View Core CTTP Model

Figure 52 shows an asset's management. A user can make use of the screen to either examine the current elements of a previously created asset or update them if he/she wishes to.



Software Asset Management

Name*	CRTool				
Vendor*	Ivan Rashid S.r.l.				
Version*	19.1.2				
Type*	SAL	Status*	draft	Kind	Service
Value	500	Currency	EUR		
Active from	2020-02-14 14:39:33	Active to			
Description	Internal application for managing patients				

Figure 52: Edit/View an existing asset

4.4.2 Add Core CTTP Model

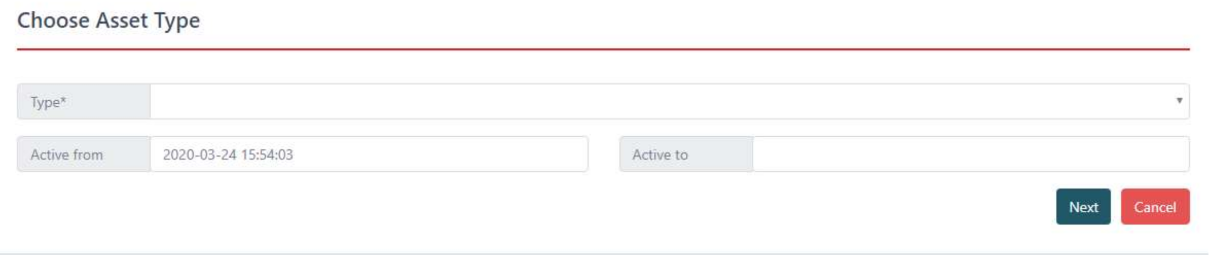
The user can add the organisation's assets either by utilising the web view asset management or by uploading a text file that contains the assets written in the CTTP Grammar described in the deliverable "D3.2 – CTTP Models and Programmes Specification Tool".

4.4.2.1 Create new Asset (Web View)

In order to create a new asset through the web view, the user needs to follow the steps as detailed below.

4.4.2.1.1 Choose asset type

The first step is to choose the type of the asset and add an expiration date (if applicable) (see Figure 53). The type of the asset can be: (a) hardware, (b) software, (c) data and (d) people.



Choose Asset Type

Type*

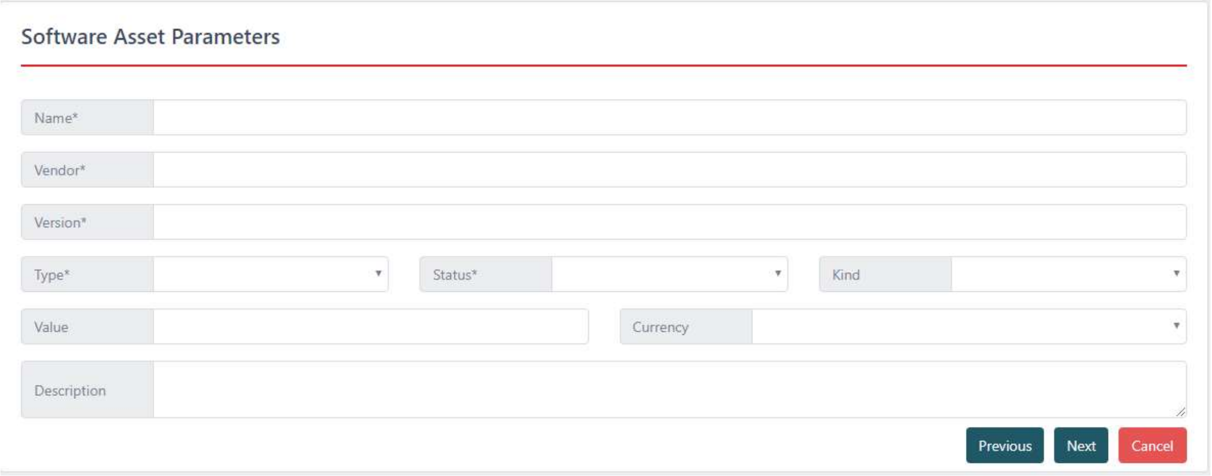
Active from 2020-03-24 15:54:03

Active to

Figure 53: Choose Asset Type

4.4.2.1.2 Add Asset Parameters

Each asset type has its corresponding asset parameters. For instance, in the previous page the user chose to create a new software asset and is now asked to add the software asset parameters (see Figure 54).



Software Asset Parameters

Name*

Vendor*

Version*

Type* Status* Kind

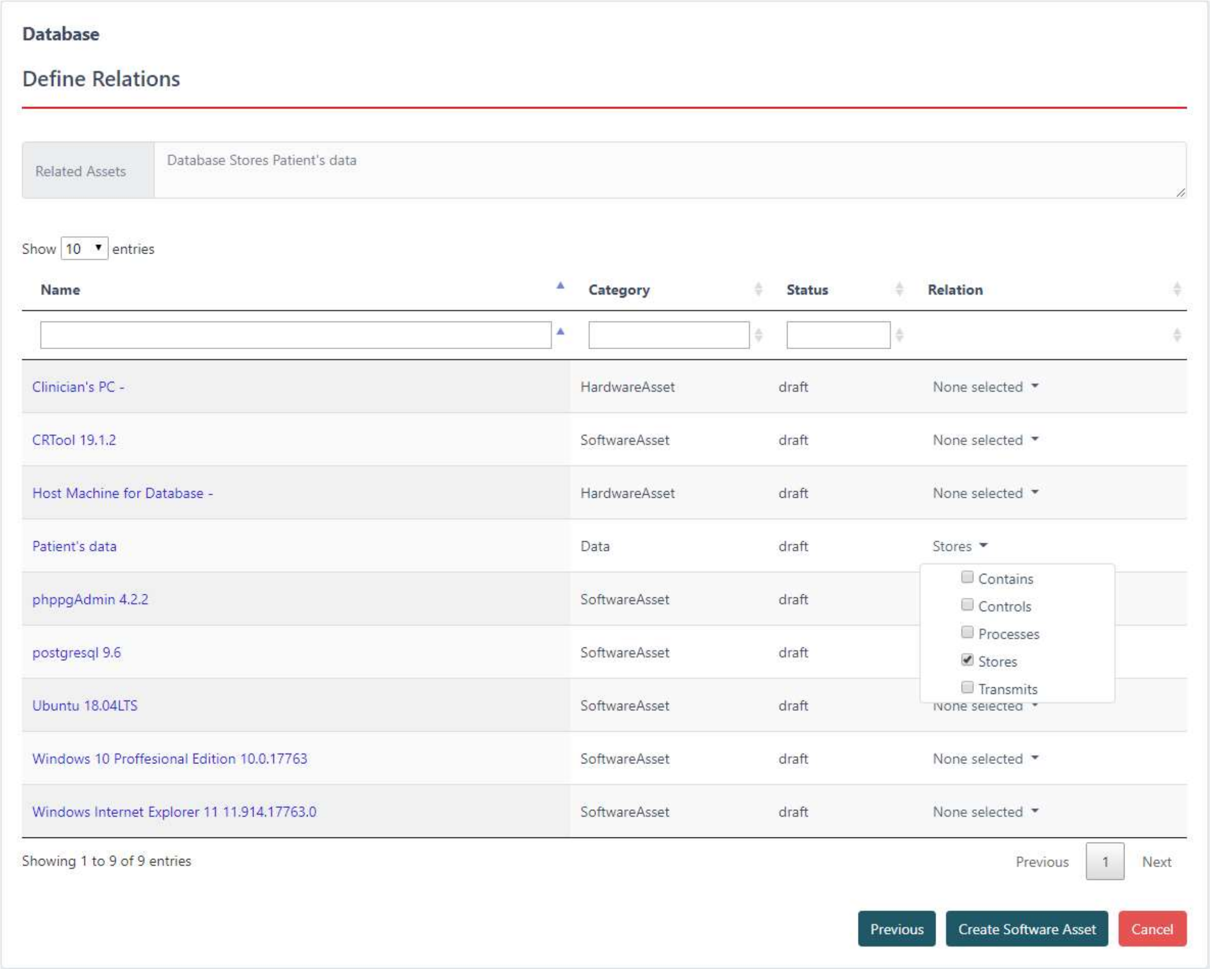
Value Currency

Description

Figure 54: Software Asset Parameters

4.4.2.1.3 Define Relations

Lastly, the user will need to define the relations between the newly created asset and the existing ones (if any). For instance, Figure 55 shows the asset relations (Stores) between the software asset created before (Database) and the patient’s data (Data asset) created in the past.



Database

Define Relations

Related Assets: Database Stores Patient's data

Show 10 entries

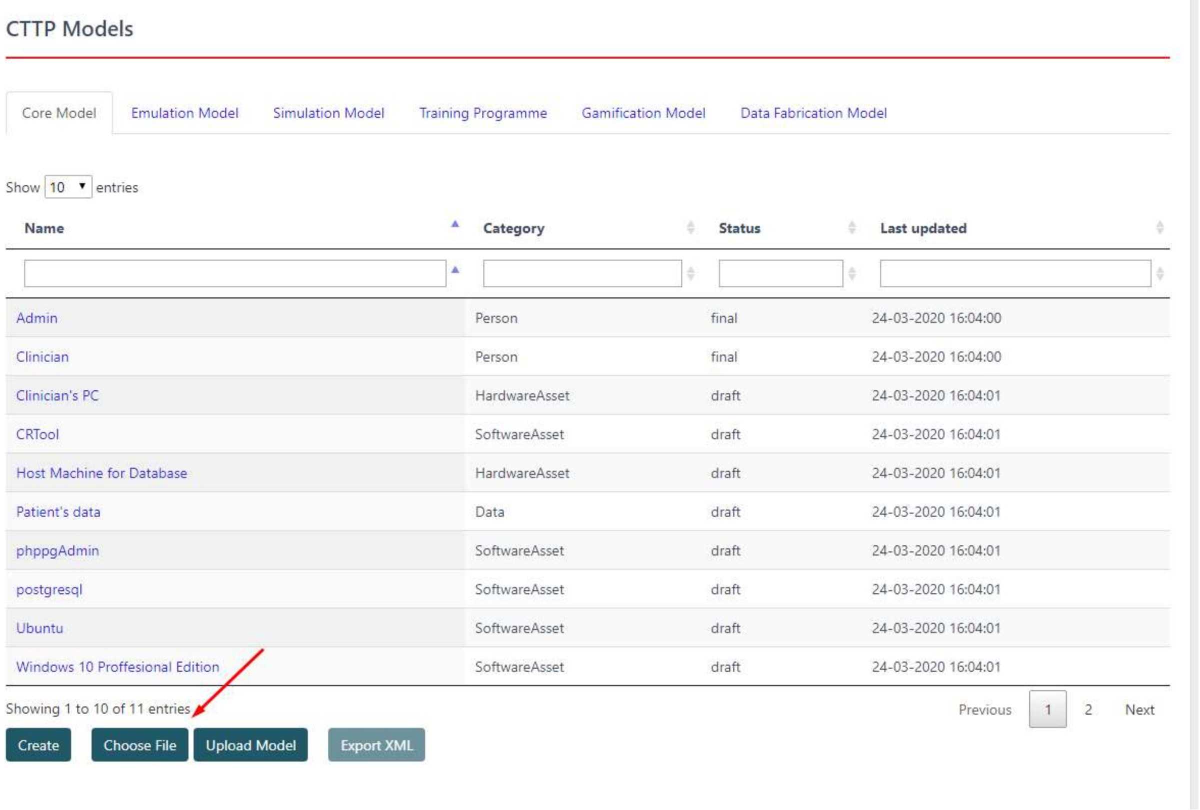
Name	Category	Status	Relation
Clinician's PC -	HardwareAsset	draft	None selected
CRTool 19.1.2	SoftwareAsset	draft	None selected
Host Machine for Database -	HardwareAsset	draft	None selected
Patient's data	Data	draft	Stores □ Contains □ Controls □ Processes ☑ Stores □ Transmits
phppgAdmin 4.2.2	SoftwareAsset	draft	
postgresql 9.6	SoftwareAsset	draft	
Ubuntu 18.04LTS	SoftwareAsset	draft	None selected
Windows 10 Proffesional Edition 10.0.17763	SoftwareAsset	draft	None selected
Windows Internet Explorer 11 11.914.17763.0	SoftwareAsset	draft	None selected

Showing 1 to 9 of 9 entries

Figure 55: Asset relations

4.4.2.2 Create new Asset (Grammar)

The user can also choose to upload a file (see Figure 56) that contains the assets written in the CTTP grammar. An example of such a file can be found in the deliverable “D3.3 – Reference CTTP Models and Programmes Specifications v1”.



CTTP Models

Name	Category	Status	Last updated
Admin	Person	final	24-03-2020 16:04:00
Clinician	Person	final	24-03-2020 16:04:00
Clinician's PC	HardwareAsset	draft	24-03-2020 16:04:01
CRTool	SoftwareAsset	draft	24-03-2020 16:04:01
Host Machine for Database	HardwareAsset	draft	24-03-2020 16:04:01
Patient's data	Data	draft	24-03-2020 16:04:01
phppgAdmin	SoftwareAsset	draft	24-03-2020 16:04:01
postgresql	SoftwareAsset	draft	24-03-2020 16:04:01
Ubuntu	SoftwareAsset	draft	24-03-2020 16:04:01
Windows 10 Proffesional Edition	SoftwareAsset	draft	24-03-2020 16:04:01

Showing 1 to 10 of 11 entries

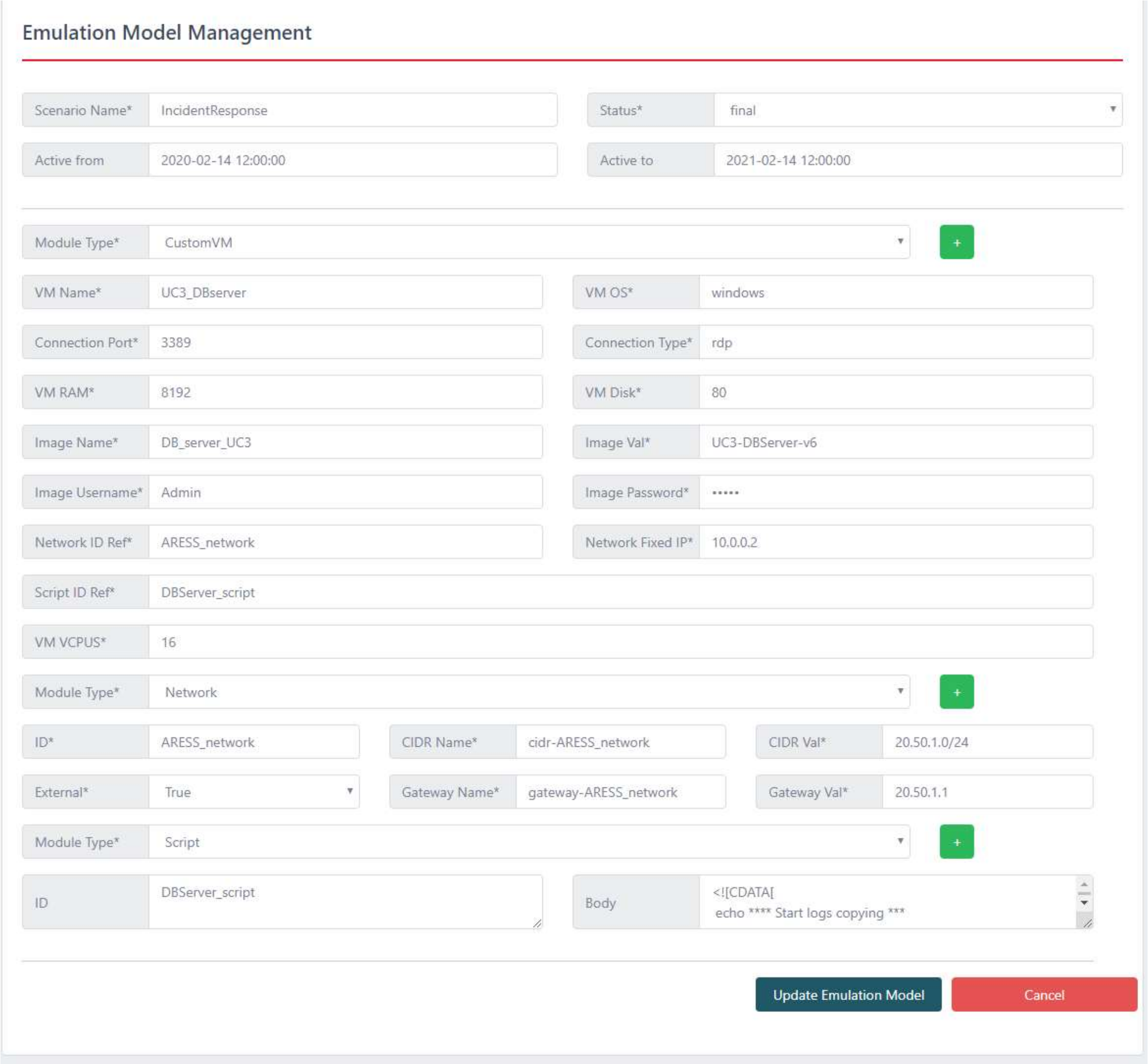
Figure 56: Upload a file that contains the CTTP Model grammar

4.5 Emulation Model

The user can choose to edit/view existing emulation models or add a new one.

4.5.1 Edit/View Emulation Model

Figure 57 shows the emulation model management. A user can make use of the screen to either examine the current elements of a previously created model and/or update them if he/she wishes to.



Emulation Model Management

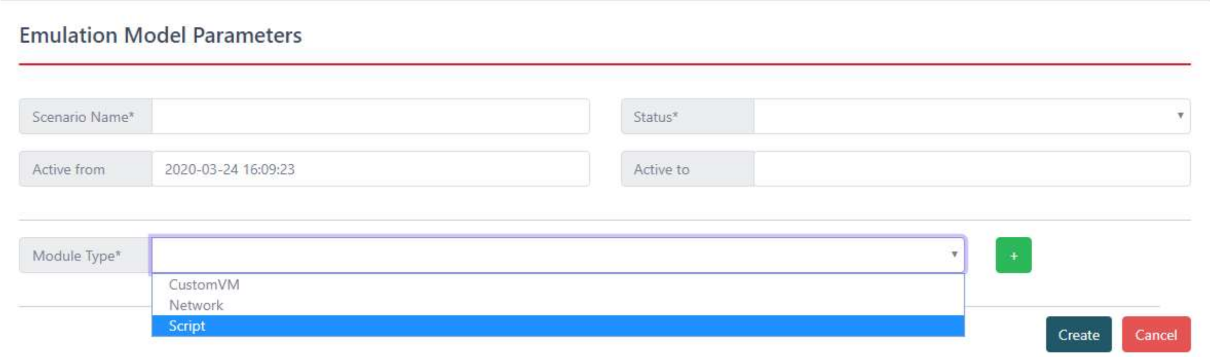
Scenario Name*	IncidentResponse	Status*	final ▾		
Active from	2020-02-14 12:00:00	Active to	2021-02-14 12:00:00		
Module Type*	CustomVM ▾	+			
VM Name*	UC3_DBserver	VM OS*	windows		
Connection Port*	3389	Connection Type*	rdp		
VM RAM*	8192	VM Disk*	80		
Image Name*	DB_server_UC3	Image Val*	UC3-DBServer-v6		
Image Username*	Admin	Image Password*	•••••		
Network ID Ref*	ARESS_network	Network Fixed IP*	10.0.0.2		
Script ID Ref*	DBServer_script				
VM VCPUS*	16				
Module Type*	Network ▾	+			
ID*	ARESS_network	CIDR Name*	cidr-ARESS_network	CIDR Val*	20.50.1.0/24
External*	True ▾	Gateway Name*	gateway-ARESS_network	Gateway Val*	20.50.1.1
Module Type*	Script ▾	+			
ID	DBServer_script	Body	<![CDATA[echo **** Start logs copying ***		

Figure 57: View/Edit emulation models

4.5.2 Add Emulation model

In order to create a new Emulation model, the user needs to add a scenario name, the model's status (final or draft) and the expiration date (if applicable).

The user can also choose to add 1 or more module types (see Figure 58). An emulation model can have the following module types: (a) Custom VM (see Figure 59), (b) Network (see Figure 60) and (c) Script (see Figure 61). Each module type has its own parameters.



Emulation Model Parameters

Scenario Name*

Status*

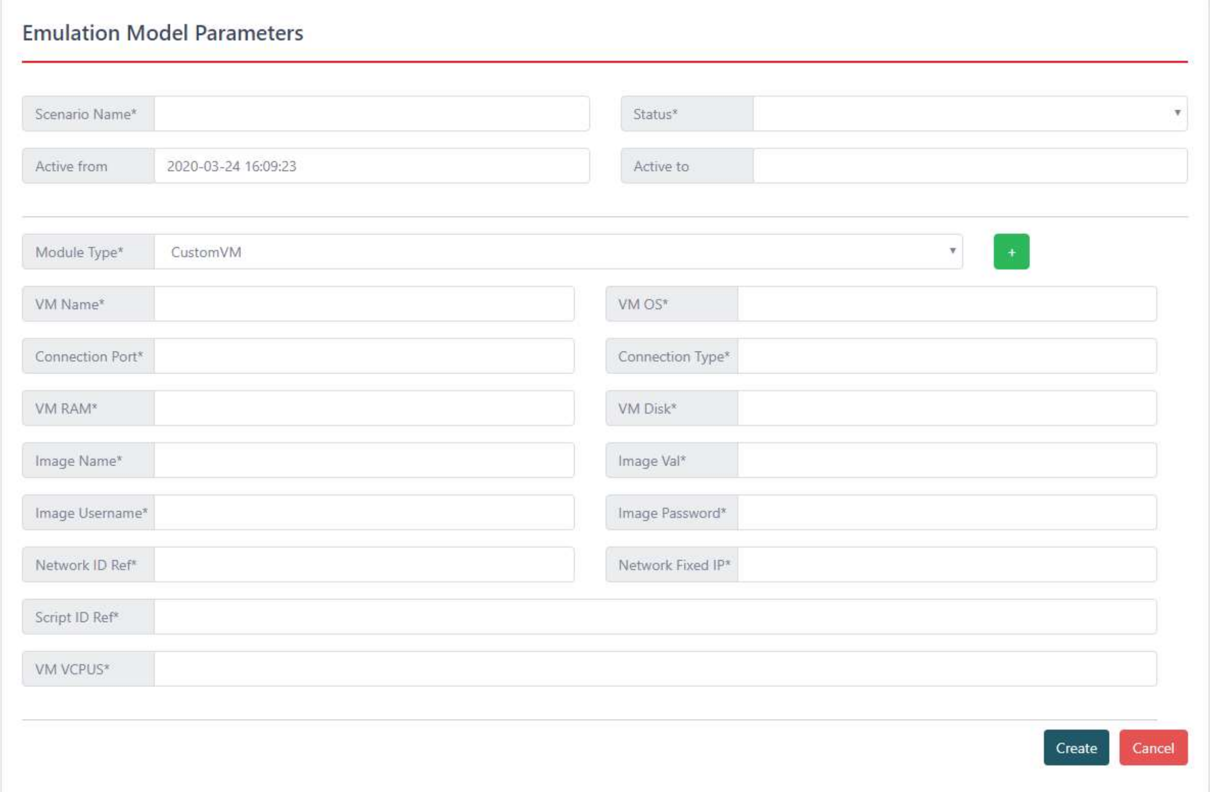
Active from 2020-03-24 16:09:23

Active to

Module Type*

CustomVM
Network
Script

Figure 58: Emulation Model parameters



Emulation Model Parameters

Scenario Name*

Status*

Active from 2020-03-24 16:09:23

Active to

Module Type* CustomVM

VM Name*

VM OS*

Connection Port*

Connection Type*

VM RAM*

VM Disk*

Image Name*

Image Val*

Image Username*

Image Password*

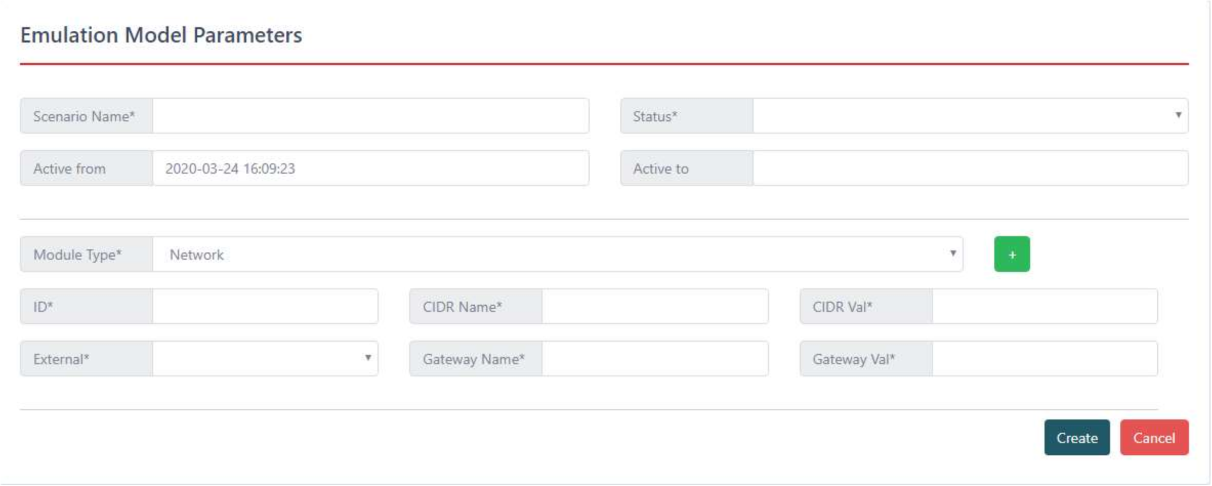
Network ID Ref*

Network Fixed IP*

Script ID Ref*

VM VCPUS*

Figure 59: Custom VM parameters

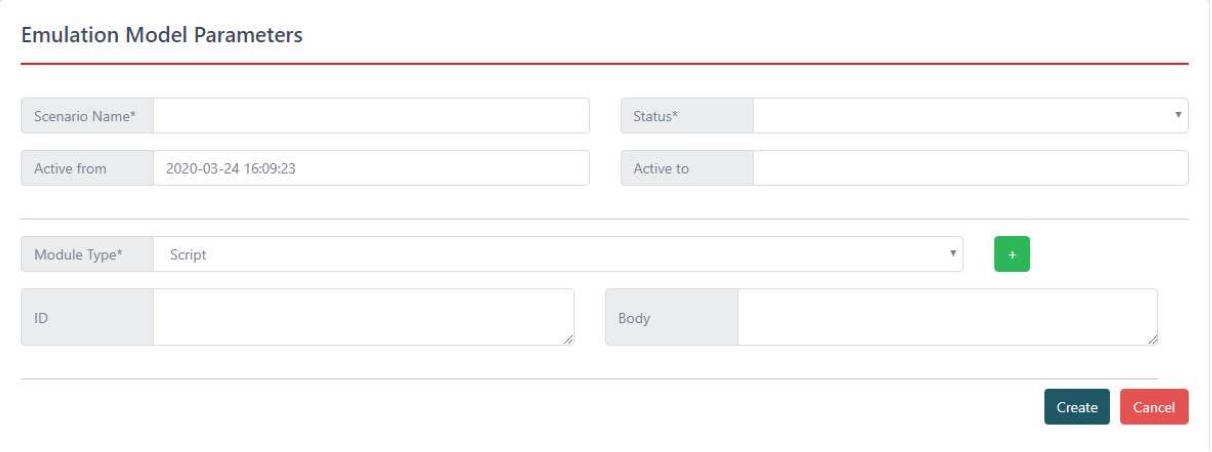


Emulation Model Parameters

Active from: 2020-03-24 16:09:23

Module Type*: Network

Figure 60: Network parameters



Emulation Model Parameters

Active from: 2020-03-24 16:09:23

Module Type*: Script

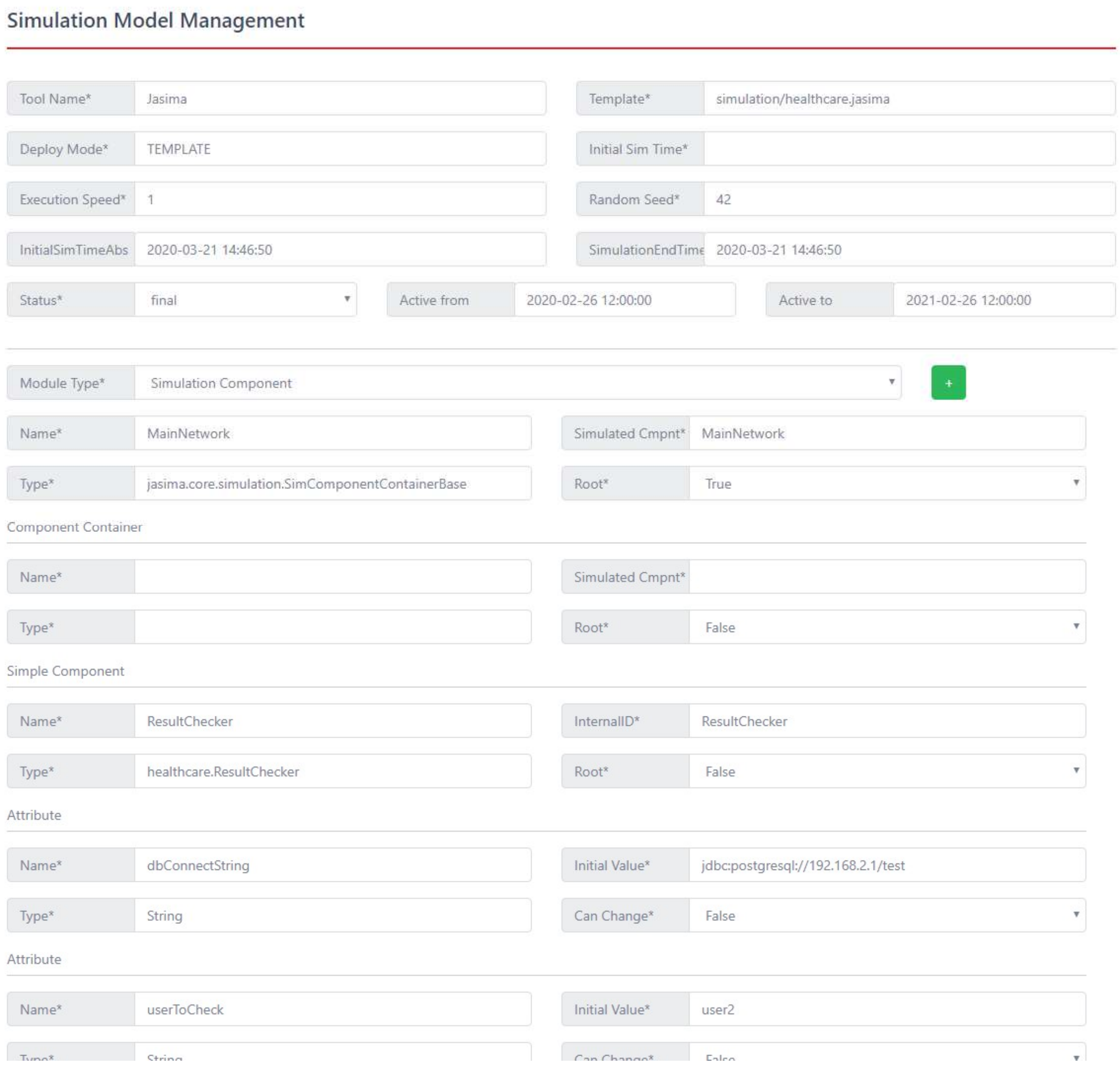
Figure 61: Script parameters

4.6 Simulation Model

The user can choose to edit/view existing simulation models or add a new one.

4.6.1 Edit/View Simulation Model

Figure 62 shows the simulation model management. A user can make use of the screen to either examine the current elements of a previously created model or update them if he/she wishes to.



Simulation Model Management

Tool Name*	Jasima	Template*	simulation/healthcare.jasima
Deploy Mode*	TEMPLATE	Initial Sim Time*	
Execution Speed*	1	Random Seed*	42
InitialSimTimeAbs	2020-03-21 14:46:50	SimulationEndTime	2020-03-21 14:46:50

Status*	final	Active from	2020-02-26 12:00:00	Active to	2021-02-26 12:00:00

Module Type*	Simulation Component

Name*	MainNetwork	Simulated Cmpnt*	MainNetwork
Type*	jasima.core.simulation.SimComponentContainerBase	Root*	True

Component Container

Name*		Simulated Cmpnt*	
Type*		Root*	False

Simple Component

Name*	ResultChecker	InternalID*	ResultChecker
Type*	healthcare.ResultChecker	Root*	False

Attribute

Name*	dbConnectString	Initial Value*	jdbc:postgresql://192.168.2.1/test
Type*	String	Can Change*	False

Attribute

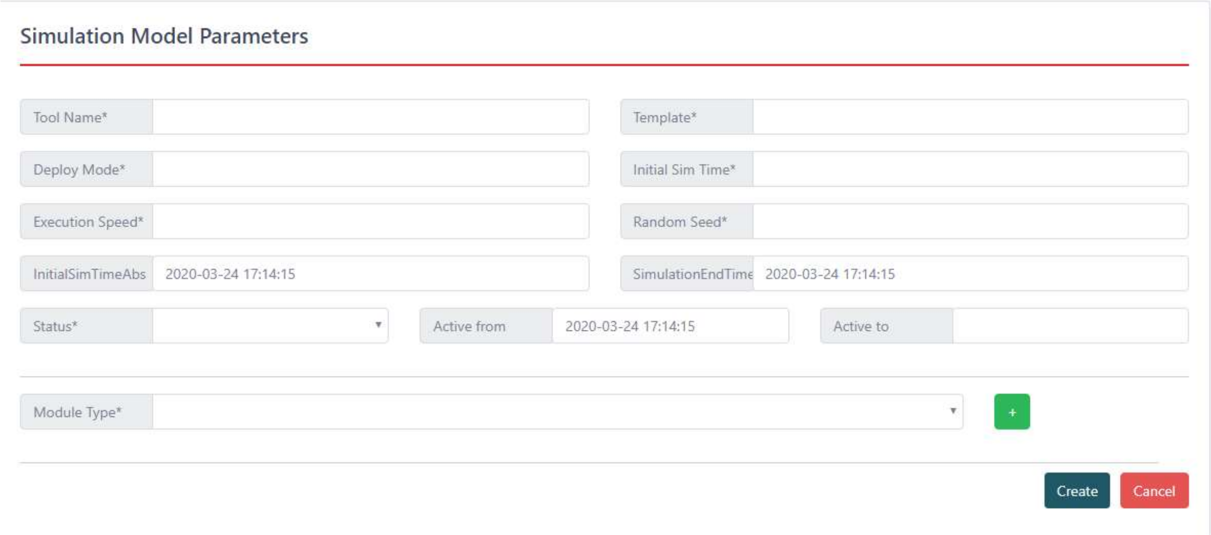
Name*	userToCheck	Initial Value*	user2
Type*	String	Can Change*	False

Figure 62: Edit/view simulation model

4.6.2 Add Simulation Model

In order to create a new Simulation model, the user needs to add the tool name, the template, the deployment mode, the initial simulation time, the execution speed, the random seed, the initial abs simulation time, the simulation end time and the expiration date (if applicable) (see Figure 63).

The user can also choose to add one or more simulation components (see Figure 64). A simulation component consists of a number of attributes, the simulation container, a simple component and the attributes.



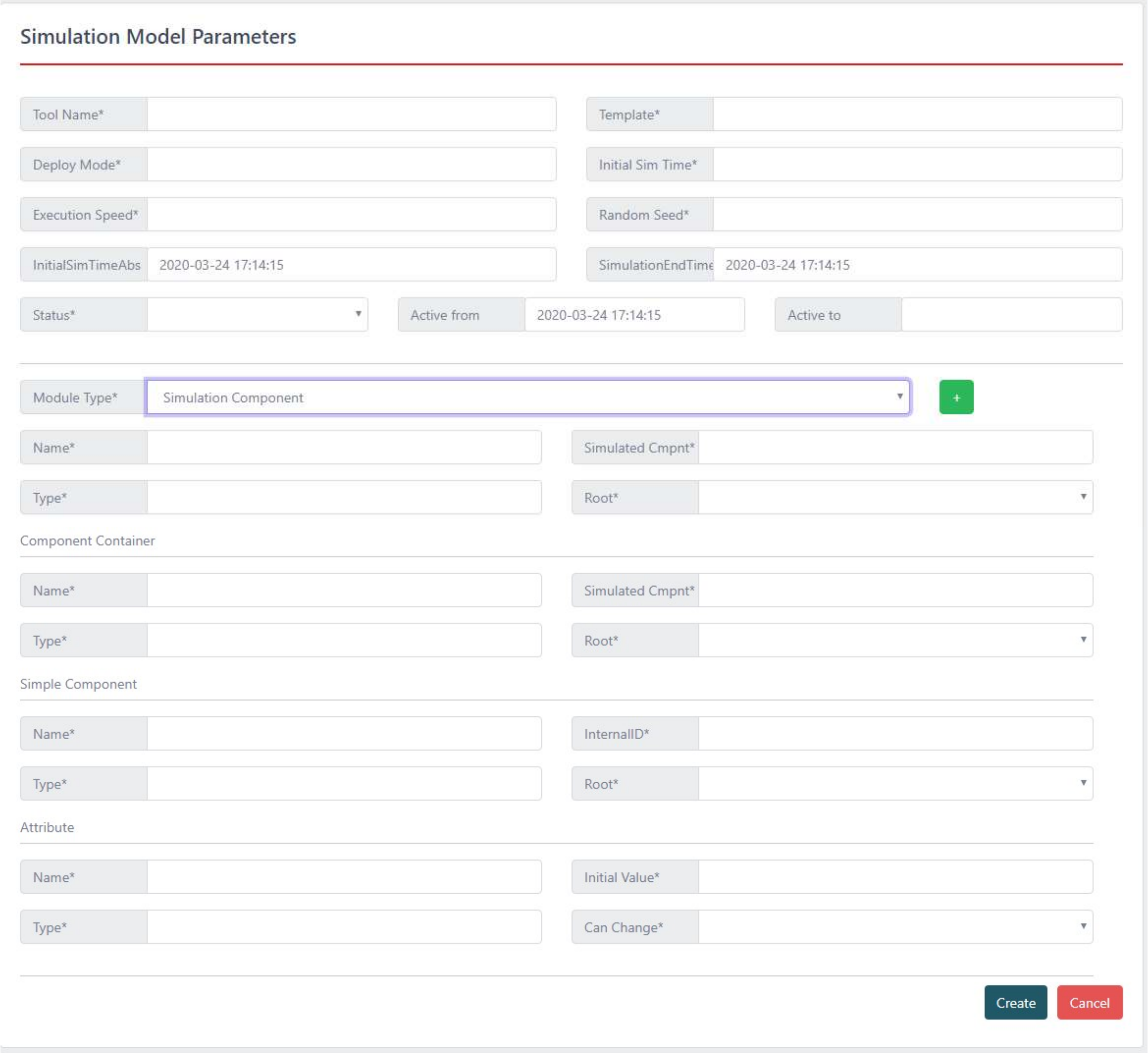
Simulation Model Parameters

Tool Name*		Template*	
Deploy Mode*		Initial Sim Time*	
Execution Speed*		Random Seed*	
InitialSimTimeAbs	2020-03-24 17:14:15	SimulationEndTime	2020-03-24 17:14:15

Status* ▾ Active from 2020-03-24 17:14:15 Active to

Module Type* ▾

Figure 63: Add simulation model main parameters



Simulation Model Parameters

Tool Name*		Template*	
Deploy Mode*		Initial Sim Time*	
Execution Speed*		Random Seed*	
InitialSimTimeAbs	2020-03-24 17:14:15	SimulationEndTime	2020-03-24 17:14:15

Status* ▾ Active from 2020-03-24 17:14:15 Active to

Module Type* Simulation Component ▾

Name*		Simulated Cmpnt*	
Type*		Root*	▾

Component Container

Name*		Simulated Cmpnt*	
Type*		Root*	▾

Simple Component

Name*		InternalID*	
Type*		Root*	▾

Attribute

Name*		Initial Value*	
Type*		Can Change*	▾

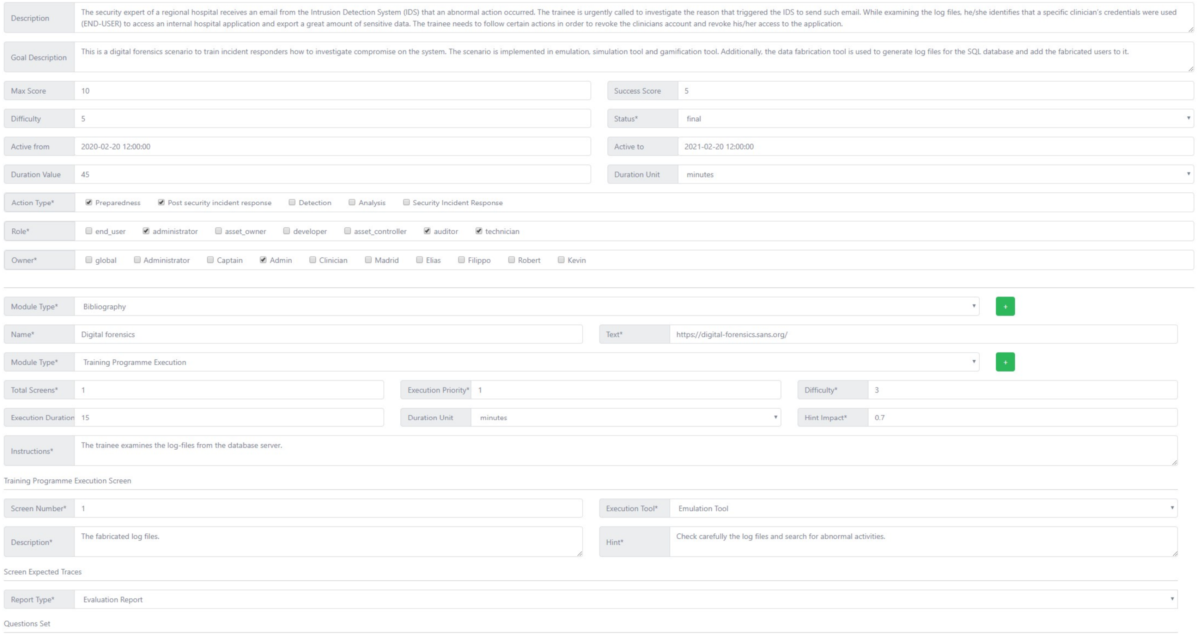
Figure 64: Add a new module

4.7 Training Programme

The user can choose to edit/view existing training programmes or add a new one.

4.7.1 Edit/View Training Programme

Figure 65 shows the Training Programme management. A user can make use of the screen to either examine the current elements of a previously created programme and/or update them if he/she wishes to.



Description: The security expert of a regional hospital receives an email from the Intrusion Detection System (IDS) that an abnormal action occurred. The trainee is urgently called to investigate the reason that triggered the IDS to send such email. While examining the log files, he/she identifies that a specific clinician's credentials were used (END-USER) to access an internal hospital application and export a great amount of sensitive data. The trainee needs to follow certain actions in order to revoke the clinicians account and revoke his/her access to the application.

Goal Description: This is a digital forensics scenario to train incident responders how to investigate compromise on the system. The scenario is implemented in emulation, simulation tool and gamification tool. Additionally, the data fabrication tool is used to generate log files for the SQL database and add the fabricated users to it.

Max Score	10	Success Score	5
Difficulty	5	Status*	final
Active from	2020-02-20 12:00:00	Active to	2021-02-20 12:00:00
Duration Value	45	Duration Unit	minutes

Action Type*: ☑ Preparedness ☑ Post security incident response ☐ Detection ☐ Analysis ☐ Security Incident Response

Role*: ☐ end_user ☑ administrator ☐ asset_owner ☐ developer ☐ asset_controller ☑ auditor ☑ technician

Owner*: ☐ global ☐ Administrator ☐ Captain ☑ Admin ☐ Clinician ☐ Madrid ☐ Elias ☐ Filippo ☐ Robert ☐ Kevin

Module Type*: Bibliography +

Name*: Digital forensics Text*: https://digital-forensics.sans.org/

Module Type*: Training Programme Execution +

Total Screens*	1	Execution Priority*	1	Difficulty*	3
Execution Duration	15	Duration Unit	minutes	Hint Impact*	0.7

Instructions*: The trainee examines the log-files from the database server.

Training Programme Execution Screen

Screen Number*: 1 Execution Tool*: Emulation Tool

Description*: The fabricated log files. Hint*: Check carefully the log files and search for abnormal activities.

Screen Expected Traces

Report Type*: Evaluation Report

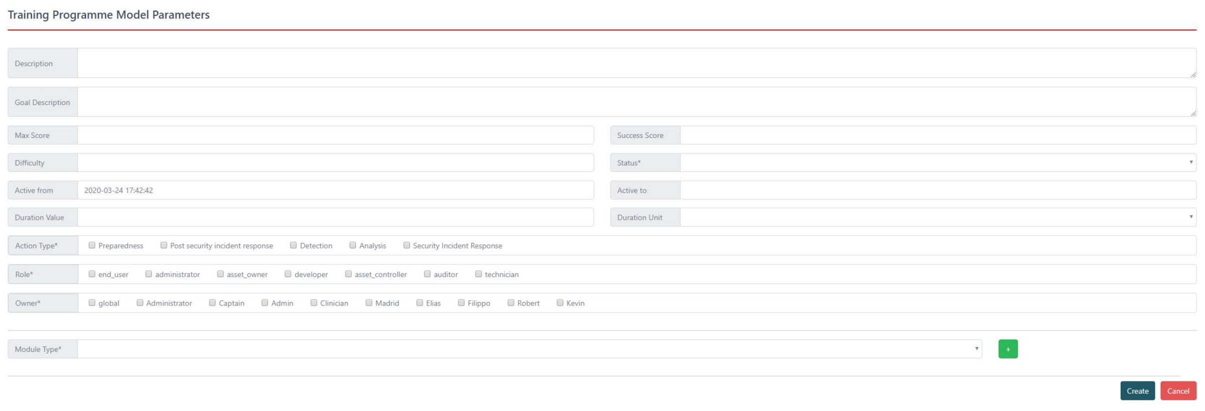
Questions Set

Figure 65: Edit/View Training Programme

4.7.2 Add Training Programme

In order to create a new Training Programme, the user needs to insert its main attributes (see Figure 66). Furthermore, each programme has one or more training modules (see Figure 67), namely: (a) Bibliography (see Figure 68) and (b) Training Programme Execution (see Figure 69).

Upon creation of a new Training Programme, the CTTP Model Editor notifies the Training Tool that a new programme was created. This is being done by utilising the message broker of the platform.



Training Programme Model Parameters

Description

Goal Description

Max Score		Success Score	
Difficulty		Status*	
Active from	2020-03-24 17:42:42	Active to	
Duration Value		Duration Unit	

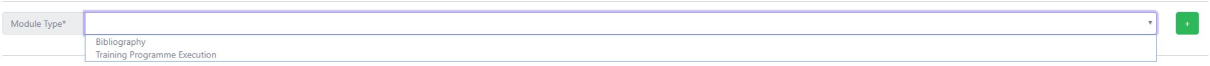
Action Type*: ☐ Preparedness ☐ Post security incident response ☐ Detection ☐ Analysis ☐ Security Incident Response

Role*: ☐ end_user ☐ administrator ☐ asset_owner ☐ developer ☐ asset_controller ☐ auditor ☐ technician

Owner*: ☐ global ☐ Administrator ☐ Captain ☐ Admin ☐ Clinician ☐ Madrid ☐ Elias ☐ Filippo ☐ Robert ☐ Kevin

Module Type* +

Figure 66: Training Programme main attributes

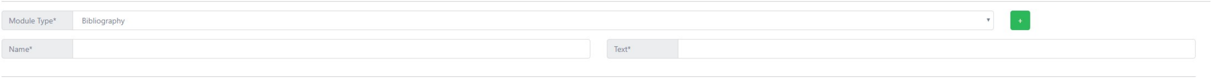


Module Type*

Bibliography

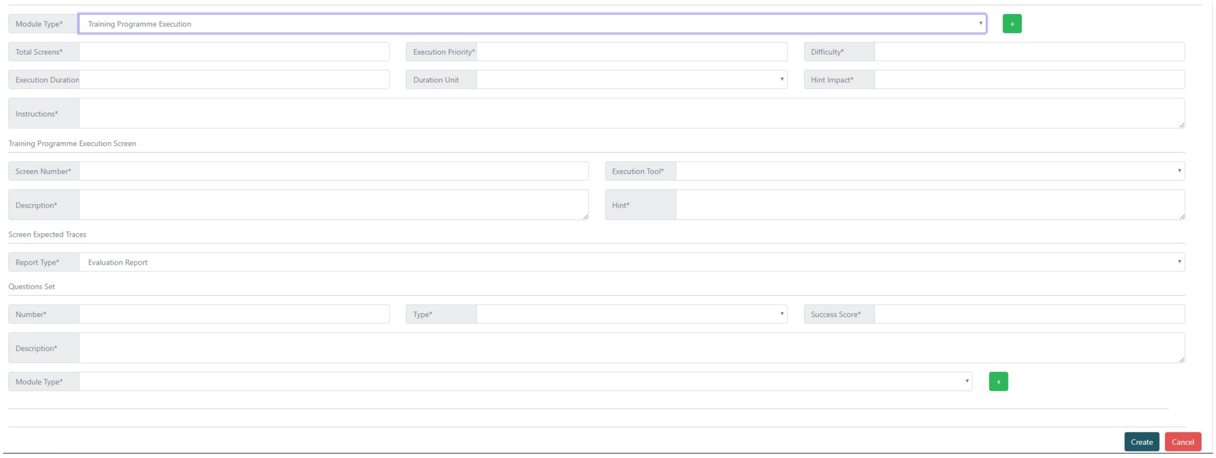
Training Programme Execution

Figure 67: Training Programme modules



Module Type*	Bibliography		
Name*		Text*	

Figure 68: Bibliography module



Module Type*	Training Programme Execution				
Total Screens*		Execution Priority*		Difficulty*	
Execution Duration		Duration Unit		Hint Impact*	
Instructions*					

Training Programme Execution Screen

Screen Number*		Execution Tool*	
Description*		Hint*	

Screen Expected Traces

Report Type*	Evaluation Report

Questions Set

Number*		Type*		Success Score*	
Description*					
Module Type*					

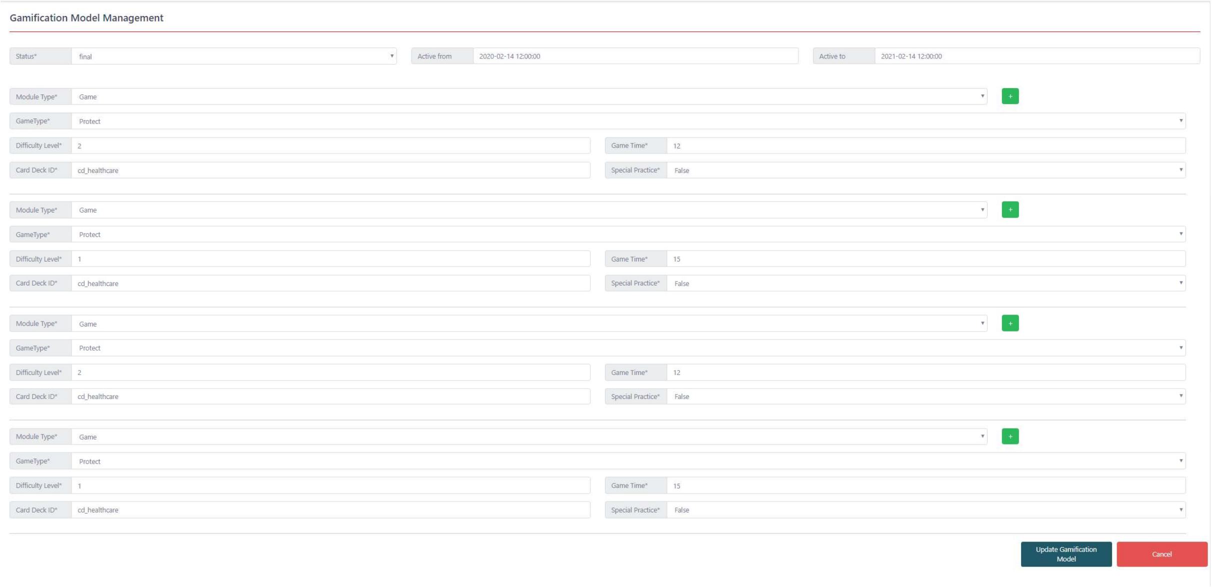
Figure 69: Training Programme Execution Module

4.8 Gamification Model

The user can choose to edit/view existing gamification models or add a new one.

4.8.1 Edit/View Gamification Model

Figure 70 shows the Gamification model management. A user can make use of the screen to either examine the current elements of a previously created programme or update them if he/she wishes to.



Gamification Model Management

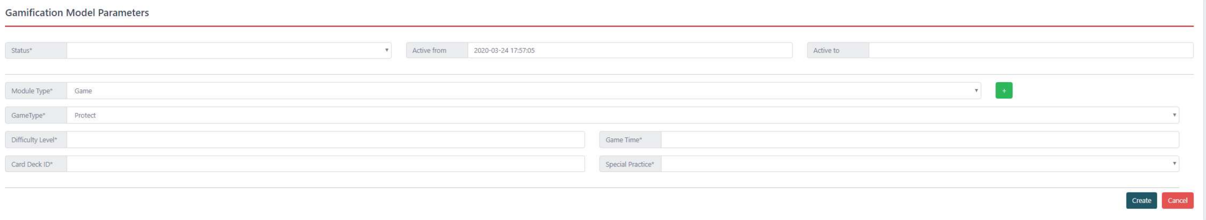
Status*	final	Active from	2020-02-14 12:00:00	Active to	2021-02-14 12:00:00

Module Type*	Game		
GameType*	Protect		
Difficulty Level*	2	Game Time*	12
Card Deck ID*	cd_healthcare	Special Practice*	False
Module Type*	Game		
GameType*	Protect		
Difficulty Level*	1	Game Time*	15
Card Deck ID*	cd_healthcare	Special Practice*	False
Module Type*	Game		
GameType*	Protect		
Difficulty Level*	2	Game Time*	12
Card Deck ID*	cd_healthcare	Special Practice*	False
Module Type*	Game		
GameType*	Protect		
Difficulty Level*	1	Game Time*	15
Card Deck ID*	cd_healthcare	Special Practice*	False

Figure 70: Edit/View Gamification model

4.8.2 Add Gamification Model

In order to add a new Gamification model the user needs to choose the game type (i.e. the game PROTECT or AWARENESS QUEST) and fill the requested attributes (see Figure 71).



Gamification Model Parameters

Status*		Active from	2020-03-24 17:57:05	Active to	
Module Type*	Game				
GameType*	Protect				
Difficulty Level*		Game Time*			
Card Deck ID*		Special Practice*			

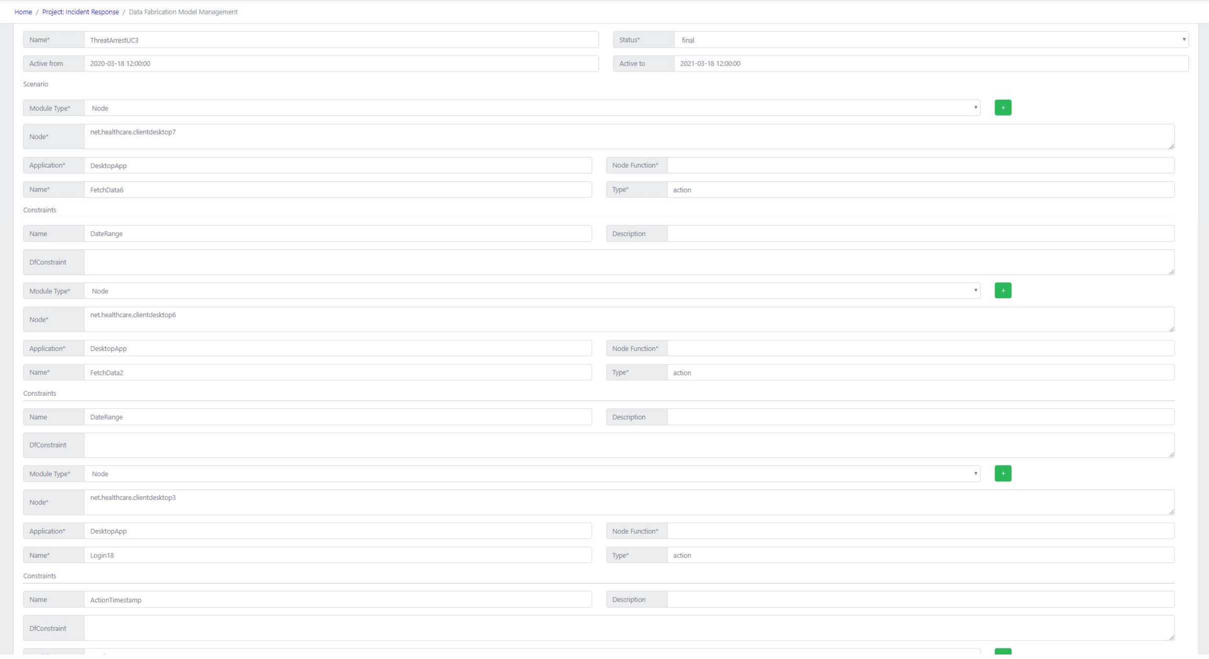
Figure 71: Add Gamification model

4.9 Data Fabrication Model

The user can choose to edit/view existing data fabrication models or add a new one.

4.9.1 Edit/View Data Fabrication Model

Figure 72 shows the Data Fabrication model management. A user can make use of the screen to either examine the current elements of a previously created programme or update them if he/she wishes to.



Home / Project: Incident Response / Data Fabrication Model Management

Name*	ThreatArrestUC3	Status*	final
Active from	2020-03-18 12:00:00	Active to	2021-03-18 12:00:00

Scenario

Module Type*	Node		
Node*	net.healthcare.clientdesktop7		
Application*	DesktopApp	Node Function*	
Name*	FetchData6	Type*	action

Constraints

Name	DateRange	Description	
DfConstraint			
Module Type*	Node		
Node*	net.healthcare.clientdesktop6		
Application*	DesktopApp	Node Function*	
Name*	FetchData2	Type*	action

Constraints

Name	DateRange	Description	
DfConstraint			
Module Type*	Node		
Node*	net.healthcare.clientdesktop3		
Application*	DesktopApp	Node Function*	
Name*	Login18	Type*	action

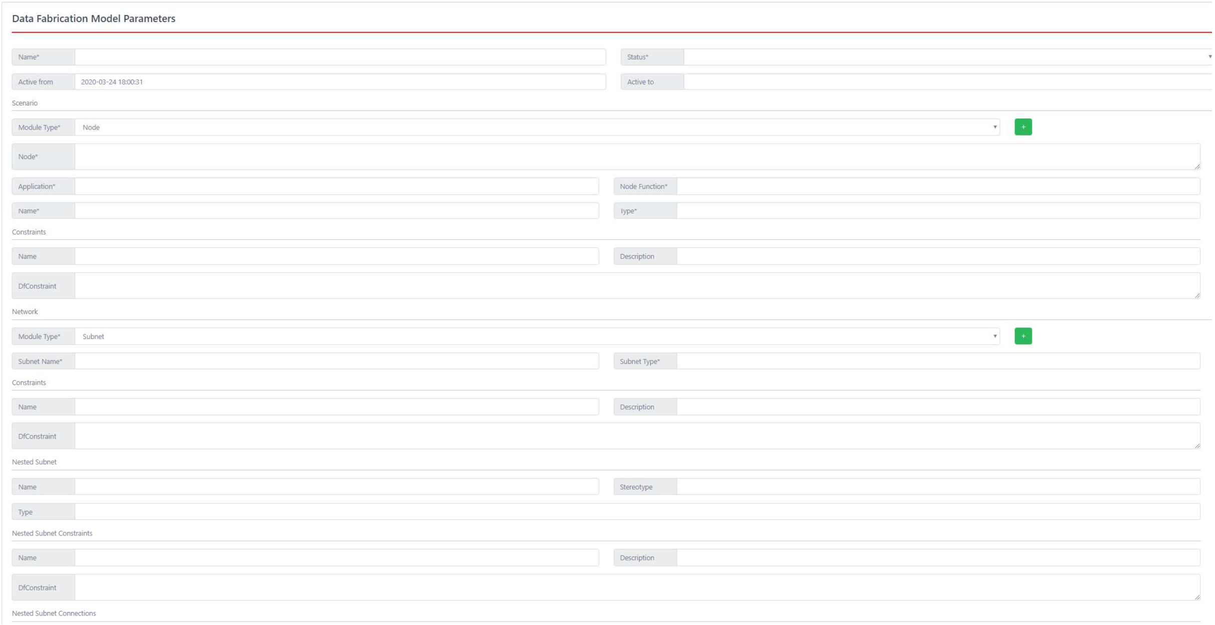
Constraints

Name	ActionTimestamp	Description	
DfConstraint			

Figure 72: Edit/View Data Fabrication model

4.9.2 Add Data Fabrication Model

In order to add a new Data Fabrication model, the user needs to add one or more nodes and one or more subnets. Both the node and the subnet hold a number of attributes as depicted in Figure 73.



Data Fabrication Model Parameters

Name* | Status*

Active from: 2020-03-24 18:00:31 | Active to

Scenario

Module Type*: Node

Node*

Application* | Node Function*

Name* | type*

Constraints

Name | Description

DfConstraint

Network

Module Type*: Subnet

Subnet Name* | Subnet Type*

Constraints

Name | Description

DfConstraint

Nested Subnet

Name | Stereotype

Type

Nested Subnet Constraints

Name | Description

DfConstraint

Nested Subnet Connections

Figure 73: Add Data Fabrication model

5 Conclusions

We have presented the documentation and guidelines for the use of the first version of the integrated THREAT-ARREST platform. Particularly, we have presented the hardware and software requirements necessary for platform operation. The hardware requirements may vary from one platform instance to another depending on the training needs in each domain in terms of the number of simultaneous training sessions supported and the complexity of cyber system emulation/simulation. We have presented the installation guidelines of the platform from OpenStack installation, VM and network setup to individual components' installation procedures and software dependencies. We have overviewed the GUI of the platform's dashboard showing the different platform capabilities available for trainees and trainers, and the GUI of the CTTP model editor.

Next version of the document is "D6.6 – Final Installation and usage guidelines for the THREAT-ARREST platform" due to M36 which corresponds to the final version of the platform.

In addition to the expected refinement and improvement of the usage guidelines with respect to the final platform's capabilities and different end users' categories, next steps will also address the installation and usage guidelines of the Assurance Tool. In particular this includes how Assurance Tool's interfaces and event captors are to be used and deployed in (pilot) organisations' infrastructures to get full benefit of security assurance, training program evaluation and user assessment before, during and after employee's cyber security training.

References

GDPR, 2016. European Parliament, Council of The European Union: Regulation (EU), 2016/679 General Data Protection Regulation (GDPR). http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 [26 February 2019]

Goeke, L.; Quintanar, A.; Beckers, K. and Pape, S.: PROTECT - An Easy Configurable Serious Game to Train Employees Against Social Engineering Attacks. In Computer Security - ESORICS 2019 International Workshops, IOSec, MSTEC, and FINSEC, Luxembourg City, Luxembourg, September 26-27, 2019, Revised Selected Papers, pages 156-171, Springer International Publishing, Cham, Lecture Notes in Computer Science 11981, 2019

IBM, 2017 “Create high-quality test data while minimizing the risks of using sensitive production data.” *IBM InfoSphere Optim Test Data Fabrication*, https://www.ibm.com/ilen/marketplace/infosphere-optim-test-data-fabrication

Jasima, 2019. Jasima: Java Simulator for Manufacturing and Logistics. SimPlan AG. https://www.simplan.de/en/software/jasima/ [26 February 2019]

OpenStack, 2019. https://www.openstack.org/ [26 February 2019]

RabbitMQ, 2019. RabbitMQ: An open source messaging broker. https://www.rabbitmq.com/ [26 February 2019]

RFC 6455, 2011. RFC 6455 - The WebSocket Protocol. Internet Engineering Task Force (IETF), https://tools.ietf.org/html/rfc6455 [26 February 2019]

THREAT-ARREST DoA, 2018. THREAT-ARREST Grant Agreement Annex I – “Description of Action” (DoA).

THREAT-ARREST D4.2, 2019. THREAT-ARREST serious games v1, THREAT-ARREST Project deliverable D4.2, https://www.threat-arrest.eu