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

D3.3: Reference CTTP Models and Programmes Specifications v1†

Abstract: This deliverable provides the first version of the reference CTTP models and CTTP programmes for the three pilots of THREAT-ARREST. The models specification is programmed with the language developed in task "T3.1 – CTTP Language definition and Tool Support", taking into account the analysis of existing security assurance profiles (e.g., Common Criteria protection profiles and Commercial Product Assurance security schemes) for the targeted pilot systems, known threats for the various underlying components, as well as, the deployed security controls. This document constitutes the first outcome of the task "T3.2 – CTTP models and programmes development" and addresses the related KPIs 7.1-7.4.

Contractual Date of Delivery	29/02/2020
Actual Date of Delivery	29/02/2020
Deliverable Security Class	Public
Editor	*Smyrlis Michail, Konstantinos Fysarakis (STS)*
Contributors	STS, FORTH, UMIL, CZNIZ, DANAOS, TUV, LSE, ARES
Quality Assurance	*George Leftheriotis (TUV),* *George Tsakirakis (ITML),* *George Hatzivasilis (FORTH)*

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

The *THREAT-ARREST* Consortium

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

Document Revisions & Quality Assurance

Internal Reviewers

1. *George Leftheriotis (TUV)*
2. *George Tsakirakis (ITML)*
3. *George Hatzivasilis (FORTH)*

Revisions

Version	Date	By	Overview
1.1	28/02/2020	Michail Smyrlis	Ready for PCC
1.0	27/02/2020	Michail Smyrlis	Addressed TUV's comments
0.9	26/02/2020	Michail Smyrlis	Added UC1 details, deliverable ready for internal review.
0.8	15/02/2020	Michail Smyrlis	Addressed comments from the contributors
0.7	11/02/2020	Michail Smyrlis	Finalised UC2, Added draft Core models for UC2 and UC3
0.6	06/02/2020	Michail Smyrlis	Finalised UC3
0.5	05/11/2019	Editor	Finalised programme definition
0.4	08/10/2019	Editor	Threat Landscapes completed
0.3	02/08/2019	Editor	Refined Scenarios for all use cases
0.2	30/06/2019	Editor	Updated with Requirements and early Scenarios
0.1	15/12/2018	Editor	First Draft

Executive Summary

This deliverable presents the first version of the reference CTTP Models and Programmes for the three pilots of THREAT-ARREST and is developed under task "T3.2 - CTTP models and programmes development".

The goal of this first version is to analyse the existing security assurance schemes and assurance profiles landscape and identify possible threats and existing controls in the piloting environments. This analysis will drive the creation of well-defined training CTTP Programmes.

Following the creation of the training programmes, this deliverable will include the specification of the scenario models for the piloting environments which include the core CTTP Model and sub models resulting in the initiation of the Training Programme.

Summarising, this deliverable includes: (a) an overview of the current landscape and the threats and controls identified in the piloting environments, (b) the definition of the CTTP Programmes, and (c) the specification of the scenario CTTP Models.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ANTLR ANother Tool for Language Recognition

API Application Programming Interface

CC Common Criteria

CIO Chief-Information-Officers

CSO Chief-Security-Officers

CTTP Cyber Threat and Training Preparation

DAO Data Access Object

DFP Data Fabrication Platform

DER Distributed Energy Resource

EBNF Extended Backus–Naur Form

HTTP Hypertext Transfer Protocol

HSM Hardware Security Module

IDS Intrusion Detection System

IPS Intrusion Prevention System

JSON JavaScript Object Notation

IT Information Technology

OT Operational Technology

POJO Plain Old Java Object

REST Representational state transfer

SQL Structured Query Language

TOE Target Of Evaluation

VM Virtual Machine

XML eXtensible Markup Language

1 Introduction

This deliverable is the initial output of task "T3.2 – CTTP Models and Programmes development". As such, it details the development of the CTTP Models and Programmes for all the three pilots of THREAT-ARREST, and the specification of these in an executable form, using the language developed in Task 3.1 ("CTTP Language definition and Tool Support") and specified in D3.1 ("CTTP Models and Programmes Specification Language").

The development of Cyber Threat and Training Preparation (CTTP) models is based on the analysis of existing assurance schemes and the identification of the threats and controls in the piloting environments (as described in the deliverable "D1.1 – The pilots' requirements analysis report"). As of now, ***13 scenarios*** have been modelled for the three pilots (5 for the Smart Energy, 4 for the Healthcare, and 4 for the Smart Shipping pilots, respectively).

The creation of a CTTP model and programme includes three main phases. At first, the pilot system is examined, and the underlying assets and threats are identified. Based on the input, the Core CTTP model is being created– by using the CTTP Models and Programmes Specification Tool - and the CTTP sub models (i.e. training programme, Emulation, Simulation, Gamification and data fabrication). Thereafter, the model contains sufficient information in order to instantiate a Virtual Lab in the THREAT-ARREST platform, as well as, to automatically evaluate the trainee's actions at runtime.

In general, the THREAT-ARREST approach is modelling-intensive, in the sense that it requires some effort to deploy the core CTTP model and Virtual Labs (emulated/simulated virtual instances of actual components) for an examined system. Nevertheless, it later becomes easier to deploy several variations of the scenarios and their number can be increased exponentially. The final version of these Models and Programmes will be developed in "D3.5 – Reference CTTP Models and Programmes Specifications v2".

The work presented herein is related to a number of projects KPIs, as mentioned below:

- **[KPI-7.1]** Provide effective CTTP Models and Programmes for all known attacks and standardised security assurance profiles of all the three pilot systems.
- **[KPI-7.2]** The developed CTTP Models and Programmes cover threats against: (i) key security property types (i.e., confidentiality (C), integrity (I), availability (AV) and authentication (AU)), (ii) key data states (i.e., data-in-transit, data-at-rest and data-in-processing), as well as (iii) physical and software components of cyber systems.
- **[KPI-7.3]** The developed CTTP Models and Programmes target and cover different types of trainees, including software engineers, security experts, system administrators, end users, security auditors, as well as Chief-Information-Officers (CIO) and Chief-Security-Officers (CSO). They also cover public and private systems users.
- **[KPI-7.4]** The developed CTTP Models and Programmes cover different types of action including preparedness, detection and analysis, security incident response and post security incident response.

Finally, the document is organised as follows: Section 2 outlines the current landscape in the assurance filed and the requirements of the pilot systems; Section 3 provides the programme definition for the three use cases; Section 4 includes the model specification and details the CTTP models; while Section 5 provides the concluding remarks. Appendix I summarizes the requirements for the three pilots as identified in the related D1.1.

2 Current Landscape

The development of the CTTP Models and Programmes will be based on existing assurance profiles and security assurance schemes, while also considering the existing security landscape in the pilot environments.

To accomplish this, subsection 2.1 includes the analysis of existing assurance schemes that could be linked to the three pilots' targeted systems, whereas subsection 2.2 comprises an analysis of the three pilots' targeted systems threats and controls, in order to identify the risks of the different types of components of these systems, and the safety controls used by them.

2.1 Existing Assurance Schemes

2.1.1 Assurance Profiles

The Common Criteria for Information Technology Security Evaluation (Common Criteria or CC [(ISO, 2009), (ISO, 2008)) is the technical basis for an international agreement (namely the Common Criteria Recognition Arrangement (CCRA)) which ensures that (Common Criteria : New CC Portal, 2020):

- Items can be assessed by skilful and autonomous authorized research centres in order to decide the satisfaction of specific security properties, to a certain extent or assurance.
- Supporting documents, are utilized inside the Common Criteria accreditation procedure to characterize how the criteria and assessment strategies are applied while guaranteeing explicit innovations.
- The certification of the security properties of an assessed item can be given by various Certificate Authorizing Schemes, with this certification being founded on the consequence of their assessment.
- These certificates are recognized by all the signatories of the CCRA.

As part of the analysis, four common criteria profiles were identified as suitable for the THREAT-ARREST pilots.

2.1.1.1 Protection Profile for the Security Module of a Smart Meter Gateway

This Protection Profile characterizes the security destinations and relating security prerequisites for the Security Module (TOE) that is coordinated as focal cryptographic unit in the Smart Meter Mini-HSM. Such Smart Meter Mini-HSM with coordinated Security Module is then proposed to be utilized by the Mini-HSM User through the associated Application Server for cryptographic help. The Target of Evaluation (TOE) portrayed here, is a Security Module as an electronic unit involving equipment and programming that is integrated in the Smart Meter Mini-HSM. Regularly, a Security Module is implemented in type of a smart card (yet is not constrained to that).

The TOE or Smart Meter Mini-HSM integrating the TOE respectively provides central cryptographic services and serves as secure storage for cryptographic keys and further (sensitive) data as these are relevant for the Mini-HSM User in a Smart Metering System for its communication with other involved components or parties (Bundesamt für Sicherheit in der Informationstechnik (BSI) / Federal Office for Information Security, Germany, 2017).

The above-mentioned protection profile is applicable in the Smart Home – IoT CTTP Models and Programmes definition.

2.1.1.2 File Encryption. Mitigating the Risk of Disclosure of Sensitive Data on a System

This Extended Package (EP) (Application Software Protection Profile (ASPP), 2014) defines security requirements for an encryption system (e.g. (Hatzivasilis et al., 2016; Hatzivasilis et al., 2015)) that can be configured for the data it encrypts, and is intended to provide a basic, baseline set of requirements aimed at mitigating well-defined and identified threats. However, this EP is not complete, but rather extends the Protection Profile for Application Software (National Information Assurance Partnership, 2014).

The above-mentioned protection profile is applicable for the creation of the Healthcare CTTP Models and Programmes definition.

2.1.1.3 Common Criteria Protection Profile – Mobile Card Terminal for the German Healthcare System (MobCT)

The Mobile Card Terminal (MobCT) (Jürgen Blum,Marion Brinkkötter, 2014) is a smart card terminal (TOE type) used for the German healthcare system. It is used during visits by medical suppliers to read out health insurance data and emergency data from a health insured person's user card (e.g. (Hatzivasilis et al. 2019a; Hatzivasilis et al. 2019b)). The data may be viewed further on a display or printed by the medical supplier.

The above-mentioned protection profile is relevant in the context of the Healthcare CTTP Models and Programmes definition.

2.1.1.4 Protection Profile for Signature Activation Protocol (SAP) management

This Protection Profile (PP) (ANSSI, 2016) defines the security requirements of a software that is used as a Sole Control Component (SCC) running on a Platform and used as part of its Trustworthy System Supporting Server Signing (TW4S) that generates advanced electronic signatures.

The above-mentioned protection profile is relevant for the creation of the Smart Shipping and Healthcare CTTP Models and Programmes definition.

2.1.2 Security assurance schemes

The common objective of each information security assurance schemes is to provide some form of assurance that sensitive data is effectively protected.

Holistic standards take a general, risk-based approach to information security by endorsing controls that legitimately neutralize an association's characterized security risks. More specifically:

- ISO/IEC 27001:2013 (International Organization for Standardization, 2018) is the international quality standard for Information Security Management. It assists with guaranteeing that satisfactory controls addressing the CIA triangle (i.e. confidentiality, integrity and availability) of information are set up to defend the information of interested parties.
- NIST Special Publication 800-53 rev. 5 (NIST, 2017) is a holistic information security standard developed by NIST. It is a set of standards and guidelines to help federal agencies and contractors meet the requirements set by the Federal Information Security Management Act (FISMA).
- COBIT (Control Objectives for Information and Related Technologies) (Isaca.org, 2019) is a holistic organizational security and integrity framework created by Isaca, that utilizes processes, controls objectives, management guidelines, and maturity modelling to ensure alignment of IT with business.

Other security assurance schemes are:

- The CPA Security Characteristic for Smart Metering – Communications Hub describes requirements for assured Smart Metering – Communications Hub products for evaluation and certification under NCSC's Commercial Product Assurance (CPA) scheme (CESG, 2017)
- The CPA Security Characteristic for Secure Real-Time communications client describes requirements for assured Secure real-time communications client products for evaluation and certification under NCSC's Commercial Product Assurance (CPA) scheme (CESG, 2016)

2.2 Threats & Controls in Piloting Environments

This subsection presents the modelling requirements for the three pilots. The following paragraphs briefly mention the pilots':

- Description
- Architecture
- Virtual Lab deployment
- Actuators
- Security landscape and Training Programmes

The initial input has been provided in D1.1, while the pilot setups will be detailed under the "WP7 – Pilots Implementation and Evaluation" activities. The related training and modelling requirements are also summarized in the Appendix I.

2.2.1 Smart Home - IoT

The Smart Home - IoT pilot is based on the system that Lightsource (LSE) has already installed in smart home deployments. Smart plugs collect the energy readings of the connected home devices, and through a local gateway, they exchange information with a private cloud at the backend. The houses have also installed solar panels that collect and distribute energy to the smart grid. Figure 1 depicts the main settings.

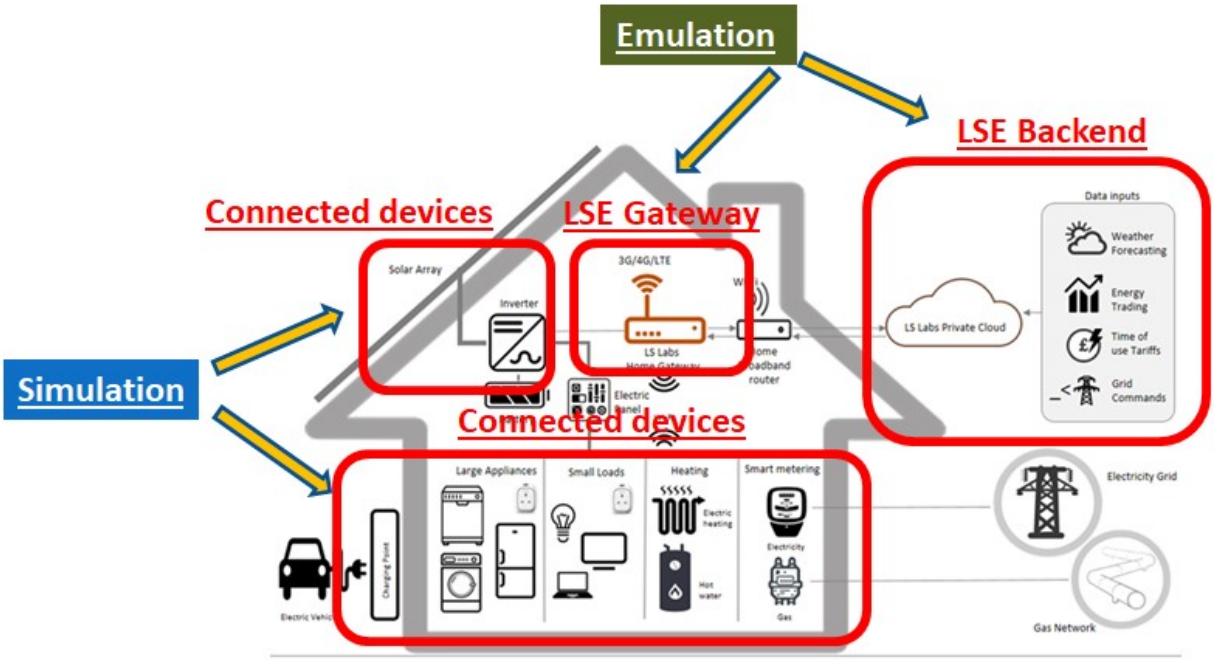

Figure 1. The Smart Energy pilot architecture and Virtual Lab deployment

For the deployment of Virtual Labs for the advance training with the Emulation and Simulation Tools, LSE's gateway and backend system will be emulated, while the operational behaviour of the smart devices and/or the solar panels at the home end will be simulated.

The main actuators here are the homeowners and the technicians who install and maintain the equipment at the edge system, as well as, the personnel of LSE in various roles (e.g. backend office employees, administrator, security expert, CIO, CSO, etc.). These roles also constitute the main trainee types considered under the THREAT-ARREST project. The first group includes trainees with zero to low security knowledge, while the LSE personnel mostly possess moderate to high cyber-security expertise. Therefore, 5 indicative scenarios have been designed, tackling the diverse training requirements for the different trainee groups.

In the current threat landscape, there are still a number of poorly secured protocols dating back to bygone technology eras when security was not a top concern leading to an easy-to-gain access and control of a person's smart device. The convenience of IoT devices and smart home hubs connected to the Internet is a double-edged sword, and there is a trade-off between ease-of-use and security.

Consumers need to be aware of the security concerns of connecting devices that control personal parts of their home to services they do not fully understand and the importance of properly configuring their devices. Industry-wide, better device-level security has been requested for IoT devices (ENISA, 2017). In order to ensure that the users' entire smart home ecosystem is secured, manufacturers need to develop IoT devices which are simple for consumers to set up and possess a high-level of security. Lastly, there is a need for more secure control solutions that allow consumers to confidently use technology in their homes with the confidence that it is secure, and their privacy protected.

2.2.2 Smart Shipping

The smart shipping pilot is based on the system of the DANAOS shipping company. This mainly includes the backend system at the organization's premises, along with the DANAOS communication platform (DANAOSone), as well as, the systems on the smart vessels and

their communication with the main system. Figure 2 depicts the pilot's architecture and main components.

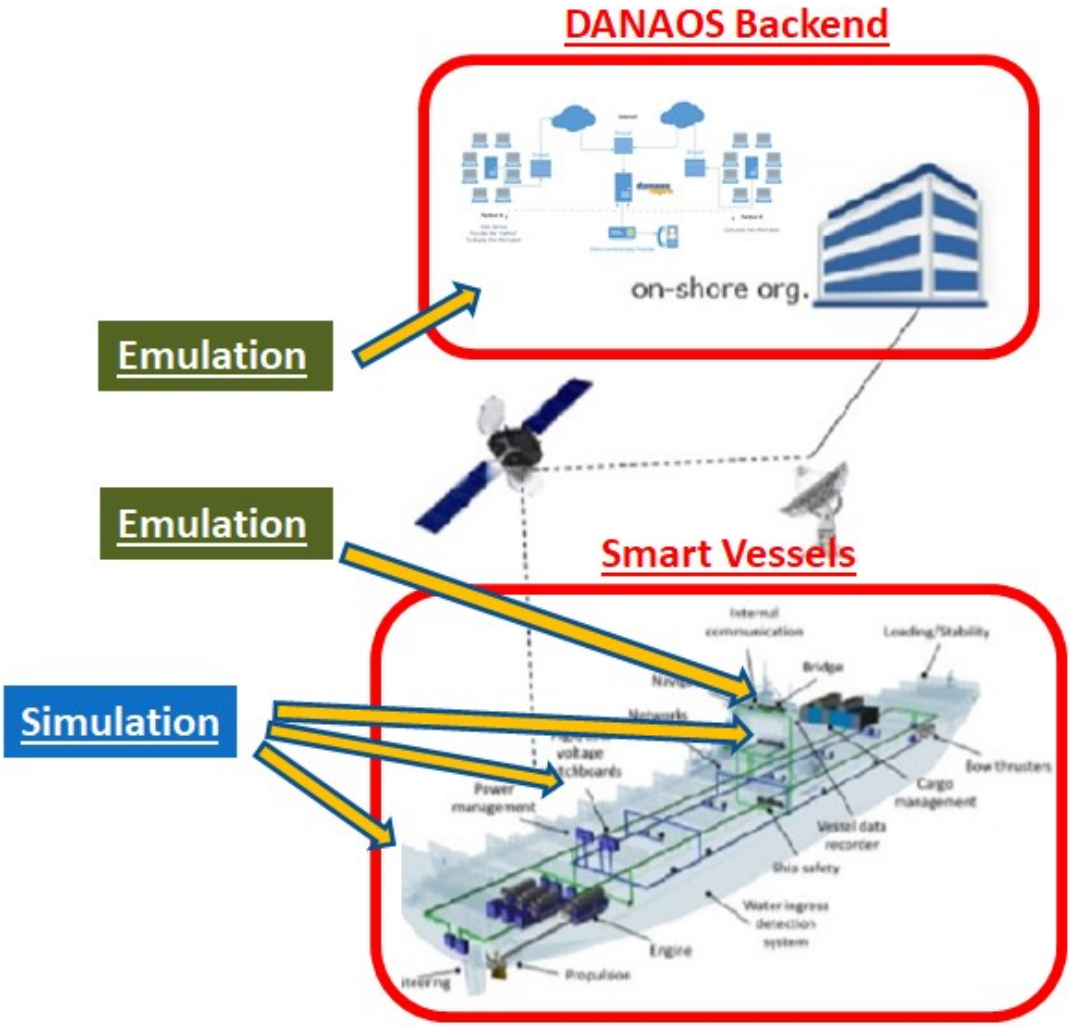

Figure 2. The Smart Shipping pilot architecture and Virtual Lab deployment

For the deployment of the main Virtual Labs under THREAT-ARREST, the backend system and the system of smart vessels will be emulated. The operational behaviour of the vessels on-board equipment (e.g. navigation modules, smart devices, etc.) will be simulated.

Therefore, the main users involve the backend employees (as in the first two use cases, e.g. office or administrative personnel, security experts, CSO, etc.), as well as, the captain and the crew of a smart vessel, who must be in position to face cyber threats even in the case where the communication with the backend systems / experts is not feasible. In general, the captain is a valuable actuator and he is the person in charge with the responsibility to take decisions for a potential ongoing cyber security incident in the vessel. Although he/she is not a security expert, he/she ought to possess sufficient knowledge in order to take the correct actions. On the other hand, the crew is ordinarily considered as users with low security awareness.

Shipping Company's staff have a key role in protecting Information Technology (IT) and Operational Technology (OT) systems. Training and awareness should be tailored to the appropriate levels for:

- on-board personnel including the master, officers and crew
- shore-side personnel, who support the management and operation of the ship.

An awareness or training framework should be in place for all personnel, covering at least the following **risk factors and awareness aspects**:

1. Risks related to emails and how to behave in a safe manner (examples are phishing attacks where the user clicks on a link to a malicious site).
2. Risks related to Internet usage, including social media, chat forums and cloud-based file storage where data movement is less controlled and monitored.
3. Risks related to the use of own devices (these devices may be missing security patches and controls, such as anti-virus, and may transfer the risk to the environment to which they are connected to).
4. Risks related to installing and maintaining software on company hardware using infected hardware (removable media) or software (infected package).
5. Risks related to poor software and data security practices where no anti-virus checks or authenticity verifications are performed.
6. Safeguarding user information, passwords and digital certificates.
7. Cyber Risks in relation to the physical presence of non-company personnel, e.g., where third-party technicians are left to work on equipment without supervision.
8. Detecting suspicious activity or devices and how to report if a possible Cyber Incident is in progress (examples of this are strange connections that are not normally seen or someone plugging in an unknown device on the ship network).
9. Awareness of the consequences or impact of Cyber Incidents to the safety and operations of the ship.

Applicable personnel should be able to **identify the signals when a system has been compromised**. The objective is to increase the security awareness in shipping ICT systems' operators, and security attacks and help towards identifying new threats which jeopardize the operations of ICT systems in the Shipping Management industry.

A secure network depends on the IT/OT set up on-board the ship, and the effectiveness of the company policy based on the outcome of the risk assessment.

Special attention should be given when there has been no control over who has access to the on-board systems. This could, for example, happen during drydocking, layups or when taking over a new or existing ship.

Cyber Security protection measures may be technical and focused on ensuring that on-board systems are designed and configured to be resilient to Cyber Attacks. Protection measures may also be procedural and should be covered by company policies, safety management procedures, security procedures and access controls.

Implementation of Cyber Security controls should be prioritized, focusing first on those measures, or combinations of measures, which offer the greatest benefit.

The guidelines for preventing deliberate attacks on ships and port facilities is defined in the International Ship and Facility Security Code ISPS adopted by the International Maritime Organization (IMO) in 2002 (IMO, 2004). DANAOS is also following the guidelines of the Center of Internet security (CIS) (CIS, 2020) to apply critical security controls to equipment and data on-board vessels.

2.2.3 Healthcare

The Healthcare pilot is based on the system of the AReSS Puglia (ARESS). It is a Regional Strategic Health and Social Agency with the goal to support the definition and management of social and health policies. The pilot system itself is the informatics of a Cancer Registry. The

system consists of a backend infrastructure that aggregates information (e.g. health records) from other collaborating healthcare organizations in the region. Figure 3 illustrates the pilot infrastructure.

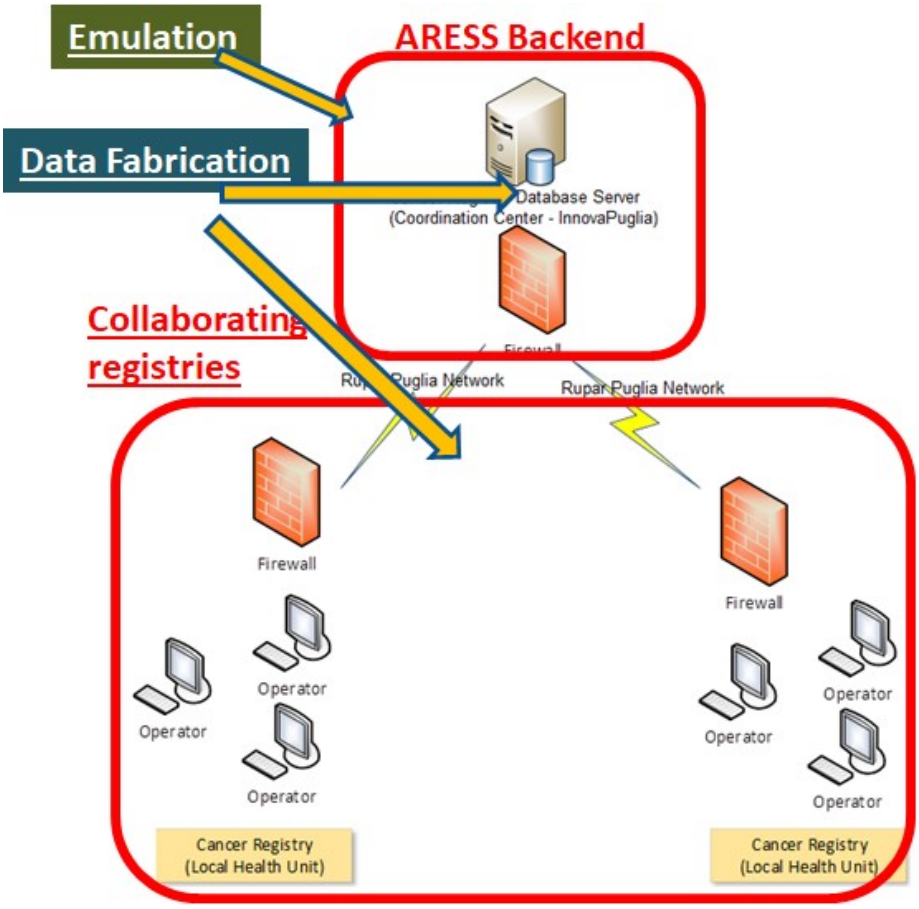

Figure 3. The Healthcare pilot architecture and Virtual Lab deployment

The information system that allows these organizations to work together reflects the structure of the Cancer Registry. The high-level architecture is described below.

- There is a virtual server at InnovaPuglia – the in-house IT partner of the Region – which hosts the Cancer Registry database. This database contains the cases of cancer of the population living in Puglia and the related personal health data.
- Members of the teams in the Local Health Units use a client desktop application that connects to the database in order to enter data and for consultation purposes.
- The exchange of data between clients and the database server takes place on a secure connection on top of the "RUPAR Puglia" network, a network that connects the IT centers and the devices of the regional public and health institutions of Puglia.

As access to the systems of the collaborating organizations is not possible, the deployment of the main Virtual Labs under THREAT-ARREST will include the Emulation of the operation of the backend system. The operation and networking of the rest of the infrastructure will be simulated under the IBM's Data Fabrication Platform (DFP), which will produce realistic log-files for the advance training with the emulated backend.

Thus, the main actuators in this use case are the personnel of ARESS. This includes office, IT, and administrative employees, system and network administrators, security experts, and

CSOs. These are also the considered trainee groups for the documented CTTP Programmes. Here again, the first group includes system operators and trainees with no to low security knowledge, while the second group includes system administrators and personnel with moderate to high cyber-security expertise. Henceforth, 4 main scenarios are designed to cover the requirements for the different Training Programmes.

Today, cyber security is the biggest obstacle and challenge to the efficient evolution of the healthcare sector. It is therefore necessary to provide this sector with appropriate solutions that can restore a climate of trust in digital innovation by ensuring the highest levels of security and privacy for the data of all those involved. In consideration of its enormous amount of sensitive data, some of the common threats are:

- Security gaps in database containing sensitive data (data concerning health) systems
- Loss of control over computer systems
- Unauthorized access to information systems that would jeopardize the health and personal data of patients as well as the organisation itself.

Each of these threats may violate a security property of the system, such as the:

- Availability, i.e. protection of information assets in the guarantee of access, usability and confidentiality of data. From a security management point of view, it means reducing to acceptable levels the risks connected with access to information (intrusions, data theft, etc.).
- Integrity, intended as a guarantee that the information will not be modified or deleted as a result of errors or voluntary actions, but also as a result of malfunctions or damage to technological systems.
- Confidentiality, i.e. management of security in such a way as to mitigate the risks associated with access to or use of information in an unauthorised manner.
- Privacy, i.e. information is intelligible only to its rightful recipients.

With the increase in networked objects in the hospital environment, the healthcare sector is also increasingly becoming a victim of Cyber Crime. For this reason, the European Union Agency for Network and Information Security (ENISA) published on 24 November 2016 “Smart hospitals - Security and resilience for smart health service and infrastructures” (ENISA, 2016), which proposes some key recommendations for information security in the world of health, particularly in hospitals.

The research, carried out with the support of experts from different sectors, focuses first on documents and empirical data, and then analyse potential attack scenarios, such as attacks on hospital staff through social engineering techniques, tampering or theft of equipment or medical devices, ransomware attacks and DDoS attacks.

The document also proposes some 'recommendations' and best practices, both organisational and technical. These include precisely indicating roles and responsibilities for security; creating Cyber Security policies and procedures; developing training and awareness programs; identifying risks, resources and threats; drawing up contingency plans; adopting high standards; conducting consistent security audits; and using contractual clauses with suppliers; implement intrusion control; increase the use of firewall equipment; use anti-malware software; make regular data backups; best configure and manage resources; use update procedures; strengthen user access control; enforce the use of encryption (e.g. (Manifavas et al., 2015; Manifavas et al., 2013)); and classify data and protect remote and mobile health systems.

3 Programmes Definition

This section aims to specify the initial training scenarios that will be used as the baseline training programmes for each of the covered domains. In total 13 scenarios are specified, 5 for the Smart Energy, 4 for the Healthcare, and 4 for the Smart Shipping pilots.

3.1 Smart Home – IoT

Table 1 summarizes the main features of each scenario defined for the Smart Home - IoT environment.

Table 1. Overview of Smart Home/IoT scenarios

#	Description	Trainee type	Tools
1	Response & Mitigation	Homeowner	• Emulation • Simulation • Gamification
2	Secure Configuration	Technician	• Emulation
3	Bad Actor – Cloned Gateway	Administrator	• Emulation
4	Compromised Gateway - Botnet	Administrator	• Emulation • Gamification
5	Attacks on the Backend System	Administrator; Security Auditor;	• Emulation • Assurance tool

3.1.1 Scenario 1 - Response & Mitigation

3.1.1.1 Description

As the owner of a smart plug, the web based Lightsource application allows you to monitor its power consumption and/or its on/off behaviour. It also provides alerts of the system if an abnormal behaviour is detected. An intruder has gained access to your smart plug and executed a malicious application which stopped the smart plug from reporting its power consumption and turned a switch on and off at random time points. You were notified by an alert, through the web application, that an abnormal behaviour was detected, and you are asked to read the Lightsource guideline provided during the setup phase, in order to bring the device back to its expected behaviour.

This scenario trains an end user with no security knowledge on how to response to an abnormal behaviour and take immediate actions in order to mitigate the risk. The scenario is implemented in the **Emulation, Simulation** and **Gamification tool**.

3.1.1.2 Progression

I. The trainer sets up the gateway and provides the log files and the database schema that contains the end users' credentials (in an encrypted form) and the IP of the smart plug. He also sets up the private cloud that provides the alerts to the web-based application of the trainee.

II. The trainee is informed about the security concerns surrounding smart devices and, upon installation of the edge device, receives an incident response and abnormal behaviour guideline.

III. The trainee receives an alert to its web-based application letting him/her know that the smart plug stopped reporting the power consumption and that the device connected to it reports abnormal on/off patterns. The trainee opens the web-based application to check if the alert was correct.

IV. The trainee reads the guideline and, as instructed in the first step, resets the smart plug to its factory settings by pressing its button for 10 seconds. Then, he checks the graphs presented in the web application, but he observes that the abnormal behaviour is still there (i.e. no power consumption is presented).

V. The trainee then moves to the second step of the guideline and resets the device itself.

VI. Finally, the trainee checks the graphs, and observers that both the smart plug started reporting its power consumption and the connected device was not reporting abnormal behaviour.

3.1.1.3 Scenario Modelling

For the purposes of this scenario the **Emulation tool** facilitates the following VMs:

- Gateway VM with log files and database schema preinstalled.
- The VM for simulator.
- The private cloud
- The trainee PC that includes a web browser

The **Simulation and visualisation tool:**

- Simulates the smart plug and a button for the device connected to it.
- Three different phases are presented:
    - Normal Behaviour
    - Faulty/Compromised smart plug device
    - Compromised Device

The **Gamification tool:**

- Presents a game for smart home security awareness

The **training tool includes**:

- A short course for security awareness in general
- Lightsource' incident response guideline

3.1.2 Scenario 2 – Secure Configuration

3.1.2.1 Description

As a technician, you are in the process of commissioning a new installation. During the gateway setup stage, the provisioning application notifies you of a possible misconfiguration in the distributed firewall policy on this gateway. Such situations arise from either the security policy not being applied (service not running) or from an old version of the policy that is shipped with the selected gateway. Since a gateway must be configured with the correct firewall policy you are asked to investigate the current security setup and restore the correct policy.

This scenario trains technicians on how to practically secure a system affected by such incidents. The scenario is implemented in an **Emulation tool**.

3.1.2.2 Progression

1. The trainer sets up the gateway and the machine for the technician to use.
    a. The gateway does not have the distributed firewall installed.
    b. The provisioning application is set to detect a misconfigured firewall.
2. The technician runs the provisioning application which triggers a misconfigured firewall notification.
3. The technician proceeds to log into the gateway and inspect the configured firewall.
4. Since the firewall is not present, the technician proceeds to install the correct package and configure the firewall.
5. He validates that the gateway complies with the security policy and proceeds with the provisioning.

3.1.2.3 Scenario Modelling

For the purposes of this scenario the **Emulation tool** facilitates the following VMs:

- Gateway VM with missing firewall.
- Technician PC with provisioning software.

3.1.3 Scenario 3 – Bad Actor – Cloned Gateway

3.1.3.1 Description

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

This scenario trains a member of the administrator team on how to practically secure a system affected by such incidents. The scenario is implemented in an **Emulation tool**.

3.1.3.2 Progression

I. The trainer (USER4) sets up the backend infrastructure and launches 2 instances of the same gateway which run the exact same configuration.

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

III. An administrator notices the alert raised by the Intrusion Detection System.

IV. He gathers information about the incident, assesses the cause and nature of it and determines no (personal) data has been breached, and informs the legal department of such conclusion.

V. He revokes the security credentials associated with the gateway and generates new credentials.

VI. He logs in over 3G to the affected gateway and changes the old credentials to the new ones.

VII. The gateway software is restarted which in turn uses the new credentials to connect to the backend.

VIII. The administrator logs into the backend system and validates that the Intrusion Detection System no longer alerts.

3.1.3.3 Scenario Modelling

For the purposes of this scenario the **Emulation tool** facilitates the following VMs:

- Gateway 1 VM with fixed 3G IP (simulated SIM card).
- Gateway 2 VM without fixed 3G IP (no SIM card).
- VMs that takes the roles of the Backend System.
- Administrator PC

IBM's Data Fabrication tool generates the data required by backend system and gateway to support normal/misconfigured/malicious behaviour.

3.1.4 Scenario 4 – Compromised Devices - Botnet

3.1.4.1 Description

An alert is raised on the backend system by a gateway that is reporting higher than normal resource usage (CPU, RAM). Since the resource usage is always within the configured thresholds, this is an early sign that the gateway is not operating under normal circumstances. As a member of the administrators' team, you are urgently called to investigate the alert. All gateways are accessible over VPN. Connect to the affected gateway and validate the integrity of its configuration.

In this scenario the administrator learns about common malware linked to botnets and their characteristics; attacks enabled by botnets; best practices to prepare, prevent, mitigate and post breach identify infected systems; and, indications that a system is compromised (part of a botnet). Then the user analyses different patterns of behaviour (traffic, system logs) to identify botnet malware infection. The scenario is implemented in the **Emulation** and **Gamification** tool.

3.1.4.2 Progression

I. The trainee is educated about the security concerns surrounding botnets, by answering question cards. More precisely, the trainee is now aware about common malware linked to botnets and their characteristics; attacks enabled by botnets; best practices to prevent, mitigate and post breach identify botnet infected systems; procedures on how to respond to security incidents and personal data breaches and, indications that a system is compromised (part of a botnet).

II. The trainee notices that an alert is raised by the gateway on the backend system. Upon further investigation, the trainee notices that this alert is related to particular gateway and proceeds to connect to the gateway over VPN for further analysis.

III. The gateway logs do not show any signs of compromise, just high resource usage. Investigate possible misconfigurations on the gateway.

IV. Check known botnet targets and devices connected to the gateway (for example VPNFilter targets some NETGEAR, Linksys and more routers).

V. A high amount of traffic is coming to the gateway from one of the smart plugs.

VI. Upon closer inspection of the smart plug, it is identified that the device has been compromised and the malware is now trying to propagate to the gateway.

VII. The trainee gathers further information on what happened and determines that personal data were involved and creates a report.

VIII. The trainee fears the incidentis a personal data breach and notifies the internal incident response team by submitting a report including:

   a. Details of the incident (i.e. nature/type of incident, cause of incident, circumstances in which the incident was discovered, description of the data affected, description of data subjects affected, approximate number of records and data subjects affected, etc.)

   b. A description of the likely consequences of the incident

   c. A description of the measures taken or proposed to be taken to address the incident, including where appropriate measures to mitigate adverse effects

The trainee, in cooperation with the incident response team, stops the malware running on the smart plug and restores the smart plug to the original state by removing the malware.

3.1.4.3 Modelling

For the purposes of this scenario the **Emulation tool** facilitates the following VMs:

- Simulated smart plug with malware.
- Gateway VM.
- VMs that takes the roles of the Backend System.
- Administrator PC

IBM's Data Fabrication tool generates the data required by the devices to support normal/misconfigured/malicious behaviour. **The Gamification tool** provides learning content for known security awareness countermeasures to prevent the corruption of IoT devices by botnets.

3.1.5 Scenario 5 – Attacks on the Backend System

3.1.5.1 Description

The backend system maintenance team has been notified that there are a number of vulnerabilities currently present in the environment. As a member of this team, administrators and security auditors are asked to identify and secure the environment within 5 hours. Once this time elapses, attackers will look to compromise the system and gain access to restricted assets.

This is a capture the flag (CTF) type scenario, where the trainer injects vulnerabilities to targeted emulated components of the smart home environment. The blue team is then called to find the vulnerabilities and secure the system, given a predefined time frame. Upon the expiration of the time frame, the red team may try to exploit the target system. The red team will have an agenda that will include finding hidden text files representing sensitive data in restricted places of the system, altering user/admin accounts, creating new accounts, changing access rights. The scenario will be implemented in the **Emulation** and **assurance tool.**

3.1.5.2 Progression

I. The trainer sets up the backend infrastructure
   a. Inject vulnerabilities
   b. Specify the evaluation mechanisms
II. The trainees inspect the overall setting and perform mitigation actions within the time limit allocated, taking into account the sensitivity of the data.
III. The platform monitors evaluate if the related actions were performed and inform the trainers
IV. The CTF exercise begins and the trainer triggers the attacks.
V. The trainees try to defend the system.
VI. The exercise is completed, and the results are evaluated.

3.1.5.3 Modelling

Before the exercise starts, the trainers are required to setup a backend infrastructure that includes:

- An MQTT service listening on an insecure port
- A relational database with a default (weak) username/password.
- A time-series database with no SSH login security.
- And a RESTful API with an open backdoor URL endpoint.

Restricted access assets are identified and agreed with in advance. These include but are not limited to time series data in transit (MQTT), time series data at rest and relational data.

Two VMs are configured to be used by the blue team when looking to patch and defend the system.

Once the predefined limit has expired, the trainers will initiate an attack from an outside VM that looks to exploit the vulnerabilities listed above. Success and failure are calculated based on the success of the attack.

3.2 Smart Shipping

Table 2 summarizes the main features of each scenario defined for the Smart Shipping environment.

Table 2. Smart Shipping Scenarios

#	Description	Trainee type	Tools
1	Navigation combo attack (phishing email and GPS spoofing)	Captain (highly-privilege actuator with low/moderate security knowledge)	• Emulation • Simulation • Gamification
2	Vishing (social engineering)	Crew / Offshore officers (non-security actuators with low access privileges)	• Training • Gamification
3	Digital Forensics	The organization's security engineers (security experts)	• Emulation • Simulation • Data Fabrication
4	Attacks on the Offshore system	IT Administrators of the shipping company (highly-privilege actuators with moderate/high security knowledge)	• Emulation • Assurance tool

3.2.1 Scenario 1 – Navigation combo attack (phishing email and GPS spoofing)

3.2.1.1 Description

This is a social engineering scenario which targets valuable actuators with moderate security training, more specifically the captain of the ship. The scenario consists of two different phases. During the first phase, a set of malicious / faulty / 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 has 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.

This scenario trains an end user with moderate security knowledge. The scenario is implemented in an **Emulation, Simulation and Gamification tool**.

3.2.1.2 Progression

All referred actions test the captain's decision making.

- The trainee must start a journey from the Heraklion port to Piraeus (which will be designated by the backend office via an email to the captain).
- A faulty (but legitimate) email, commanding the captain to go to the Thessaloniki port, is being sent. The email contains the details of another journey and was sent to the trainee by mistake.
    - The trainee identifies that this is a legitimate email.
    - Since the destination port was Piraeus, the trainee understands that this email was sent to him/her by mistake.
    - The trainee ignores the email and reports it back to the backend office.
- Then, the trainee receives a malicious (phishing) email, alerting him/her that a bad weather condition will take place, thus, he/she needs to go to another port to make a stop.
    - The trainee identifies that this is a phishing email.
    - Ignores the email and reports it to the backend office.
- Lastly, the captain receives a legitimate email with the weather forecast, denoting that the weather is good, and the destination is the Piraeus port.
    - The trainee understands that this is a legitimate email and starts the journey.
- During the trip, the trainee checks a simulated digital map that presents the current ship's position based on GPS data and the predetermined route (checkpoints) from Heraklion to Piraeus. The trainee suddenly realizes that the ships position on the digital map (receiving signal from a GPS receiver) is away from the designated waypoint and the ship is off course. The trainee should check if this is due to his own navigational orders or due to external factors (strong current streams) and should correct course by returning to the predetermined route or, if something is wrong, with the navigational monitor (digital map). The trainee proceeds with an order of actions to validate position from the GPS signal.
- The trainee checks a magnetic compass and the marine paper map (Nautical Charts), in order to understand the actual / "true" position of the ship.
- While checking the compass, he/she understands that it points towards a different direction to the ship course. Following, the trainee marks on the Nautical Charts the position as depicted in the GPS (faulty coordinates). Then, the trainee is crosschecking objects (navigation aids, restrictions, bathymetry) mapped on charts with what he observes by looking outside the ship's bridge windows with his binoculars and with what he receives from other bridge equipment (e.g. bathymetry on the map against see depth from echo sounder). The trainee understands that the ship is navigating on different waters than those corresponding to the position given by GPS (faulty coordination).
- Finally, the trainee understands that a GPS spoofing attack might have occurred, stops following the Digital Map Application (received signal from GPS receiver) and manually navigates the ship to its correct destination (by turning off the auto pilot).

The emails will be sent either automatically based on triggered events (e.g. timestamps) or manually by the trainer. Moreover, the message types (legitimate, faulty, or malicious), as they are defined for the aforementioned scenario, can be altered between different training sessions.

3.2.1.3 Scenario modelling

For the purposes of this scenario the **Emulation tool** facilitates the following VMs:

- The trainee operates the VM for the captain's PC.
- The faulty/malicious and legitimate messages are being sent by the VM that includes the trainer's mail application.
- The Simulation and visualisation VM.

The **Simulation and visualisation tool:**

- It contains the simulated on-deck navigation equipment, i.e. the Digital Map (GPS Receiver), the magnetic compass and the Nautical Charts

The **Gamification tool:**

- Presents a game for social engineering.

The **training tool includes**:

- A short course for social engineering.

3.2.2 Scenario 2 – Vishing

3.2.2.1 Description

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

The scenario is implemented solely in the **Gamification tool** based on teaching material that is included in the **training** procedures.

The trainees answer questionnaires and try to choose the proper action that must be performed. The trainee is evaluated under a series of sub-cases, like the interaction with:

- (potential) organization employees
- third-party suppliers
- other

3.2.2.2 Progression

- Vishing with the aim to target Crew:
  - Call over the phone and pretend to be back office staff
  - Get them to install malicious software from website or USB stick
- Vishing with the aim to target offshore Backoffice:
  - Call over the phone pretending to be a lead IT admin (or other key personnel) and get them to install a "patch" on the backend server
  - The attacker can use the backdoor installed by the "patch" to send malicious data to the ship via remote connection

3.2.2.3 Scenario modelling

The scenario will be solely implemented by the Gamification tools. The trainee will have to answer related security questions and choose the appropriate action that must be performed. The following options will be modelled:

- Fake Third-Party Service Provider in Port
  - Come on board with a fake maintenance laptop or USB stick
  - Install it on the ships system
- Maintenance staff
  - clean tanks and perform planned maintenance job orders on vessel machinery properly and interval
  - check the data is manipulated
- Real Third-Party Service Provider has infected IT equipment (**target:** crew)
- Corrupt data for pollution levels, maintenance of the ship etc. (**target:** crew) entered via unprotected network)
- GPS Spoofing and manipulated navigation with replicating GNS spoofing/jammer equipment, capable of "tricking" the GNSS signal by sending dedicated signals that the GNSS will interpret as genuine and consequently will show a wrong position. This attack is usually triggered from ashore, when a vessel is in line of sight from the coastline or from a moving platform by air with the use of a drone or at sea with a transmitter located on board a small boat sailing close to the target (**target**: Captain, First Officers)
- USB port of Powerline Connection (PLC) controller software abused by connected mobile phone that got infected beforehand (**target:** crew)

3.2.3 Scenario 3 – Digital forensics

3.2.3.1 Description

This is a digital forensics scenario where the organization's security experts have to perform a digital investigation on the ship's cyber infrastructure when the vessel is in the port. The crew have reported that the sensory equipment displayed abnormal values during the last trip and called the organization's experts to examine the cyber components. The scenario targets security experts with high security training, who must check if the machinery, sensors or data acquisition aggregators, network configuration works properly, are malfunctioning, or are compromised. Furthermore, the security experts should assess whether the technical and organizational measures deployed on the cyber infrastructure effectively ensure a level of security appropriate to the risk and are in line with applicable policies and requirements.

The scenario is deployed on the **Simulation** and **Emulation tools**. Moreover, several log files in both tools are generated by the **IBM's Data Fabrication tool**. The VMs that emulate the captain's PC or the crew's personal devices could have pre-installed unauthorized or even malicious software. On the other hand, all the on-deck simulated modules maintain local logs that store the latest sensed events. As aforementioned, for most operations, there are redundant/alternative mechanisms that the trainee can correlate and check the legitimacy of each simulated module.

3.2.3.2 Progression

All referred steps evaluate the security experts' knowledge.

- Perform digital forensic analysis for the emulated operating systems (OSs). There are three potential cases:
    1. Everything is normal
    2. Unauthorized software has been installed but no malicious actions have been performed
    3. Unauthorized software is detected, and the malicious effects must be identified
- Assess whether the technical and organizational measures deployed on the cyber infrastructure ensure a level of security appropriate to the risk and are in line with applicable policies and requirements
- Check the local log file of each simulated component
- Correlate the local log files of related simulated components

3.2.3.3 Scenario modelling

For modelling the scenario, 2 VMs that emulate the captain's PC and the crew's personal devices were deployed, and 1 Virtual Machine that runs the simulator for the on-deck monitoring and management infrastructure. The trainee executes specialized software and conducts digital investigation on the first two VM types, while in the third case, he/she analyses the local logs.

The trainer adjusts the three VMs beforehand. He/she chooses the faults and/or malicious traces that will be injected in and the trainee has to discover them.

3.2.4 Scenario 4 – Attacks on the Offshore backend system / Capture the flag

3.2.4.1 Description

This is a capture the flag (CTF) scenario where the organization's IT administrators try to defend the offshore backend system against ongoing attacks (performed by the trainers). The scenario evaluates these highly privileged actuators with moderate/high security expertise in responding to real attacks. At first, the trainers set the emulated environment of the backend system and inject vulnerabilities in it, which will be later exploited at the evaluation phase. Then, the trainees are given a few hours or one day in order to explore the overall setting, detect vulnerable points, and perform mitigation actions (e.g. system updates, patching, etc.). When this period elapses, the two teams get ready and the attacks begin. The red team tries to disclose specific assets that have been agreed with the blue team before the exercise. If the attackers manage to access or manipulate these assets, the defenders lose points.

The scenario is implemented in the **Emulation tool**, while **real equipment** (e.g. email server) can also take part. As aforementioned, the VMs that emulate the backend system are instantiated. The trainers inject specific vulnerabilities, like default username/passwords, services that use no encryption, outdated software versions, vulnerable system settings and configurations, software flaws in the organization's software (i.e. SQL injection or cross-site scripting (XSS)), pre-installed unauthorized software, disabled security mechanisms or lower levels of secure operation, etc. For each one of these threats, there is one related mechanism that evaluates if the trainee has performed the proper mitigation action. These mechanisms are implemented:

i. either as platform monitors (i.e. via the assurance tool), which are triggered when the

trainee performs the correct action (i.e. activate a disabled protection mechanism)

ii. or as events/attacks that are triggered by the trainer (i.e. try to login the system with the default username/password).

When the CTF exercise is over, the THREAT-ARREST platform surveys the trainees' achievements.

3.2.4.2 Progression

- The trainers set up the involved VMs or the real equipment
  - Inject vulnerabilities
  - Specify the evaluation mechanisms
- The trainees inspect the overall setting and perform mitigation actions
- The platform monitors if the related actions were performed and informs the trainers
- The CTF exercise begins and the trainers trigger the attacks
- The trainees try to defend the system
- The exercise is completed, and the results are exported

3.2.4.3 Scenario modelling

For modelling the CTF scenario, 3 VM types are needed. The trainees must defend the VMs (and/or real equipment) that represent the backend infrastructure, i.e. the servers or the backend office PCs. The trainers operate the attacker's VM, which launches the triggered attacks.

3.3 Healthcare

Table 3 summarizes the main features of each scenario defined for the Healthcare environment.

Table 3. Overview of Healthcare Scenarios

#	Description	Trainee type	Tools
1	EHR – Incident Response	Incident responder Security experts	• Simulation • Emulation • Data Fabrication • Gamification
2	EHR– Social Engineering	Medical Staff	• Emulation • Data Fabrication • Gamification
3	EHR - Secure	Administrator	• Emulation

	Configuration	Security experts	• Gamification
4	Procedures	Tech Staff	• Emulation • Simulation

3.3.1 Scenario 1 – Incident Response

3.3.1.1 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.

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.

3.3.1.2 Progression

All referred actions test the security's expert decision making.

I. The database event log shows that a specific clinician's credentials were used to access the hospitals internal application and the contents of the patients' database table were retrieved. This access happened out of office hours. The trainee uses a training environment as a workstation for his investigation.

II. Upon interviewing the doctor, the trainee identifies that the credentials were retrieved through a malware and he begins investigating the application log files.

III. Traces of keylogging activity are detected on the PC (keystrokes log) that hosts the internal application and, upon further investigation, a keylogger is found. The trainee understands that this happened due to an unknown USB device used by the clinician.

IV. The trainee then gathers further information on what happened and whether personal data were involved by examining the log files of the database. He/she identifies that several sensitive data were exported from it.

V. The trainee utilises the web tool that handles the administration of the database to:

   I. Find the user table and set the security flag values (i.e. accountNonExpired, credentialsNonExpired and accountNonLocked) to false. This action immediately disables the clinicians account.

   II. Find the tables that store the permissions of each user and revoke the clinician's read and write permissions by removing his/her ID from the table.

VI. The trainee then sends an email to the clinician asking him/her to immediately change the password. He/she also includes a text that informs the clinician on how to setup a strong password.

3.3.1.3 Scenario Modelling

For the purposes of this scenario the **Emulation tool** facilitates the VM for the simulator and the VM that hosts the database and an email client. The simulator's VM runs **the Simulation tool** (i.e., Jasima) that acts as an event captor and notifies the training tool of the trainee's performed actions. **IBM's Data Fabrication tool** generates the data required for the user and permissions tables and the log files for the database and application server. The Gamification tool provides learning content regarding the responses of the trainee corresponding to general security incidents.

Accordingly, in the game the trainee would have to select the card with the correct response activities for an incident. Lastly, the training tool provides a short course for incident response actions to the trainee.

3.3.2 Scenario 2 – Social Engineering

3.3.2.1 Description

This scenario examines various social engineering incidents that the healthcare sector is prone to. Such as, "It has been detected that some of the patients' Electronic Health Records (EHR) have been manipulated and doctors issued false treatments based on this". This scenario aims to train non-security expert users such as medical staff (i.e., doctors).

This scenario is implemented in **Emulation** and **Gamification**, while the data (e.g., emails) are generated using **IBM's Data Fabrication tool**.

3.3.2.2 Progression

All referred actions test the non-security expert's decision making.

I. You receive a call from a new doctor of staff, asking you to update the EHR record of patient Jon Doe with new health values, due to the recent symptoms the patient exhibited. You answer questionnaires and must choose the appropriate course of action.

II. While checking your email, you locate an email with subject "Staff Planning for 2020" and an excel file attachment with the same name. You open the email and investigate. Upon opening the attachment, you lose points; While opening the file, excel asks you if you want to enable macros, if you answer "YES", the malicious code runs, and you fail.

III. While checking your email, you locate an email from the IT department warning about a compromise of their systems; the IT department suggests that all users must change their password via a secure portal (via a link that they provide in the email) as soon as possible. The email address appears legitimate. Upon clicking the link, you are issued a warning that you are about to enter an external site. If you continue, you lose points; then a password changing page with the company's logo is presented, requesting only for the current password and a new one. If you type in your current credentials, the training fails.

3.3.2.3 Scenario Modelling

For the purposes of this scenario **the Emulation tool** facilitates the VM for the training (VM-Training) and a VM for the attacker. VM-Training has deployed an emulated email; VM-Attacker has deployed an emulated web server that is used for the credentials harvesting. The **Data Fabrication tool** generates the mailbox, including the excel file. Finally, the Gamification tool is used to sensitize the medical staff of a local health unit against social engineering attacks.

3.3.3 Scenario 3 – Secure Configuration

3.3.3.1 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 in 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.

This scenario trains the system administrator or a security expert how to practically secure a system affected by such incidents. The scenario is implemented in **Emulation** and **Gamification tool**.

3.3.3.2 Progression

All referred actions test the system's administrator skills with regards to incident response.

I. Identify attack vectors. Discover open ports accessible from outside. Which services are running on those ports? Define which services are not secured with encryption. Determine and use tools to identify those attack vectors. (by using specialized software installed in training VM to assess the vulnerable machine).

II. Determine vulnerabilities (telnet service, outdated SQL database, unencrypted communication with frontend including user credentials and health records). The trainee uses specialized software installed in the training VM to assess the vulnerable VM.

III. Determine how to minimize attack vectors. This involves closing unnecessary ports and services such as telnet. Adjust the firewall rules and server configuration accordingly. Update SQL database. Harden the security of the vulnerable VM.

IV. Determine from the log if there is need for an IDS/IPS to get an early warning about attacks ongoing in the system. What should the IDS be monitoring? Anomalies to detect activities outside office hours, exceptionally high database traffic, DOS attack, brute force/dictionary attacks on the database (The trainee uses the Gamification tool to answer relevant questions).

3.3.3.3 Modelling

For the purposes of this scenario the **Emulation tool** accommodates the VM that is used as the training environment and a VM that is used as the vulnerable machine. The training machine has preinstalled all the software needed for this scenario; similarly, the vulnerable

VM comes preinstalled with all software (e.g., Firewall) and is configured accordingly (e.g., open ports, services running, vulnerable components). Finally, the **Gamification tool** is used to respond to present and answer relevant questions.

3.3.4 Scenario 4 – Procedures

3.3.4.1 Description

The director of one of the hospitals has changed and the accreditation process still is not concluded. The director calls the Tech staff for the release of new credentials to access the database using the client software, since he needed an urgent access to the data. An attacker can try to impersonate the director sending a fake accreditation and leveraging the urgency and delay in the process. The hospital's medical staff access the database via a 3rd party application, while an SQL server runs at the back end.

This scenario aims to train tech staff appropriate procedures with regard to account creation and credential sharing. This scenario is driven by a trainer (Red team - Attacker) that interacts with the user (Tech staff - Blue team); the trainee must follow the correct procedure to give or not credentials to the requester. The scenario is implemented in the **Emulation** and **Simulation tool.**

3.3.4.2 Progression

I. John Doe (Trainer) sends an email to Bob, the Tech staff (trainee), claiming to be the new director of one of the hospitals. He asks for the release of new credentials to access the database using the client software, since he needs an urgent access to the data.

II. (alternative scenario) Alice (Trainer), the doctor secretary, calls Bob since she lost the doctor password

III. Bob (Trainee) is reluctant to give to John Doe (Trainer) the credentials and calls (i.e., emails) Alice, a secretary of the hospital he knows to get references.

IV. Alice is not at work but an unknown colleague (Trainer) confirms (i.e., by email) that John Doe is the new director.

V. Bob (Trainee) accepts to create a new account and sends to John Doe the credentials.

VI. John Doe (Trainer) uses the credentials to access the database.

3.3.4.3 Modelling

For the purpose of this scenario the Emulation tool enables the training environment used by the trainee, the attacker's environment and the simulator. An emulated email client is deployed on the training VM; An emulated email server and an emulated email client is deployed on the Attacker's VM. The simulator supports the system's database, in which upon entering specific credentials you get a successful login message or an unsuccessful one.

To mitigate the risks highlighted in this scenario, appropriate **Security Controls** have to be selected.

- Social engineering/phishing attack training for medical staff

- Proper server configuration training for admin staff (no telnet access, no remote access directly into SQL server etc.) & introduction of Intrusion Detection/Prevention Systems to alert in case of suspicious (e.g., out of office hours traffic).
- Training of tech staff on the proper procedures related to handling of personal data in accordance with the GDPR and internal policies.

4 Scenario Models Specification

As part of this deliverable, a model specification for one scenario description per programme definition will be included. More complex models and scenarios will be presented during the 2nd version of this deliverable, i.e. "Reference CTTP Models and Programmes Specifications v2" which is due in month 30.

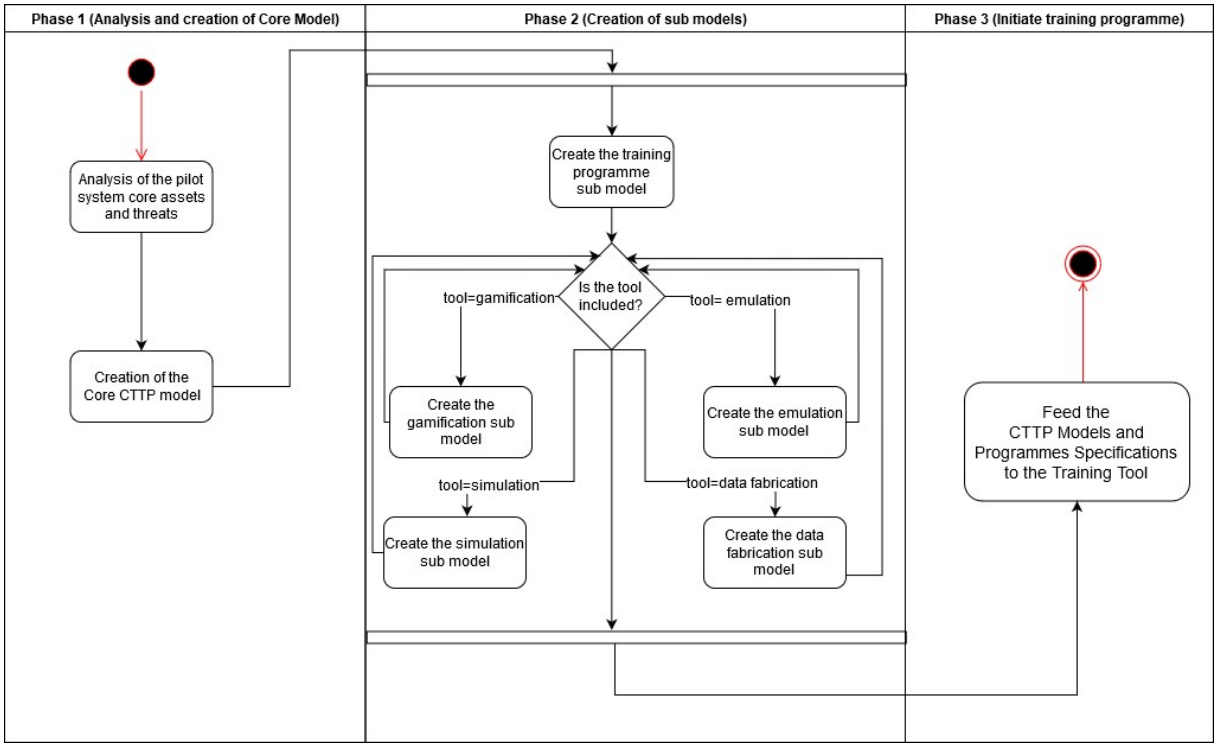

Figure 4. Initial CTTP Model creation (activity diagram)

Figure 4 provides an initial activity diagram that describes how the CTTP Models and Programmes specifications are created. The process includes:

- The **first phase** includes an analysis of the pilot system where one identifies the assets of the system and the existing threats. This analysis leads to the creation of the core CTTP Model. The latter includes the assets that will be used by the training programme in order to initiate a training scenario.
- The **second phase** consists of the creation of the CTTP sub models. Each tool has its own sub model. If the tool is included within the scenario description, then the sub model will be created and parsed to the Training Tool.
- Lastly, the **third phase** consists of the creation of the final CTTP Model and Programme specification, where it is parsed to the training tool in order to initiate the training process.

Each core model will contain the grammar –as described in "D3.1 – CTTP Models and Programmes Specification Language"– expected as an input from the CTTP models and programmes specification tool editor as described in "D3.2 – CTTP Models and Programmes Specification Tool". The Core CTTP model acts as the backbone of the model-driven approach, as it contains the assets and the threats that will lead to the creation of the sub models.

Moreover, the CTTP sub models will contain the format expected by the corresponding tool (e.g. in JSON or XML). More specifically, the Emulation Tool (i.e. OpenStack (OpenStack, 2020)) will receive the sub model in an XML format and convert it in the HEAT template

described in "D2.1 – Emulated Components Generator Modules v1" while the Gamification, Simulation, and Data Fabrication will receive it in JSON, based on the instantiation procedures that are described in the related deliverables "D4.2 – THREAT-ARREST serious games v1", "D5.2 – Simulated components and network generator v1", and "D5.1 – Real event logs statistical profiling module and synthetic event log generator v1", respectively.

In the following subsections, the CTTP models for one main scenario for each pilot are presented:

- Smart Home - IoT – Scenario 1 (Response & Mitigation)
- Smart Shipping – Scenario 1 (Navigation combo attack)
- Healthcare – Scenario 1 (Incident response)

The full implementation of them will form the means to evaluate and deliver the 1st version of the THREAT-ARREST platform, due M20. This also constitute the milestone "MS4 – 1st version of Integrated training platform".

4.1 Smart Home – IoT

The model for Scenario 1 of the Smart Home – IoT use case will be presented. The description, progression and modelling of this scenario can be found in Section 3.1.1.

4.1.1 Core CTTP Model

The scenario's core CTTP model, specified using the CTTP specification language grammar is as follows:

```
Person(firstName("Filippo"),lastName("N/A"),email("filippo@lig
htsourcelabs.com"), project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB LTD "),
description("He is the system administrator. He performs the
initial gateway configuration for the system that needs to be
installed by a technician (gateway provisioning) and monitor
the overall functionality of the cyber system from the
backend."),roles(administrator))
Person(firstName("Robert"),lastName("N/A"),email("robert@light
sourcelabs.com"), project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB LTD "),
description("The organization's security experts. They
establish the defense strategies and enhance the security
culture of the company. They could also be the same personnel
as administrators or CISOs."),roles(security_auditor))
Person(firstName("Elias"),lastName("N/A"),email("elias@lightso
urcelabs.com"), project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB LTD "),
description("Install a new system in a client's home and carry
out on-site visits for repairs and
maintenance."),roles(trainer))
Person(firstName("Kevin"),lastName("N/A"),email("captain@danao
s.gr"),value(4000.0),currency(EUR),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),activeTo(2025-11-19 13:55),description("The captain of
the ship"),roles(technicians)),
SoftwareAsset(vendor("LSE"),version("2.0.1"),name("ubiworx
server"),kind(Service),type(SAL),project("Response &
```

```
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("MQTT server (gateways
connect to this machine)"))
SoftwareAsset
(vendor("MariaDB"),version("10.3.18"),name("MariaDB"),kind(Ser
vice),type(SAL),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("The organization's server
relational database service."))
SoftwareAsset
(vendor("LSE"),version("2.0.1"),name("HistDB"),kind(Service),t
ype(SAL),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("Microservice software that
handles admin/user related requests."))
SoftwareAsset (vendor("LSE"),version("2.0.1"),name("Broker
RESTful API"),kind(Service),type(SAL),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("TLS connection termination
service for MQTT and HTTP traffic."))
SoftwareAsset
(vendor("NGINX"),version("1.17.7"),name("NGINX"),kind(Service)
,type(SAL),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("MQTT service which support
the MQTT protocol"))
SoftwareAsset (vendor("Redis
Labs"),version("5.0.3"),name("Redis"),kind(Service),type(PAL),
project("Response & Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("Filippo") ,description("In-memory cash service
that facilitates inter service resource discovery"))
SoftwareAsset (vendor("LSE"),version("2.0.1"),name("ubiworx
core"),kind(Service),type(PAL),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("The IoT edge software
framework."))
SoftwareAsset
(vendor("sqlite"),version("3.29.0"),name("sqlite"),kind(Servic
e),type(SAL),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("Gateway Relational
Database"))
SoftwareAsset (vendor("LSE"),version("2.0.1"),name("ubiworx
gateway API"),kind(Service),type(SAL),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("Microservice software that
handles gateway related tacks (gateway RESTful API)."))
SoftwareAsset (vendor("LSE"),version("1.6.0"),name("HEMS
platform"),kind(Service),type(SAL),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("Distributed firewall
```

```
package that enforces the security policy on the edge
gateway."))
SoftwareAsset (vendor("TP-Link"),version("HS110"),name("TP-
LINK Wi-Fi Smart Plug
"),kind(Component),type(PAL),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("Software that runs on the
Smart plugs."))
SoftwareAsset (vendor("Sungrow"),version("SH5K-
20"),name("Hybrid Inverter
SH5K"),kind(Component),type(PAL),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("Software that runs on the
Inverter."))
SoftwareAsset (vendor("Meazon"),version("-"),name("DinRail 3-
phase Ultra"),kind(Component),type(PAL),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("Software that runs on the
Energy Meters."))
SoftwareAsset
(vendor("OpenVPN"),version("2.4.7"),name("OpenVPN"),kind(Servi
ce),type(PAL),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("Remote access client
application for 3G and VPN access to the gateways from the
administrator PC."))
SoftwareAsset (vendor("OpenJS
Foundation."),version("2.19.4"),name("Node Red
Dashboard"),kind(Service),type(SAL),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("Simulated homeowner app
that is used to view recorded data samples.")),

HardwareAsset(vendor("LSE"),version("2.0.1"),name("ubiworx
Broker"), hwType(compute),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("RESTful API server")
,PortModule(ioType(network),isAlwaysConnected(TRUE)),NetworkAd
apter(connectionType(Integrated),supportedProtocol(ethernet),S
peed(100.0),IP("192.168.33.20"),Netmask("255.255.255.0"),IpTyp
e(Dynamic)))
HardwareAsset(vendor("TP-Link"),version("HS110"),name("TP-LINK
Smart Plug"), hwType(compute),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("Smart plugs")
,PortModule(ioType(network),isAlwaysConnected(TRUE)),NetworkAd
apter(connectionType(Integrated),supportedProtocol(ethernet),S
peed(100.0),IP("192.168.33.10"),Netmask("255.255.255.0"),IpTyp
e(Static)))
HardwareAsset(vendor("LSE"),version("2.0.1"),name("ubiworx
Gateway"), hwType(compute),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
```

```
LTD"),owner("filippo"),description("Smart plugs")
,PortModule(ioType(network),isAlwaysConnected(TRUE)),NetworkAd
apter(connectionType(Integrated),supportedProtocol(ethernet),S
peed(100.0),IP("192.168.33.21"),Netmask("255.255.255.0"),IpTyp
e(Static)))
HardwareAsset(vendor("Meazon"),version("-"),name("DinRail 3-
phase Ultra"), hwType(compute),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("kevin"),description("Smart plugs")
,PortModule(ioType(network),isAlwaysConnected(TRUE)),NetworkAd
apter(connectionType(usb),supportedProtocol(Token Ring) IP("-
")))
HardwareAsset(vendor("Sungrow"),version("SH5K-
20"),name("Hybrid Inverter SH5K"),
hwType(compute),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("kevin"),description("Smart
plugs"),PortModule(ioType(network),isAlwaysConnected(TRUE)),Ne
tworkAdapter(connectionType(Integrated),supportedProtocol(ethe
rnet),Speed(100.0),IP("10.172.154.100"),Netmask("255.255.255.0
"),IpType(Static)))
HardwareAsset(vendor("Debian"),version("10"),name("PC
installer"), hwType(compute),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("kevin"),description("Smart plugs")
,PortModule(ioType(network),isAlwaysConnected(TRUE)),NetworkAd
apter(connectionType(Integrated),supportedProtocol(ethernet),S
peed(100.0),IP("-"),Netmask("255.255.255.0"),IpType(Dynamic)))
HardwareAsset(vendor("LSE"),version("2.0.1"),name("Ubiwork
broker"), hwType(compute),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("Smart plugs")
,PortModule(ioType(network),isAlwaysConnected(TRUE)),NetworkAd
apter(connectionType(Integrated),supportedProtocol(ethernet),S
peed(100.0),IP("192.168.33.20"),Netmask("255.255.255.0"),IpTyp
e(Static)))
HardwareAsset(vendor("LSE"),version("2.0.1"),name("Ubiwork
broker"), hwType(compute),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("Smart plugs")
,PortModule(ioType(network),isAlwaysConnected(TRUE)),NetworkAd
apter(connectionType(Integrated),supportedProtocol(ethernet),S
peed(100.0),IP("192.168.33.20"),Netmask("255.255.255.0"),IpTyp
e(Static)))
HardwareAsset(vendor("Debian"),version("10"),name("PC Admin"),
hwType(compute),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("Smart plugs")
,PortModule(ioType(network),isAlwaysConnected(TRUE)),NetworkAd
apter(connectionType(Integrated),supportedProtocol(ethernet),S
peed(100.0),IP("-
"),Netmask("255.255.255.0"),IpType(Dynamic))),
```

```
Data(name("Gateway
logic"),category(config),datastate(at_rest),project("Response
& Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("Information related the
gateway configuration and data processing logic that is
maintained on the Edge IoT Gateways"))
Data(name("HEMS
platform"),category(security),datastate(at_rest),project("Resp
onse & Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("Distributed firewall
configuration file"))
Data(name("Consumption"),category(operational),datastate(in_tr
ansit),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("The data that is recorded
by the smart plugs"))
Data(name("Energy
produced"),category(operational),datastate(in_transit),project
("Response & Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("The data that is recorded
by the inverter"))
Data(name("Amount exported /
imported"),category(operational),datastate(in_transit),project
("Response & Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("The data that is recorded
by the energy meters"))
Data(name("Device
readings"),category(operational),datastate(in_transit),project
("Response & Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("The data that is exchanged
via the technician installation equipment with Wi-Fi Internet
capabilities"))
Data(name("health status"),category(admin),
datastate(in_transit),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("3G communication data"))
Data(name("Access
info"),category(admin),datastate(in_transit),project("Response
& Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("VPN gateway IP
information"))
Data(name("Sensor
readings"),category(operational),datastate(in_transit),project
("Response & Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("The data that is exchanged
via the administrator PC over 3G and VPN"))
Data(name("Recorded
samples"),category(operational),datastate(at_rest),project("Re
sponse & Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("The sensor data on the
backend server"))
```

```
Data(name("Relational
data"),category(config),datastate(at_rest),project("Response &
Mitigation"),organisation("LIGHTSOURCE LAB
LTD"),owner("filippo"),description("The organization's data
that are maintained in the backend DBs"))
```

4.1.2 Training Programme Sub Model

The scenario's training programme sub model, specified using the CTTP specification language grammar and fed to the training tool using a JSON format is as follows:


```
[
    {
        "description": "As the owner of a smart plug, the Lightsource application (web or m
obile) allows you to monitor its power consumption and/or it on/off behaviour. It also prov
ides alerts of the system if an abnormal behaviour is traced. An intruder has gain access t
o your smart plug and executed a malicious application where it stopped the smart plug from
 reporting its power consumption and turned a switch on and off at random time points. You
were notified by an alert, through the web application, that an abnormal behaviour was dete
cted, and you are asked to read the Lightsource guideline provided during the setup phase,
in order to bring the device back to its expected behaviour.",
        "scenarioGoal": {
            "description": "This scenario trains an end user with no security knowledge on
how to response to an abnormal behaviour and take immediate actions in order to mitigate th
e risk. The scenario is implemented in an Emulation, Simulation and Gamification tool.",
            "maxScore": 10,
            "successScore": 5
        },
        "difficulty": 7,
        "activeFrom": "2020-02-20 12:00:00",
        "activeTo": "2021-02-20 12:00:00",
        "organisation": {
            "organisationID": 1,
            "name": "Lightsource LAB LTD ",
            "activeFrom": "2020-02-14 13:37:28",
            "typeID": 3,
            "currencyID": 4,
            "value": 500000.0
        },
        "project": {
            "projectID": 1,
            "name": "Response & Mitigation",
            "activeFrom": "2020-02-14 13:40:51",
            "activeTo": "2020-02-14 13:40:51",
            "statusID": 3,
            "organisationID": 1,
            "lastUpdated": "2020-02-14 13:40:51"
        },
        "statusType": {
            "statusID": 2,
            "statusField": "status",
            "statusValue": "final",
            "statusSymbol": "status_final"
        },
        "durationType": {
            "value": 60,
            "durationUnit": {
                "durationUnitID": 1,
```

```
            "unit": "minutes"
        }
    },
    "typesOfActionTypes": [
        {
            "toatID": 4,
            "toatValue": "Analysis"
        },
        {
            "toatID": 3,
            "toatValue": "Detection"
        }
    ],
    "roles": [
        {
            "personroleID": 3,
            "personRoleField": "personRole",
            "personRoleValue": "asset_owner",
            "personRoleSymbol": "personRole_assetOwner"
        },
        {
            "personroleID": 5,
            "personRoleField": "personRole",
            "personRoleValue": "asset_controller",
            "personRoleSymbol": "personRole_assetController"
        }
    ],
    "bibliographies": [
        {
            "name": "Incident Response & Abnormal behaviour",
            "text": "Lightsource's incident response guideline"
        },
        {
            "name": "Security Awareness training",
            "text": "https://www.sans.org/security-awareness-training"
        }
    ],
    "owners": [
        {
            "personID": 47,
            "firstName": "Elias",
            "lastName": "N/A",
            "email": "elias@lightsourcelabs.com",
            "asset": {
                "assetID": 76,
                "typeID": 4,
                "activeFrom": "2020-02-25 14:12:31",
                "tableName": "Person",
                "organisationID": 1,
                "projects": [
                    {
                        "projectID": 1,
                        "name": "Response & Mitigation",
                        "activeFrom": "2020-02-14 13:40:51",
                        "activeTo": "2020-02-14 13:40:51",
                        "statusID": 3,
                        "organisationID": 1,
                        "lastUpdated": "2020-02-14 13:40:51"
```

```
                        }
                    ]
                },
                "statusID": 2,
                "personRoles": [
                    {
                        "prID": 30,
                        "personRole": {
                            "personroleID": 7,
                            "personRoleField": "personRole",
                            "personRoleValue": "technician",
                            "personRoleSymbol": "personRole_technician"
                        }
                    }
                ]
            }
        ],
        "trainingProgrammeExecutions": [
            {
                "totalScreens": 1,
                "executionPriority": 1,
                "difficulty": 1,
                "instructions": "The trainee is educated about the security concerns surrou
nding smart devices and, upon installation of the edge device, receives an incident respons
e and abnormal behaviour guideline.",
                "screens": [
                    {
                        "screenNumber": 1,
                        "executionTool": {
                            "toolTypeID": 5,
                            "tool": "Training Tool"
                        },
                        "description": "Read the guideline of the abnormal behaviour."
                    }
                ],
                "executionDuration": {
                    "value": 10,
                    "durationUnit": {
                        "durationUnitID": 1,
                        "unit": "minutes"
                    }
                },
                "hintImpact": 0.0
            },
            {
                "totalScreens": 1,
                "executionPriority": 2,
                "difficulty": 3,
                "instructions": "The trainee receives an alert to its web-
based application letting him/her know that its smart plug stopped reporting the power cons
umption and that the device connected to it reports abnormal on/off patterns. The trainee o
pens the web-based application to check if the alert was correct.",
                "screens": [
                    {
                        "screenNumber": 1,
                        "executionTool": {
                            "toolTypeID": 1,
                            "tool": "Emulation Tool"
```

```
                        },
                        "description": "LSE's web application",
                        "hint": "Is the power consumption shown in the web application corr
ect?"
                    }
                ],
                "executionDuration": {
                    "value": 5,
                    "durationUnit": {
                        "durationUnitID": 1,
                        "unit": "minutes"
                    }
                },
                "hintImpact": 0.7
            },
            {
                "totalScreens": 2,
                "executionPriority": 3,
                "difficulty": 6,
                "instructions": "The trainee reads the guideline and, as instructed in the
first step, resets the smart plug to its factory settings by pressing its button for 10 sec
onds. Then, it checks the graphs presented in the web application, but he observes that the
 abnormal behaviour is still there (i.e. no power consumption is presented).",
                "screens": [
                    {
                        "screenNumber": 1,
                        "executionTool": {
                            "toolTypeID": 2,
                            "tool": "Simulation Tool"
                        },
                        "description": "Press the button to reset the smart plug.",
                        "hint": "Did you reset the smart plug?"
                    },
                    {
                        "screenNumber": 2,
                        "executionTool": {
                            "toolTypeID": 1,
                            "tool": "Emulation Tool"
                        },
                        "description": "The web application that shows the grapgh",
                        "hint": "Did your previous action fixed the graph?"
                    }
                ],
                "executionDuration": {
                    "value": 20,
                    "durationUnit": {
                        "durationUnitID": 1,
                        "unit": "minutes"
                    }
                },
                "hintImpact": 0.4
            },
            {
                "totalScreens": 1,
                "executionPriority": 4,
                "difficulty": 5,
                "instructions": "The trainee resets the device connected to the smart plug.
 ",
```

```
                "screens": [
                    {
                        "screenNumber": 1,
                        "executionTool": {
                            "toolTypeID": 2,
                            "tool": "Simulation Tool"
                        },
                        "description": "Press the button to reset the device",
                        "hint": "Did you reset the device?"
                    }
                ],
                "executionDuration": {
                    "value": 10,
                    "durationUnit": {
                        "durationUnitID": 1,
                        "unit": "minutes"
                    }
                },
                "hintImpact": 0.5
            },
            {
                "totalScreens": 1,
                "executionPriority": 5,
                "difficulty": 5,
                "instructions": "The trainee checks the graphs, and observers that both the
 smart plug started reporting its power consumption and the connected device was not report
ing abnormal behaviour.",
                "screens": [
                    {
                        "screenNumber": 1,
                        "executionTool": {
                            "toolTypeID": 1,
                            "tool": "Emulation Tool"
                        },
                        "description": "LSE's web application"
                    }
                ],
                "executionDuration": {
                    "value": 5,
                    "durationUnit": {
                        "durationUnitID": 1,
                        "unit": "minutes"
                    }
                },
                "hintImpact": 0.0
            },
            {
                "totalScreens": 1,
                "executionPriority": 6,
                "difficulty": 6,
                "instructions": "The trainee starts the card game.",
                "screens": [
                    {
                        "screenNumber": 1,
                        "executionTool": {
                            "toolTypeID": 3,
                            "tool": "Gamification Tool"
                        },
```

```
                    "description": "PROTECT card game",
                    "hint": "The training success depends on the number of attack cards
that the trainee has repeled successfully by selecting the correct defense card"
                }
            ],
            "executionDuration": {
                "value": 10,
                "durationUnit": {
                    "durationUnitID": 1,
                    "unit": "minutes"
                }
            },
            "hintImpact": 0.4
        }
    ]
  }
]
```

4.1.3 Emulation Sub Model

The scenario's Emulation sub model, specified using the CTTP specification language grammar and fed to the training tool using an XML format is as follows:

```
<?xml version="1.0" encoding="Unicode" standalone="yes"?>
<Scenario name="UC1-LSE">
    <CustomVM name="cloud_UC1" os="linux">
        <connectionmode port="22" connectiontype="ssh"/>
        <ram val="4096"/>
        <vcpus val="2"/>
        <disk val="40"/>
        <image name="LSE_cloud" value="LSE_cloud" username="admin"/>
        <Network idref="home_network"/>
    </CustomVM>
    <CustomVM name="trainee_UC1" os="windows">
        <connectionmode port="3389" connectiontype="rdp"/>
        <ram val="4096"/>
        <vcpus val="4"/>
        <disk val="40"/>
        <image name="trainee_UC1" value="win10" username="win10" password="win10"/>
        <Network idref="home_network"/>
    </CustomVM>
    <CustomVM name="sim_UC1" os="linux">
        <connectionmode port="22" connectiontype="ssh"/>
        <ram val="4096"/>
        <vcpus val="2"/>
        <disk val="40"/>
        <image name="home_sensors" value="ubuntu-sim-red" username="ubuntu"/>
        <Network idref="home_network" fixedip="20.10.1.1"/>
        <Scripts idref="Simulation_script"/>
    </CustomVM>
    <CustomVM name="gateway_UC1" os="linux">
        <connectionmode port="22" connectiontype="ssh"/>
        <ram val="4096"/>
        <vcpus val="2"/>
        <disk val="40"/>
        <image name="LSE-gateway" value="LSE-gateway" username="admin"/>
        <Network idref="internal_network"/>
    </CustomVM>
```

```
    <Networks>
        <network id="home_network">
            <gateway name="gateway-home_network" val="20.10.1.1"/>
            <cidr name="cidr-home_network" val="20.10.1.0/24"/>
            <is_external val="false"/>
        </network>
    </Networks>
    <Scripts><Script id="Simulation_script">![CDATA[ echo "start user data" java -jar sim-
controller.jar & echo "end user data" ]]></Script>
</Scripts>
</Scenario>
```

4.1.4 Simulation Sub Model

The scenario's Simulation sub model, specified using the CTTP specification language grammar and fed to the training tool using a JSON format is as follows:

```
[
    {
        "tool": "Jasima",
        "template": "Simulation/smartHome.jasima",
        "simTime": 0,
        "executionSpeed": 1,
        "randomSeed": 42,
        "project": {
            "projectID": 1,
            "name": "Response & Mitigation",
            "activeFrom": "2020-02-14 13:40:51",
            "activeTo": "2020-02-14 13:40:51",
            "statusID": 3,
            "organisationID": 1,
            "lastUpdated": "2020-02-14 13:40:51"
        },
        "organisation": {
            "organisationID": 1,
            "name": "Lightsource LAB LTD ",
            "activeFrom": "2020-02-14 13:37:28",
            "typeID": 3,
            "currencyID": 4,
            "value": 500000.0
        },
        "activeFrom": "2020-02-14 12:00:00",
        "activeTo": "2021-02-14 12:00:00",
        "deploymentMode": {
            "dmtID": 2,
            "dmtField": "DeploymentMode",
            "dmtValue": "Template",
            "dmtSymbol": "DeploymentMode_Template"
        },
        "SimulationComponents": [
            {
                "name": "SmartHome",
                "simulatedComponent": "SmartHome",
                "type": "jasima.core.Simulation.SimComponentContainerBase",
                "root": true,
                "componentContainers": [
                    {
                        "simpleComponents": [
                            {
```

```
                                "name": "SmartPlug",
                                "internalID": "SmartPlug",
                                "type": "smarthome.SmartPlug",
                                "root": false,
                                "attributes": [
                                    {
                                        "name": "plugState",
                                        "initialValue": "WORKING",
                                        "type": "smarthome.SmartPlugStateEnum",
                                        "canChange": true
                                    },
                                    {
                                        "name": "ipAddress",
                                        "initialValue": "192.168.1.2",
                                        "type": "String",
                                        "canChange": false
                                    }
                                ]
                            },
                            {
                                "name": "ConnectedDevice",
                                "internalID": "ConnectedDevice",
                                "type": "smarthome.ConnectedDevice",
                                "root": false,
                                "attributes": [
                                    {
                                        "name": "deviceState",
                                        "initialValue": "WORKING",
                                        "type": "smarthome.ConnectedDeviceStateEnum
",
                                        "canChange": true
                                    }
                                ]
                            }
                        ]
                    }
                ]
            }
        ],
        "simExpectedTraces": [
            {
                "value": "true",
                "name": "smarthome.DeviceReset",
                "seqNo": 1
            },
            {
                "value": "true",
                "name": "smarthome.SmartPlugReset",
                "seqNo": 2
            }
        ]
    }
]
```

4.1.5 Gamification Sub Model

The scenario's Gamification sub model, specified using the CTTP specification language grammar and fed to the training tool using a JSON format is as follows:


```
[
    {
        "project": {
            "projectID": 1,
            "name": "Response & Mitigation",
            "activeFrom": "2020-02-14 13:40:51",
            "activeTo": "2020-02-14 13:40:51",
            "statusID": 3,
            "organisationID": 1,
            "lastUpdated": "2020-02-14 13:40:51"
        },
        "organisation": {
            "organisationID": 1,
            "name": "Lightsource LAB LTD ",
            "activeFrom": "2020-02-14 13:37:28",
            "typeID": 3,
            "currencyID": 4,
            "value": 500000.0
        },
        "statusType": {
            "statusID": 2,
            "statusField": "status",
            "statusValue": "final",
            "statusSymbol": "status_final"
        },
        "activeFrom": "2020-02-14 12:00:00",
        "activeTo": "2021-02-14 12:00:00",
        "games": [
            {
                "gameType": {
                    "gameTypeID": 1,
                    "game": "Protect"
                },
                "protects": [
                    {
                        "difficultyLevel": 2,
                        "gameTime": 12,
                        "cardDeckID": "cd_smarthome",
                        "specialPractice": false
                    }
                ]
            },
            {
                "gameType": {
                    "gameTypeID": 1,
                    "game": "Protect"
                },
                "protects": [
                    {
                        "difficultyLevel": 2,
                        "gameTime": 12,
                        "cardDeckID": "cd_smarthome",
                        "specialPractice": false
                    }
```

```
                ]
            },
            {
                "gameType": {
                    "gameTypeID": 1,
                    "game": "Protect"
                },
                "protects": [
                    {
                        "difficultyLevel": 1,
                        "gameTime": 15,
                        "cardDeckID": "cd_smarthome",
                        "specialPractice": false
                    }
                ]
            },
            {
                "gameType": {
                    "gameTypeID": 1,
                    "game": "Protect"
                },
                "protects": [
                    {
                        "difficultyLevel": 1,
                        "gameTime": 15,
                        "cardDeckID": "cd_smarthome",
                        "specialPractice": false
                    }
                ]
            }
        ],
        "GamificationExpectedTraces": [
            {
                "action": "fend off attacks",
                "value": "number of correctly and incorrectly fend off attack cards
"
            }
        ]
    }
]
```


4.2 Smart Shipping

4.2.1 Overview

The model for Scenario 1 of the Smart Shipping use case will be presented. The description, progression and modelling of this scenario can be found in Section 3.2.1.

4.2.2 Core CTTP Model

The scenario's core CTTP model, specified using the CTTP specification language grammar is as follows:

```
Person(firstName("Filippo"),lastName("N/A"),email("admin@danaos.gr"),value(3000.0),currency(EUR),project("Threat Arrest"),organisation("DANAOS SHIPPING COMPANY LTD"),activeTo(2020-11-19 13:55),description("The project administrator for DANAOS SHIPPING COMPANY LTD"),roles(administrator)),
```

```
Person(firstName("captain"),lastName("DANAOS Shipping Company
LTD"),email("captain@danaos.gr"),value(4000.0),currency(EUR),p
roject("Threat Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),activeTo(2025-11-19 13:55),description("The captain of
the ship"),roles(end_user)),

SoftwareAsset(vendor("Microsoft
Corporation"),version("11.914.17763.0"),name("Windows Internet
Explorer 11"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("win.rar
GmbH"),version("4.20.0"),name("WinRAR 4.20 (64-
bit)"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("Uknown"),version("-"),name("GPL
Ghostscript Fonts"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("Uknown"),version("-"),name("GPL
Ghostscript 8.54"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("Ivan
Zahariev"),version("4.1.8"),name("IZArc"),kind(Service),type(S
AL),project("Threat Arrest"),organisation("DANAOS SHIPPING
COMPANY LTD"),owner("system"))
SoftwareAsset (vendor("Uknown"),version("9.3.0"),name("K-Lite
Codec Pack"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("pdfforge
GmbH"),version("2.5.1"),name("PDFCreator"),kind(Service),type(
SAL),project("Threat Arrest"),organisation("DANAOS SHIPPING
COMPANY LTD"),owner("system"))
SoftwareAsset (vendor("Microsoft
Corporation"),version("19.012.0121.0011"),name("Microsoft
OneDrive"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("HP"),version("38.0.0"),name("HP
OfficeJet Pro 8710
Help"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("HP"),version("36.0.41.58587"),name("HP
Google Drive Plugin"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("HP"),version("36.0.41.58587"),name("HP
Dropbox Plugin"),kind(Service),type(SAL),project("Threat
```

```
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("Global Technology
Limited"),version("2.00.1502"),name("GTMailPlus
Dashboard"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("Microsoft
Corporation"),version("1.2.0.10168"),name("Teams Machine-Wide
Installer"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("Microsoft
Corporation"),version("1.2.00.10168"),name("Microsoft
Teams"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("HP
Inc."),version("40.12.1161.1896"),name("HP OfficeJet Pro 8710
Basic Device
Software"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("UK Hydrographic
Office"),version("19.0.0.520"),name("ADMIRALTY Digital
Publications"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset
(vendor("UKHO"),version("1.3.15300.901"),name("ADMIRALTY e-NP
Reader"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("Oracle
Corporation"),version("8.0.2310.11"),name("Java 8 Update
231"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("Oracle
Corporation"),version("2.8.231.11"),name("Java Auto
Updater"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("Adobe Systems
Incorporated"),version("19.021.20056"),name("Adobe Acrobat
Reader DC"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("Microsoft
Corporation"),version("10.0.40219"),name("Microsoft Visual C++
2010"),kind(Service),type(SAL),project("Threat
```

```
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("Microsoft
Corporation"),version("8.3.11"),name("SPOS
8"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("Microsoft
Corporation"),version("16.0.12228.20364"),name("Office 16
Click-to-Run Extensibility
Component"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("Microsoft
Corporation"),version("16.0.12228.20364"),name("Microsoft
Office 365 Business"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("Check Point Software Technologies
Ltd."),version("82.10.9575"),name("Check Point Endpoint
Security"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("Mozilla"),version("71.0"),name("Mozilla
Firefox"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset (vendor("Check Point Software Technologies
Ltd."),version("82.10.9575"),name("Check Point Endpoint
Security"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"))
SoftwareAsset
(vendor("Microsoft"),version("10.0.17763"),name("Windows 10
Proffesional
Edition"),kind(Service),value(20032.0),currency(EUR),type(PAL)
,project("Threat Arrest"),organisation("DANAOS SHIPPING
COMPANY LTD"),owner("system"),description("OS"))
SoftwareAsset
(vendor("Oracle"),version("12.1.0.2"),name("Database
Server"),kind(Service),value(20032.0),currency(EUR),type(PAL),
project("Threat Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"),description("OS")),

HardwareAsset(vendor("Dell
Inc."),version("790"),name("Optiplex"),value(50000.0),currency
(EUR),hwType(compute),project("Threat
Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"),activeTo(2022-12-26
19:50),description("V114-
CAPTAIN"),CpuModule(processorName("Intel Core
i5"),cores(4),threads(4),baseFrequency(3.3),socket("LGA1155"))
```

```
,MemoryModule(size(8),type("DDR3"),speed(1066.0),manufacturer(
"Dell
Inc.")),PortModule(ioType(usb),isAlwaysConnected(TRUE)),Networ
kAdapter(connectionType(Integrated),MAC("00:0c:29:6f:cf:bc"),s
upportedProtocol(ethernet),Speed(100.0),IP("10.207.24.20"),Net
mask("255.255.255.0"),IpType(Static),dhcp("False")))

HardwareAsset (vendor("Furuno"),version("150"),name("Furuno
GP150"),value(22950.0),currency(USD),hwType(compute),project("
Threat Arrest"),organisation("DANAOS SHIPPING COMPANY
LTD"),owner("system"),activeTo(2022-12-26
19:50),NetworkAdapter(connectionType(Integrated),MAC("00:0c:29
:01:e9:d9"),supportedProtocol(ethernet),Speed(100.0),IP("10.20
7.24.21"),Netmask("255.255.255.0"),IpType(Dynamic),dhcp("True"
)))
HardwareAsset (vendor("JRC"),version("JUE-85"),name("Inmarsat
C Mobile Earth
Station"),value(6439.0),currency(USD),hwType(compute),project(
"Threat Arrest"),organisation("Sphynx Technology Solutions
AG"),owner("system"),activeTo(2022-12-26
19:50),NetworkAdapter(connectionType(Integrated),MAC("00:0c:29
:60:a9:c6"),supportedProtocol(ethernet),Speed(100.0),IP("192.1
68.114.6"),Netmask("255.255.255.0"),IpType(Static),dhcp("False
")))
```

4.2.3 Training Programme Sub Model

The scenario's training programme sub model, specified using the CTTP specification language grammar and fed to the training tool using a JSON format is as follows:


```
[
    {
        "description": "This is a social engineering scenario which targets valuable actuat
ors 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 traine
e 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.",
        "scenarioGoal": {
            "description": "This scenario trains an end user with moderate security knowled
ge. The scenario is implemented in an Emulation, Simulation and Gamification tool.",
            "maxScore": 10,
            "successScore": 5
        },
        "difficulty": 8,
        "activeFrom": "2020-02-14 12:00:00",
        "activeTo": "2021-02-14 12:00:00",
        "organisation": {
            "organisationID": 2,
            "name": "DANAOS Shipping Company LTD ",
            "activeFrom": "2020-02-14 13:38:42",
            "typeID": 3,
            "currencyID": 1,
            "value": 500000.0
        },
```

```
        "project": {
            "projectID": 2,
            "name": "Navigation combo attack (phishing email and GPS spoofing)",
            "activeFrom": "2020-02-14 13:41:21",
            "statusID": 2,
            "organisationID": 2,
            "lastUpdated": "2020-02-14 13:42:10"
        },
        "statusType": {
            "statusID": 2,
            "statusField": "status",
            "statusValue": "final",
            "statusSymbol": "status_final"
        },
        "durationType": {
            "value": 60,
            "durationUnit": {
                "unit": "minutes"
            }
        },
        "typesOfActionTypes": [
            {
                "toatValue": "Preparedness"
            },
            {
                "toatValue": "Post security incident response"
            }
        ],
        "roles": [
            {
                "personroleID": 7,
                "personRoleField": "personRole",
                "personRoleValue": "technician",
                "personRoleSymbol": "personRole_technician"
            },
            {
                "personroleID": 6,
                "personRoleField": "personRole",
                "personRoleValue": "auditor",
                "personRoleSymbol": "personRole_auditor"
            },
            {
                "personroleID": 2,
                "personRoleField": "personRole",
                "personRoleValue": "administrator",
                "personRoleSymbol": "personRole_administrator"
            }
        ],
        "bibliographies": [
            {
                "name": "GPS Spoofing",
                "text": "https://www.ship-technology.com/features/ship-navigation-risks/"
            },
            {
                "name": "Phishing email",
                "text": "https://www.ncsc.gov.uk/pdfs/guidance/phishing.pdf"
            }
        ],
```

```
        "owners": [
            {
                "personID": 43,
                "firstName": "Captain",
                "lastName": "Danaos",
                "email": "captain@danaos.gr",
                "asset": {
                    "assetID": 2,
                    "typeID": 4,
                    "activeFrom": "2020-02-14 13:44:19",
                    "tableName": "Person",
                    "organisationID": 2,
                    "projects": [
                        {
                            "projectID": 2,
                            "name": "Navigation combo attack (phishing email and GPS spoofi
ng)",
                            "activeFrom": "2020-02-14 13:41:21",
                            "statusID": 2,
                            "organisationID": 2,
                            "lastUpdated": "2020-02-14 13:42:10"
                        }
                    ]
                },
                "statusID": 2,
                "personRoles": [
                    {
                        "prID": 26,
                        "personRole": {
                            "personroleID": 1,
                            "personRoleField": "personRole",
                            "personRoleValue": "end_user",
                            "personRoleSymbol": "personRole_endUser"
                        }
                    }
                ]
            }
        ],
        "trainingProgrammeExecutions": [
            {
                "totalScreens": 1,
                "executionPriority": 1,
                "difficulty": 4,
                "instructions": "A faulty email commanding the captain to go to the Thessal
oniki port is being sent.  The email contains the details of another journey and was sent t
o the captain/trainee by mistake. Firstly, the captain identifies that this is a legitimate
 email.  Since the destination port was Piraeus, the captain understands that this email wa
s sent to him/her by mistake. Thus, the captain ignores the email and reports it back to th
e office.",
                "screens": [
                    {
                        "screenNumber": 1,
                        "executionTool": {
                            "tool": "Emulation Tool"
                        },
                        "description": "The faulty email is being sent by the VM that inclu
des the trainers mail application",
                        "hint": "Check for the email content"
```

```
                    }
                ],
                "executionDuration": {
                    "value": 5,
                    "durationUnit": {
                        "unit": "minutes"
                    }
                },
                "hintImpact": 0.6
            },
            {
                "totalScreens": 1,
                "executionPriority": 2,
                "difficulty": 8,
                "instructions": "The captain receives a malicious (phishing) email alerting
 him/her that a bad weather condition will take place, thus, he/she needs to go to another
port to make a stop.Then, the captain identifies that this is a phishing email and first ig
nores the email and then report it to the office.",
                "screens": [
                    {
                        "screenNumber": 1,
                        "executionTool": {
                            "tool": "Emulation Tool"
                        },
                        "description": "The phishing email is being sent by the VM that inc
ludes the trainers mail application.",
                        "hint": "Check for the email content"
                    }
                ],
                "executionDuration": {
                    "value": 10,
                    "durationUnit": {
                        "unit": "minutes"
                    }
                },
                "hintImpact": 0.2
            },
            {
                "totalScreens": 1,
                "executionPriority": 3,
                "difficulty": 6,
                "instructions": "The captain receives a legitimate email with the weather f
orecast, denoting that the weather is good, and the destination is the Piraeus port. Then,
the captain understands that this is a legitimate email and starts the journey.",
                "screens": [
                    {
                        "screenNumber": 1,
                        "executionTool": {
                            "tool": "Emulation Tool"
                        },
                        "description": "The legitimate email is being sent by the VM that i
ncludes the trainers mail application",
                        "hint": "Check for the email content"
                    }
                ],
                "executionDuration": {
                    "value": 5,
                    "durationUnit": {
```

```
                        "unit": "minutes"
                    }
                },
                "hintImpact": 0.4
            },
            {
                "totalScreens": 4,
                "executionPriority": 4,
                "difficulty": 9,
                "instructions": "1)During the trip, the captain checks a simulated digital
map that presents the current ship’s position based on the GPS and the predetermined route
(checkpoints) from Heraklion to Piraeus. Captain suddenly realizes that his position on the
 digital map (receiving signal from a GPS receiver) is away from the designated waypoint an
d the ship is off course. Master should check if this is due to his own navigational orders
 or due to external factors (strong current streams) and correct course by returning to the
 predetermined route or if something is wrong with the navigational monitor (digital map).
Captain proceeds with an order of actions to validate position from the GPS signal. 2) The
captain checks a magnetic compass and then marine paper map (Nautical Charts) in order to u
nderstand the actual position of the ship. 3) While checking the compass he understands tha
t it points a different direction to the vessel course. Following, Master mark on the Nauti
cal Charts the position as depicted in the GPS (faulty coordination). Then, the captain is
crosschecking objects (navigation aids, restrictions, bathymetry) mapped on charts with wha
t he observes outside bridge windows with his binoculars and with that he receives from oth
er bridge equipment (e.g. bathymetry on the map against see depth from echo sounder). Capta
in understands that the ship is navigating on different waters than those corresponding to
the position given by GPS (faulty coordination) 4)Finally, the captain understands that a G
PS spoofing attack might occurred, stops following the Digital Map Application (received si
gnal from GPS receiver) and manually navigates the ship to its destination (by turning off
the auto pilot). ",
                "screens": [
                    {
                        "screenNumber": 3,
                        "executionTool": {
                            "tool": "Simulation Tool"
                        },
                        "description": "A marine paper map (Nautical Charts)",
                        "hint": "Check for the actual position of the ship."
                    },
                    {
                        "screenNumber": 2,
                        "executionTool": {
                            "tool": "Simulation Tool"
                        },
                        "description": "A magnetic compass.",
                        "hint": "Does the magnetic compass showing the same direction as th
e digital map?"
                    },
                    {
                        "screenNumber": 5,
                        "executionTool": {
                            "tool": "Simulation Tool"
                        },
                        "description": "Stop the Digital Map Application",
                        "hint": "Should you still check the digital map application?"
                    },
                    {
                        "screenNumber": 1,
                        "executionTool": {
```

```
                        "tool": "Simulation Tool"
                    },
                    "description": "A simulated digital map that presents the current s
hip's position based on the GPS and the predetermined route (checkpoints) from Heraklion to
 Piraeus",
                    "hint": "Check the position on the map."
                },
                {
                    "screenNumber": 4,
                    "executionTool": {
                        "tool": "Simulation Tool"
                    },
                    "description": "The GPS (Nautical Charts)"
                }
            ],
            "executionDuration": {
                "value": 40,
                "durationUnit": {
                    "unit": "minutes"
                }
            },
            "hintImpact": 0.1
        },
        {
            "totalScreens": 1,
            "executionPriority": 5,
            "difficulty": 6,
            "instructions": "The trainee starts the card game.",
            "screens": [
                {
                    "screenNumber": 1,
                    "executionTool": {
                        "tool": "Gamification Tool"
                    },
                    "description": "PROTECT card game",
                    "hint": "The training success depends on the number of attack cards
 that the trainee has repeled successfully by selecting the correct defense card"
                }
            ],
            "executionDuration": {
                "value": 5,
                "durationUnit": {
                    "unit": "minutes"
                }
            },
            "hintImpact": 0.4
        }
    ]
  }
]
```


4.2.4 Emulation Sub Model

The scenario's Emulation sub model, specified using the CTTP specification language grammar and fed to the training tool using an XML format is as follows:


```
<?xml version="1.0" encoding="Unicode" standalone="yes"?>
<Scenario name="UC2-DANAOS">
    <CustomVM name="SimDeck" os="linux">
```

```
        <connectionmode port="22" connectiontype="ssh"/>
        <ram val="8192"/>
        <vcpus val="2"/>
        <disk val="80"/>
        <image name="SimDeck_UC2" value="ubuntu-sim-red" username="ubuntu"/>
        <Network idref="on_board_network"/>
        <Scripts idref="Simulation_script"/>
    </CustomVM>
    <CustomVM name="Backend_PC" os="windows">
        <connectionmode port="3389" connectiontype="rdp"/>
        <ram val="8192"/>
        <vcpus val="4"/>
        <disk val="80"/>
        <image name="Backend_PC_UC3" value="Backend_PC_UC3" username="win10" password="wind
10"/>
        <Network idref="on_board_network" fixedip="20.70.1.2"/>
    </CustomVM>
    <CustomVM name="Captain_PC" os="windows">
        <connectionmode port="3389" connectiontype="rdp"/>
        <ram val="8192"/>
        <vcpus val="4"/>
        <disk val="80"/>
        <image name="Captain_PC_UC3" value="Captain_PC_UC3" username="win10" password="win1
0"/>
        <Network idref="on_board_network"/>
    </CustomVM>
    <Networks>
        <network id="on_board_network">
            <gateway name="gateway-on_board_network" val="20.70.1.1"/>
            <cidr name="cidr-on_board_network" val="20.70.1.0/24"/>
            <is_external val="false"/>
        </network>
    </Networks>
    <Scripts><Script id="Simulation_script">![CDATA[ echo "start user data" java -jar sim-
controller.jar & echo "end user data" ]]></Script>
</Scripts>
</Scenario>
```

4.2.5 Simulation Sub Model

The scenario's Gamification sub model, specified using the CTTP specification language grammar and fed to the training tool using a JSON format is as follows:

```
[
    {
        "tool": "Jasima",
        "template": "Simulation/smartShipping.jasim",
        "simTime": 0,
        "executionSpeed": 1,
        "randomSeed": 42,
        "project": {
            "projectID": 2,
            "name": "Navigation combo attack (phishing email and GPS spoofing)",
            "activeFrom": "2020-02-14 13:41:21",
            "statusID": 2,
            "organisationID": 2,
            "lastUpdated": "2020-02-14 13:42:10"
        },
```

```
        "organisation": {
            "organisationID": 2,
            "name": "DANAOS Shipping Company LTD ",
            "activeFrom": "2020-02-14 13:38:42",
            "typeID": 3,
            "currencyID": 1,
            "value": 500000.0
        },
        "statusType": {
            "statusID": 2,
            "statusField": "status",
            "statusValue": "final",
            "statusSymbol": "status_final"
        },
        "activeFrom": "2020-02-26 12:00:00",
        "activeTo": "2021-02-26 12:00:00",
        "deploymentMode": {
            "dmtID": 2,
            "dmtField": "DeploymentMode",
            "dmtValue": "Template",
            "dmtSymbol": "DeploymentMode_Template"
        },
        "SimulationComponents": [
            {
                "name": "Ship",
                "simulatedComponent": "Ship",
                "type": "jasima.core.Simulation.SimComponentContainerBase",
                "root": true,
                "componentContainers": [
                    {
                        "name": "Bridge",
                        "simulatedComponent": "Bridge",
                        "type": "jasima.core.Simulation.SimComponentContainerBase",
                        "root": false,
                        "simpleComponents": [
                            {
                                "name": "MagneticCompass1",
                                "internalID": "MagneticCompass1",
                                "type": "smartshipping.MagneticCompass1",
                                "root": false
                            },
                            {
                                "name": "GPSSensor1",
                                "internalID": "GPSSensor1",
                                "type": "smartshipping.GPSSensor1",
                                "root": false,
                                "attributes": [
                                    {
                                        "name": "gpsState",
                                        "initialValue": "WORKING",
                                        "type": "String",
                                        "canChange": true
                                    }
                                ]
                            },
                            {
                                "name": "LiveMap",
                                "internalID": "LiveMap",
```

```
                                "type": "smartshipping.LiveMap",
                                "root": false
                            }
                        ]
                    }
                ]
            }
        ],
        "simExpectedTraces": [
            {
                "value": "true",
                "name": "smartshipping.LiveMapTurnedOff",
                "seqNo": 1
            }
        ]
    }
]
```


4.2.6 Gamification Sub Model

The scenario's Gamification sub model, specified using the CTTP specification language grammar and fed to the training tool using a JSON format is as follows:


```
[
    {
        "project": {
            "projectID": 2,
            "name": "Navigation combo attack (phishing email and GPS spoofing)",
            "activeFrom": "2020-02-14 13:41:21",
            "statusID": 2,
            "organisationID": 2,
            "lastUpdated": "2020-02-14 13:42:10"
        },
        "organisation": {
            "organisationID": 2,
            "name": "DANAOS Shipping Company LTD ",
            "activeFrom": "2020-02-14 13:38:42",
            "typeID": 3,
            "currencyID": 1,
            "value": 500000.0
        },
        "statusType": {
            "statusID": 2,
            "statusField": "status",
            "statusValue": "final",
            "statusSymbol": "status_final"
        },
        "activeFrom": "2020-02-14 12:00:00",
        "activeTo": "2021-02-14 12:00:00",
        "games": [
            {
                "gameType": {
                    "game": "Protect"
                },
                "protects": [
                    {
                        "difficultyLevel": 2,
                        "gameTime": 12,
                        "cardDeckID": "cd_shipping",
```

```
                    "specialPractice": false
                }
            ]
        },
        {
            "gameType": {
                "game": "Protect"
            },
            "protects": [
                {
                    "difficultyLevel": 1,
                    "gameTime": 15,
                    "cardDeckID": "cd_shipping",
                    "specialPractice": false
                }
            ]
        },
        {
            "gameType": {
                "game": "Protect"
            },
            "protects": [
                {
                    "difficultyLevel": 1,
                    "gameTime": 15,
                    "cardDeckID": "cd_shipping",
                    "specialPractice": false
                }
            ]
        },
        {
            "gameType": {
                "game": "Protect"
            },
            "protects": [
                {
                    "difficultyLevel": 2,
                    "gameTime": 12,
                    "cardDeckID": "cd_shipping",
                    "specialPractice": false
                }
            ]
        }
    ],
    "GamificationExpectedTraces": [
        {
            "action": "fend off attacks",
            "value": "number of correctly and incorrectly fend off attack cards"
        }
    ]
  }
]
```

4.3 Healthcare

4.3.1 Overview

The model for the Scenario 1 of the Healthcare use case will be presented. The description, progression and modelling of it can be found in Section 3.3.1.

4.3.2 Core CTTP Model

The scenario's core CTTP model, specified using the CTTP specification language grammar is as follows:

```
Person(firstName("admin"),lastName("aress"),email("admin@aress
.regione.puglia.it"),value(3000.0),currency(EUR),project("Thre
at Arrest"),organisation("AreSS"),activeTo(2020-11-19
13:55),description("The project administrator for
AreSS"),roles(administrator))
Person(firstName("clinician"),lastName("aress"),email("staff@a
ress.regione.puglia.it"),value(1400.0),currency(EUR),project("
Threat Arrest"),organisation("AreSS"),activeTo(2021-11-19
13:55),description("The clinician"),roles(end_user)),
SoftwareAsset(vendor("postgresql"),version("9.6"),name("postgr
esql"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("AreSS"),owner("admin"),description("Rel
ational Database"))
SoftwareAsset(vendor("Linux"),version("18.04LTS"),name("Ubuntu
"),kind(Service),type(PAL),project("Threat
Arrest"),organisation("AreSS"),owner("admin"),description("Ser
ver OS"))
SoftwareAsset(vendor("Microsoft
Corporation"),version("11.914.17763.0"),name("Windows Internet
Explorer 11"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("AreSS"),owner("admin"))
SoftwareAsset(vendor("Microsoft"),version("10.0.17763"),name("
Windows 10 Proffesional
Edition"),kind(Service),value(259.0),currency(EUR),type(PAL),p
roject("Threat
Arrest"),organisation("AreSS"),owner("staff"),description("Sta
ff OS"))
SoftwareAsset(vendor("Ivan Rashid
S.r.l."),version("19.1.2"),name("CRTool"),kind(Service),value(
500.0),currency(EUR),type(SAL),project("Threat
Arrest"),organisation("AreSS"),owner("admin"),description("Int
ernal application for managing patients"))
SoftwareAsset(vendor("phppgadmin"),version("4.2.2"),name("phpp
gadmin"),kind(Service),type(SAL),project("Threat
Arrest"),organisation("AreSS"),owner("admin"),description("Dat
abase  Administration")),
HardwareAsset(vendor("HP Inc."),version("-"),name("Clinician's
PC"),value(1245.2),currency(EUR),hwType(compute),project("Thre
at
Arrest"),organisation("AreSS"),owner("staff"),activeTo(2022-
12-26 19:50),CpuModule(processorName("Intel Core
```

```
i7"),cores(4),threads(4),baseFrequency(1.6),socket("LG1156")),
MemoryModule(size(32),type("DDR4"),speed(1600.0),manufacturer(
"HP")),PortModule(ioType(usb),isAlwaysConnected(FALSE)),Networ
kAdapter(connectionType(Integrated),MAC("7e:00:8d:d9:ca:cc"),s
upportedProtocol(ethernet),Speed(50.0),IP("228.18.118.121"),Ne
tmask("255.255.255.0"),IpType(Static),dhcp("False")))
HardwareAsset(vendor("HP Inc."),version("-"),name("Host
Machine for
Database"),value(3000.0),currency(EUR),hwType(compute),project
("Threat
Arrest"),organisation("AreSS"),owner("staff"),activeTo(2022-
12-26 19:50),CpuModule(processorName("Intel(R) Core(TM) i7-
8700"),cores(6),threads(12),baseFrequency(3.2),socket("FCLGA11
51")),MemoryModule(size(64),type("DDR4"),speed(3200.0),manufac
turer("HP")),PortModule(ioType(usb),isAlwaysConnected(TRUE)),N
etworkAdapter(connectionType(Integrated),MAC("4e:08:77:9c:72:3
3"),supportedProtocol(ethernet),Speed(50.0),IP("253.91.247.228
"),Netmask("255.255.255.0"),IpType(Static),dhcp("False"))),
Data(name("Patient's
data"),category(security),datastate(at_rest,in_processing),pro
ject("Threat Arrest"),organisation("AreSS"),owner("admin"))
```

4.3.3 Training Programme Sub Model

The scenario's training programme sub model, specified using the CTTP specification language grammar and fed to the training tool using a JSON format is as follows:


```
[
    {
        "description": "The security expert of a regional hospital receives an email from t
he Intrusion Detection System (IDS) that an abnormal action occurred. The trainee is urgent
ly called to investigate the reason that triggered the IDS to send such email. While examin
ing 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 dat
a. The trainee needs to follow certain actions in order to revoke the clinicians account an
d revoke his/her access to the application.",
        "scenarioGoal": {
            "description": "This is a digital forensics scenario to train incident responde
rs how to investigate compromise on the system. The scenario is implemented in Emulation, S
imulation tool and Gamification tool. Additionally, the data fabrication tool is used to ge
nerate log files for the SQL database and add the fabricated users to it.",
            "maxScore": 10,
            "successScore": 5
        },
        "difficulty": 5,
        "activeFrom": "2020-02-20 12:00:00",
        "activeTo": "2021-02-20 12:00:00",
        "organisation": {
            "organisationID": 3,
            "name": "Agenzia Regionale Strategica per la Salute ed il Sociale",
            "activeFrom": "2020-02-19 08:21:47",
            "activeTo": "2020-02-19 08:21:47",
            "typeID": 4,
            "currencyID": 1,
            "value": 500000.0
```

```
        },
        "project": {
            "projectID": 3,
            "name": "Incident Response",
            "activeFrom": "2020-02-14 13:42:13",
            "statusID": 2,
            "organisationID": 3,
            "lastUpdated": "2020-02-14 13:42:35"
        },
        "statusType": {
            "statusID": 2,
            "statusField": "status",
            "statusValue": "final",
            "statusSymbol": "status_final"
        },
        "durationType": {
            "value": 40,
            "durationUnit": {
                "unit": "minutes"
            }
        },
        "typesOfActionTypes": [
            {
                "toatValue": "Preparedness"
            },
            {
                "toatValue": "Post security incident response"
            }
        ],
        "roles": [
            {
                "personroleID": 7,
                "personRoleField": "personRole",
                "personRoleValue": "technician",
                "personRoleSymbol": "personRole_technician"
            },
            {
                "personroleID": 6,
                "personRoleField": "personRole",
                "personRoleValue": "auditor",
                "personRoleSymbol": "personRole_auditor"
            },
            {
                "personroleID": 2,
                "personRoleField": "personRole",
                "personRoleValue": "administrator",
                "personRoleSymbol": "personRole_administrator"
            }
        ],
        "bibliographies": [
            {
                "name": "Digital forensics",
                "text": "https://digital-forensics.sans.org/"
            }
        ],
        "owners": [
            {
                "personID": 44,
```

```
                "firstName": "Admin",
                "lastName": "AreSS",
                "email": "admin@aress.regione.puglia.it",
                "asset": {
                    "assetID": 33,
                    "typeID": 4,
                    "activeFrom": "2020-02-14 14:19:25",
                    "tableName": "Person",
                    "organisationID": 3,
                    "projects": [
                        {
                            "projectID": 3,
                            "name": "Incident Response",
                            "activeFrom": "2020-02-14 13:42:13",
                            "statusID": 2,
                            "organisationID": 3,
                            "lastUpdated": "2020-02-14 13:42:35"
                        }
                    ]
                },
                "statusID": 2,
                "personRoles": [
                    {
                        "prID": 27,
                        "personRole": {
                            "personroleID": 2,
                            "personRoleField": "personRole",
                            "personRoleValue": "administrator",
                            "personRoleSymbol": "personRole_administrator"
                        }
                    }
                ]
            }
        ],
        "trainingProgrammeExecutions": [
            {
                "totalScreens": 1,
                "executionPriority": 1,
                "difficulty": 5,
                "instructions": "The trainee utilises the web tool that handles the adminis
tration of the database to find the user table and set the security flag values (i.e. accou
ntNonExpired, credentialsNonExpired and accountNonLocked) to false. This action immediately
 disables the clinicians account.",
                "screens": [
                    {
                        "screenNumber": 1,
                        "executionTool": {
                            "tool": "Emulation Tool"
                        },
                        "description": "The Postegresql user table that contains the user i
nformation.",
                        "hint": "Modify the security flag values."
                    }
                ],
                "executionDuration": {
                    "value": 15,
                    "durationUnit": {
                        "unit": "minutes"
```

```
                    }
                },
                "hintImpact": 0.5
            },
            {
                "totalScreens": 1,
                "executionPriority": 2,
                "difficulty": 4,
                "instructions": "The trainee utilises the web tool that handles the adminis
tration of the database to find the tables that stores the permissions of each user and rev
oke the clinician’s read and write permissions by removing his/her ID from the table.",
                "screens": [
                    {
                        "screenNumber": 1,
                        "executionTool": {
                            "tool": "Emulation Tool"
                        },
                        "description": "The Postegresql user table that contains the roles
information.",
                        "hint": "Check the roles of the user and delete them."
                    }
                ],
                "executionDuration": {
                    "value": 10,
                    "durationUnit": {
                        "unit": "minutes"
                    }
                },
                "hintImpact": 0.6
            },
            {
                "totalScreens": 1,
                "executionPriority": 3,
                "difficulty": 1,
                "instructions": "The trainee then sends an email to the clinician asking hi
m/her to immediately change the password. He/she also includes a text that informs the clin
ician on how to setup a strong password. ",
                "screens": [
                    {
                        "screenNumber": 1,
                        "executionTool": {
                            "tool": "Emulation Tool"
                        },
                        "description": "The email application.",
                        "hint": "Open the email application. Do not forget to include the s
trong password guideline!"
                    }
                ],
                "executionDuration": {
                    "value": 5,
                    "durationUnit": {
                        "unit": "minutes"
                    }
                },
                "hintImpact": 0.9
            },
            {
                "totalScreens": 1,
```

```
                "executionPriority": 4,
                "difficulty": 6,
                "instructions": "The trainee starts the card game.",
                "screens": [
                    {
                        "screenNumber": 1,
                        "executionTool": {
                            "tool": "Gamification Tool"
                        },
                        "description": "PROTECT card game",
                        "hint": "The training success depends on the number of attack cards
 that the trainee has repeled successfully by selecting the correct defense card"
                    }
                ],
                "executionDuration": {
                    "value": 10,
                    "durationUnit": {
                        "unit": "minutes"
                    }
                },
                "hintImpact": 0.4
            }
        ]
    }
]
```


4.3.4 Emulation Sub Model

The scenario's Emulation sub model, specified using the CTTP specification language grammar and fed to the training tool using an XML format is as follows:


```
<?xml version="1.0" encoding="Unicode" standalone="yes"?>
<Scenario name="UC3-ARESS">
    <CustomVM name="DB_server_UC3" os="windows">
        <connectionmode port="3389" connectiontype="rdp"/>
        <ram val="8192"/>
        <vcpus val="4"/>
        <disk val="80"/>
        <image name="DB_server_UC3" value="DB_server_UC3" username="win10" password="win10"
/>
        <Network idref="internal_network"/>
    </CustomVM>
    <CustomVM name="sim_UC3" os="linux">
        <connectionmode port="22" connectiontype="ssh"/>
        <ram val="4096"/>
        <vcpus val="2"/>
        <disk val="40"/>
        <image name="sim_UC3" value="ubuntu-sim-red" username="ubuntu"/>
        <Network idref="internal_network"/>
        <Scripts idref="Simulation_script"/>
    </CustomVM>
    <Networks>
        <network id="internal_network">
            <gateway name="gateway-internal_network" val="20.50.1.1"/>
            <cidr name="cidr-internal_network" val="20.50.1.0/24"/>
            <is_external val="false"/>
        </network>
    </Networks>
```

```
    <Scripts><Script id="Simulation_script">![CDATA[ echo "start user data" java -jar sim-
controller.jar & echo "end user data" ]]></Script>
</Scripts>
</Scenario>
```

4.3.5 Simulation Sub Model

The scenario's Simulation sub model, specified using the CTTP specification language grammar and fed to the training tool using a JSON format is as follows:

```
[
    {
        "tool": "Jasima",
        "template": "Simulation/healthcare.jasima",
        "simTime": 0,
        "executionSpeed": 1,
        "randomSeed": 42,
        "project": {
            "projectID": 3,
            "name": "Incident Response",
            "activeFrom": "2020-02-14 13:42:13",
            "statusID": 2,
            "organisationID": 3,
            "lastUpdated": "2020-02-14 13:42:35"
        },
        "organisation": {
            "organisationID": 3,
            "name": "Agenzia Regionale Strategica per la Salute ed il Sociale",
            "activeFrom": "2020-02-19 08:21:47",
            "activeTo": "2020-02-19 08:21:47",
            "typeID": 4,
            "currencyID": 1,
            "value": 500000.0
        },
        "statusType": {
            "statusID": 2,
            "statusField": "status",
            "statusValue": "final",
            "statusSymbol": "status_final"
        },
        "activeFrom": "2020-02-26 12:00:00",
        "activeTo": "2021-02-26 12:00:00",
        "deploymentMode": {
            "dmtID": 2,
            "dmtField": "DeploymentMode",
            "dmtValue": "Template",
            "dmtSymbol": "DeploymentMode_Template"
        },
        "SimulationComponents": [
            {
                "name": "MainNetwork",
                "simulatedComponent": "MainNetwork",
                "type": "jasima.core.Simulation.SimComponentContainerBase",
                "root": true,
                "componentContainers": [
                    {
                        "simpleComponents": [
                            {
                                "name": "ResultChecker",
```

```
                                "internalID": "ResultChecker",
                                "type": "healthcare.ResultChecker",
                                "root": false,
                                "attributes": [
                                    {
                                        "name": "dbUserName",
                                        "initialValue": "root",
                                        "type": "String",
                                        "canChange": false
                                    },
                                    {
                                        "name": "dbUserPassword",
                                        "initialValue": "passwd",
                                        "type": "String",
                                        "canChange": false
                                    },
                                    {
                                        "name": "checkIntervalInSeconds",
                                        "initialValue": "5",
                                        "type": "Integer",
                                        "canChange": false
                                    },
                                    {
                                        "name": "dbConnectString",
                                        "initialValue": "jdbc:postgresql://192.168.
2.1/test",
                                        "type": "String",
                                        "canChange": false
                                    },
                                    {
                                        "name": "userToCheck",
                                        "initialValue": "user2",
                                        "type": "String",
                                        "canChange": false
                                    }
                                ]
                            }
                        ]
                    }
                ]
            }
        ],
        "simExpectedTraces": [
            {
                "value": "true",
                "name": "healthcare.UserAttributesSet",
                "seqNo": 1
            }
        ]
    }
]
```


4.3.6 Gamification Sub Model

The scenario's Gamification sub model, specified using the CTTP specification language grammar and fed to the training tool using a JSON format is as follows:


```
[
    {
```

```
        "project": {
            "projectID": 3,
            "name": "Incident Response",
            "activeFrom": "2020-02-14 13:42:13",
            "statusID": 2,
            "organisationID": 3,
            "lastUpdated": "2020-02-14 13:42:35"
        },
        "organisation": {
            "organisationID": 3,
            "name": "Agenzia Regionale Strategica per la Salute ed il Sociale",
            "activeFrom": "2020-02-19 08:21:47",
            "activeTo": "2020-02-19 08:21:47",
            "typeID": 4,
            "currencyID": 1,
            "value": 500000.0
        },
        "statusType": {
            "statusID": 2,
            "statusField": "status",
            "statusValue": "final",
            "statusSymbol": "status_final"
        },
        "activeFrom": "2020-02-14 12:00:00",
        "activeTo": "2021-02-14 12:00:00",
        "games": [
            {
                "gameType": {
                    "game": "Protect"
                },
                "protects": [
                    {
                        "difficultyLevel": 2,
                        "gameTime": 12,
                        "cardDeckID": "cd_healthcare",
                        "specialPractice": false
                    }
                ]
            },
            {
                "gameType": {
                    "game": "Protect"
                },
                "protects": [
                    {
                        "difficultyLevel": 2,
                        "gameTime": 12,
                        "cardDeckID": "cd_healthcare",
                        "specialPractice": false
                    }
                ]
            },
            {
                "gameType": {
                    "game": "Protect"
                },
                "protects": [
                    {
```

```
                        "difficultyLevel": 1,
                        "gameTime": 15,
                        "cardDeckID": "cd_healthcare",
                        "specialPractice": false
                    }
                ]
            },
            {
                "gameType": {
                    "game": "Protect"
                },
                "protects": [
                    {
                        "difficultyLevel": 1,
                        "gameTime": 15,
                        "cardDeckID": "cd_healthcare",
                        "specialPractice": false
                    }
                ]
            }
        ],
        "GamificationExpectedTraces": [
            {
                "action": "fend off attacks",
                "value": "number of correctly and incorrectly fend off attack cards"
            }
        ]
    }
]
```


4.3.7 Data Fabrication Sub Model

The scenario's data fabrication sub model, specified using the CTTP specification language grammar and fed to the training tool using a JSON format is as follows:


```
[
    {
        "name": "p1",
        "activeFrom": "2020-02-14 12:00:00",
        "activeTo": "2021-02-14 12:00:00",
        "organisation": {
            "organisationID": 3,
            "name": "Agenzia Regionale Strategica per la Salute ed il Sociale",
            "activeFrom": "2020-02-19 08:21:47",
            "activeTo": "2020-02-19 08:21:47",
            "typeID": 4,
            "currencyID": 1,
            "value": 500000.0
        },
        "project": {
            "projectID": 3,
            "name": "Incident Response",
            "activeFrom": "2020-02-14 13:42:13",
            "statusID": 2,
            "organisationID": 3,
            "lastUpdated": "2020-02-14 13:42:35"
        },
        "statusType": {
            "statusID": 2,
```

```
            "statusField": "status",
            "statusValue": "final",
            "statusSymbol": "status_final"
        },
        "scenario": [
            {
                "nodes": [
                    {
                        "node": "net.victimnet.client",
                        "application": "MailClient",
                        "nodeFunction": "Login",
                        "name": "Login",
                        "type": "action"
                    },
                    {
                        "node": "net.victimnet.client",
                        "application": "FileSystem",
                        "nodeFunction": "Save",
                        "name": "SaveFile",
                        "type": "action",
                        "constraints": [
                            {
                                "name": "filename",
                                "dfConstraint": "Filename = s'trojan_horse.exe'"
                            }
                        ]
                    },
                    {
                        "node": "net.attackernet.client",
                        "application": "MailClient",
                        "nodeFunction": "Send Mail",
                        "name": "SendMail",
                        "type": "action",
                        "constraints": [
                            {
                                "name": "mailSubject",
                                "dfConstraint": "Subject = s'This is a phishing mail!!!'"
                            },
                            {
                                "name": "victimMail",
                                "dfConstraint": "To = s'victim@victimdomain.com'"
                            },
                            {
                                "name": "mailAttachment",
                                "dfConstraint": "Attachment = s'trojan_horse.exe'"
                            }
                        ]
                    },
                    {
                        "node": "net.victimnet.client",
                        "application": "MailClient",
                        "nodeFunction": "Open Mail",
                        "name": "OpenMail",
                        "type": "action",
                        "constraints": [
                            {
                                "name": "victimMail",
                                "dfConstraint": "From = s'attacker@attackerdomain.com'"
```

```
                        },
                        {
                            "name": "mailSubject",
                            "dfConstraint": "Subject = s'This is a phishing mail!!!'"
                        }
                    ]
                }
            ]
        }
    ],
    "network": [
        {
            "name": "net",
            "type": "subnet",
            "subnet": [
                {
                    "name": "victimnet",
                    "type": "subnet",
                    "subnet": [
                        {
                            "name": "client",
                            "stereotype": "client",
                            "type": "node",
                            "constraints": [
                                {
                                    "name": "Username",
                                    "dfConstraint": "MailClient.Username = s'victim'"
                                },
                                {
                                    "name": "IP",
                                    "dfConstraint": "Communicator.IP = s'192.168.2.1'"
                                }
                            ],
                            "connections": [
                                {
                                    "connection": "net.victimnet.mailserver"
                                }
                            ],
                            "apps": [
                                {
                                    "name": "MailClient"
                                },
                                {
                                    "name": "FileSystem"
                                },
                                {
                                    "name": "Communicator"
                                }
                            ]
                        },
                        {
                            "name": "mailserver",
                            "stereotype": "mailserver",
                            "type": "node",
                            "constraints": [
                                {
                                    "name": "MailDomain",
```

```
                                    "dfConstraint": "MailServer.MailDomain = s'victimdo
main.com'"
                                },
                                {
                                    "name": "IP",
                                    "dfConstraint": "Communicator.IP = s'192.168.2.0'"
                                }
                            ],
                            "connections": [
                                {
                                    "connection": "net.victimnet.client"
                                },
                                {
                                    "connection": "net.victimnet.client,net.attackernet
.mailserver"
                                }
                            ],
                            "apps": [
                                {
                                    "name": "Communicator"
                                },
                                {
                                    "name": "MailServer"
                                }
                            ]
                        }
                    ],
                    "constraints": [
                        {
                            "name": "SameMailDomain",
                            "dfConstraint": "client.MailClient.MailDomain = mailserver.
MailServer.MailDomain"
                        }
                    ]
                },
                {
                    "name": "attackernet",
                    "type": "subnet",
                    "subnet": [
                        {
                            "name": "client",
                            "stereotype": "client",
                            "type": "node",
                            "constraints": [
                                {
                                    "name": "Username",
                                    "dfConstraint": "MailClient.Username = s'attacker'"
                                },
                                {
                                    "name": "IP",
                                    "dfConstraint": "Communicator.IP = s'192.168.1.1'"
                                }
                            ],
                            "connections": [
                                {
                                    "connection": "net.attackernet.mailserver"
                                }
                            ],
```

```
                            "apps": [
                                {
                                    "name": "Communicator"
                                },
                                {
                                    "name": "MailClient"
                                },
                                {
                                    "name": "FileSystem"
                                }
                            ]
                        },
                        {
                            "name": "mailserver",
                            "stereotype": "mailserver",
                            "type": "node",
                            "constraints": [
                                {
                                    "name": "MailDomain",
                                    "dfConstraint": "MailServer.MailDomain = s'attacker
domain.com'"
                                },
                                {
                                    "name": "IP",
                                    "dfConstraint": "Communicator.IP = s'192.168.1.0'"
                                }
                            ],
                            "connections": [
                                {
                                    "connection": "net.victimnet.mailserver"
                                },
                                {
                                    "connection": "net.attackernet.client"
                                }
                            ],
                            "apps": [
                                {
                                    "name": "Communicator"
                                },
                                {
                                    "name": "MailServer"
                                }
                            ]
                        }
                    ],
                    "constraints": [
                        {
                            "name": "SameMailDomain",
                            "dfConstraint": "client.MailClient.MailDomain = mailserver.
MailServer.MailDomain"
                        }
                    ]
                }
            ]
        }
    ]
}
]
```

5 Conclusions

This deliverable is the initial output of task "T3.2 – CTTP models and programmes development". As such, it details the development of the CTTP models and CTTP programmes for all the three pilots of THREAT-ARREST, and the specification of these models and programmes in an executable form using the language developed in "T3.1 - CTTP Language definition and Tool Support".

The goal of this first version is to define the training programmes and the scenarios for the THREAT-ARREST pilots and provide the specification of a scenario per pilot.

Next steps in the second year of the project aim to address the creation of the models for every scenario identified in Section 3 and the creation of more sophisticated scenarios. The enhancement scenarios will also contain the updates of the CTTP Models and Programmes Specification Language that will be introduced later in the project.

6 References

[1] ANSSI. (2016). *Protection Profile for Signature Activation Protocol (SAP) management.*

[2] Application Software Protection Profile (ASPP). (2014). *Extended Package: File Encryption:Mitigating the Risk of Disclosure of Sensitive Data on a System.*

[3] Bundesamt für Sicherheit in der Informationstechnik (BSI) / Federal Office for Information Security, Germany. (2017, June 23). *Protection Profile for the Security Module of a Smart Meter Mini-HSM(Mini-HSM Security Module PP).* Retrieved 2020, from https://www.commoncriteriaportal.org/files/ppfiles/pp0095b_pdf.pdf

[4] CESG. (2016). *CPA Security Characteristic Smart Metering – Communication Hub v1.2.* Retrieved from https://www.ncsc.gov.uk/files/CPA_SC_CH_v1_3_0..PDF

[5] CESG. (2016). *Secure Real-Time Communications Client: CPA SC, v2.1.* Retrieved from https://www.ncsc.gov.uk/files/CPA-SC_Secure_real-time_communications_client_2-2.pdf

[6] CIS. (2020). *Center of Internet Security*. Retrieved from https://www.cisecurity.org/

[7] Common Criteria : New CC Portal. (2020). *Commoncriteriaportal.org*. Retrieved from https://www.commoncriteriaportal.org/

[8] ENISA. (2016). *Cyber Security and resilience for Smart Hospitals.* Retrieved 2019, from https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals .

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

[10] Hatzivasilis, G., et al., 2019b. Towards the Insurance of Healthcare Systems. 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Springer, LNCS, vol. 11981, Luxembourg, 27 September 2019, pp. 1-14.

[11] Hatzivasilis, G., et al., 2016. Lightweight authenticated encryption for embedded on-chip systems.Information Security Journal: A Global Perspective, Taylor & Francis, vol. 25, issue 4-6, pp. 151-161.

[12] Hatzivasilis, G., et al., 2015. Lightweight password hashing scheme for embedded systems. 9th WG 11.2 International Conference on Information Security Theory and Practice (WISTP), IFIP, Heraklion, Crete, Greece, 24-25 August 2015, Springer, LNCS, 9311, pp. 249-259.

[13] IMO. (2004). *SOLAS chapter XI-2 - International Ship and Port Facility Security Code (ISPS Code).* IMO.

[14] International Organization for Standardization. (2018). *ISO/IEC 27001 Information security management.*

[15] Isaca.org. (2020). *COBIT | Control Objectives for Information Technologies ISACA.* Retrieved from https://www.isaca.org/resources/cobit

[16] Jürgen Blum,Marion Brinkkötter. (2014). *Common Criteria Protection Profile – Mobile Card Terminal for the German Healthcare System (MobCT).*

[17] Manifavas, C., et al., 2015. A survey of lightweight stream ciphers for embedded systems. Security and Communication Networks, Wiley, vol. 9, issue 10, pp. 1226-1246.

[18] Manifavas, C., et al., 2013. Lightweight cryptography for embedded systems – a comparative analysis. 6th International Workshop on Autonomous and Spontaneous Security (SETOP 2013), in conjunction with the 18th annual European research event in Computer Security (ESORICS 2013) symposium, 12-13 September 2013, RHUL, Egham, U.K., Springer, LNCS, vol. 8247, pp. 333-349.

[19] National Information Assurance Partnership. (2014). *Protection Profile for Application Software.*

[20] NIST. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 R4).*

[21] OpenStack. (2020). *OpenStack.* Retrieved 2020, from https://www.openstack.org/

Appendix I – Pilot Requirements

This appendix summarizes the pilot requirements, as they were documented in the deliverable "D1.1 – The pilots' requirements analysis report". Totally, there are **27 defined requirements** (2 general (legal) requirements, as well as, 10 for the Smart Home - IoT, 7 for the Healthcare and 8 for the Smart Shipping pilot, respectively).

Table 4. Pilot requirements

Req.-Id	Description	Req. Level (MUST / SHOULD)	Indicative Use-Case scenario
Smart Energy			
Energy_R_01	IoT Authentication and Authorization	Must	Authentication and authorization are essential parts of basic security processes and are sorely needed in the Internet of Things (IoT). The emergence of edge and fog computing creates new opportunities for security and trust management in the IoT. Efficient and scalable trust management for the IoT based on locally centralized, globally distributed trust management using an open source infrastructure with local authentication and authorization entities to be deployed on edge devices.
Energy_R_02	Emerging Technologies for IoT Security	Must	Emerging Technologies Spearheading the IoT Security. For example: 1. **Blockchain** is already being considered as a panacea for all security and accountability related issues faced by multiple industries. The inherent security features of Blockchain makes it an ideal choice for implementing various security measures in IoT. From data security, to managing authorizations and device identification, Blockchain is being imagined as the middleware security layer for IoT systems. Many of these ideas are in the research phase, and some initial implementations exist. 2. **Software Defined Networking (SDN)** With the threat of large-scale DDoS attacks looming over the Internet and orchestrated through a huge army of compromised IoT devices, there is a lot of research going on in the areas of early detection of such attacks. SDN can possibly offer a solution to this. The SDN controllers which administer a network domain can communicate with SDNi, a set of specifications that enable Inter SDN

			controller communication. By exchanging information through SDNi, the neighbor SDN controllers can gauge some early warnings signs about an imminent DDoS attacks targeting computers in their neighbourhood. This can immensely help network administrators to take corrective actions in time to mitigate the further propagation of attacks. 3. **AI & Big Data** A big data repository of such metrics can be leveraged to run machine learning models for conducting periodic audit of networks for possible IoT security breaches. We have seen Google and other online services employing such measures to authenticate user access to their services. If you remember Google asking you for your location, or confirming your account through an OTP, then you know what is happening behind the scenes. There is big data and AI at play which checks for any anomaly in user access, such as location change, too frequent logins or even periodic checks. Something in similar lines needs to be done for IoT devices as well.
Energy_R_03	Possibilities for Hackers on IoT devices	Must	Examples and real cases of attacks in the residential Sector. Having the ability to heat up your house before you get home or use your phone to control when the coffee pot turns on really isn't a technology to be dismissive of. Using your voice to tell your TV what to play makes people feel as though they're living in the future. These rewards lead people to continue buying the new IoT device, even though their security might be on the line. So, going into the years ahead, the question cannot be about making people value their security over convenience. Instead, it should be about educating IoT professionals to do more to make their IoT devices secure and transparent with how they manage customer's information.
Energy_R_04	Lightweight cryptography for the Internet of things	Should	This topic must give an overview of the state-of-the-art technology and standardization status of lightweight cryptography, which can be implemented efficiently in constrained devices. This technology enables secure and efficient communication between networked smart objects.
Energy_R_05	Analysing the Risks	Should	This topic combines knowledge of Security Risk Management with existing practice in securing in IoT into a framework, which aim is to cover vulnerabilities in IoT systems in order to protect users' data. We propose an initial comprehensive reference

			model to management security risks to the information and data assets managed and controlled in the IoT systems. Based on the domain model for the information systems security risk management, we explore how the vulnerabilities and their countermeasures defined in the distributed energy context.
Energy_R_06	Elliptic curve cryptography (ECC) asymmetric algorithm	Must	The elliptic curve cryptography (ECC) asymmetric algorithm is widely promoted to developers for new Internet of Things (IoT) advancements. Constraints in IoT include limitations to computational resources such as the bare minimum processor speed and memory needed as such devices are typically designed for low power consumption. Challenges include the need to reengineer things such as identity management, device and user registration, and cryptography to suit IoT needs.
Energy_R_07	WiFi Vulnerabilities and security measures	Must	Common protocol vulnerabilities and ways to secure and maintain confidentiality, integrity, and availability over this protocol
Energy_R_08	ZigBee Vulnerabilities and security measures	Must	Common protocol vulnerabilities and ways to secure and maintain confidentiality, integrity, and availability over this protocol
Energy_R_09	MQTT Vulnerabilities and security measures	Must	Common protocol vulnerabilities and ways to secure and maintain confidentiality, integrity, and availability over this protocol
Energy_R_10	CoAP Vulnerabilities and security measures	Must	Common protocol vulnerabilities and ways to secure and maintain confidentiality, integrity, and availability over this protocol
Healthcare			
Health_R_01	Train user to identify risk related to email authenticity	Must	The user will receive email from known contacts with malicious code and link; assess the behaviour of the user
Health_R_02	Train user on basic Internet navigation and update procedures	Must	The user will be faced with possible tool and update download from suspicious and known website; assess the compliance of the user on security policies
Health_R_03	Train administrator on basic database management and protection procedure	Must	The administrator will face attacks of SQL injection and attempt to assess to central and distributed databases
Health_R_04	Raise awareness on the threat of external computers and equipment joining the network	Should	The administrator needs to apply suitable countermeasures in case of attacks coming from external computers and equipment that are added to the network; the administrator should react in case the common security policies does not protect in full the architecture

Health_R_05 (from Shipping_R_05)	Train designated IT security personnel of the Agency for risks related to poor software and data security practices where no anti-virus checks or authenticity verifications are performed	Should	The users will face frequent system crashes to assess their awareness on system malfunction along with mitigation actions that users should take and route cause analysis that users should perform as countermeasure
Health_R_06 (from Shipping_R_07)	Train user on identifying Cyber Risks in relation to the physical presence of non-Agency personnel	Should	System infrastructure will be attacked by compromising equipment, software or supporting services being delivered to the Agency or Hospitals by third-party providers, e.g. where third-party technicians are left to work on equipment without supervision
Health_R_07 (from Shipping_R_06)	Train user over safeguarding information, passwords and digital certificates	Must	Trigger a scenario where unexpected password changes or authorized users being locked out of a system
Smart Shipping			
Shipping_R_01	Train user to identify risks related to emails and how to behave in a safe manner	Must	Phishing attacks where a user of e.g. supplier department is called via email to click on a link to a malicious site to reach a candidate supplier in order to request quotations
Shipping_R_02	Train user to identify risks related to Internet usage, including social media, chat forums and cloud-based file storage where data movement is less controlled and monitored	Should	Social Engineering attacking while e.g. crew on-board is interacting with social media through WiFi when vessel is at terminal
Shipping_R_03	Train user to identify risks related to the use of own devices (these devices may be missing security patches and controls, such as anti-virus, and may transfer the risk to the environment to which they are connected)	Should	Trigger a scenario where a malware is infecting company's network at shore due to connection of a network component (e.g. user workstation) with suspicious uncertified devices (user mobile).
Shipping_R_04	Train user to identify risks related to installing and maintaining software on company hardware using infected hardware (removable media) or software (infected package)	Must	Trigger a scenario where an update of ECDIS navigation system is performed with an uncertified USB. False Objects on digital nautical charts will be displayed along the route and user will be assessed over identifying any anomaly on navigational information and the mitigation action that should take

Shipping_R_05	Train designated IT security personnel of the company for risks related to poor software and data security practices where no anti-virus checks or authenticity verifications are performed	Should	Release frequent system crashes to assess user awareness on system malfunction along with mitigation actions that user should take and route cause analysis that user should perform
Shipping_R_06	Train user over safeguarding information, passwords and digital certificates	Must	Trigger a scenario where unexpected password changes or authorised users being locked out of a system
Shipping_R_07	Train user on identifying Cyber Risks in relation to the physical presence of non-company personnel	Should	Attacking office or ship by compromising equipment, software or supporting services being delivered to the office or ship by third-party providers. e.g., where third-party technicians are left to work on equipment without supervision
Shipping_R_08	Raise awareness of the consequences or impact of Cyber Incidents to the safety and operations of the ship and the readiness or knowledge of user to mitigate risks by evaluating the user on following standard controls over risk in case of a Cyber Threat or attack	Must	Assessor component activated in every platform training scenario to checkout real time the set of actions trainee takes against standard procedures in case of a Cyber Attack.
General (legal)			
All -R_01	Train user on general and specific security-related legal framework and to identify violation of legal security requirements in case of a breach	Must	Any breach of security may point at a violation by the organisation of general or specific security requirements imposed upon it and would therefore require the organisation's personnel to identify and remediate such violations in order for it to improve compliance with its security-related obligations
All -R_02	Train user on statutory and non-statutory breach notification requirements	Must	Any breach of security may entail a breach notification obligation internally within the organisation or externally and would therefore require the organisation's personnel to assess the breach and identify the existence of any such statutory or non-statutory notification requirements.