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

D8.3: The THREAT-ARREST market analysis, business and marketing plan v1†

Abstract: This deliverable provides the 1st version of the market analysis, as well as the business and marketing plan, for the THREAT-ARREST solution.

Contractual Date of Delivery	31/08/2019
Actual Date of Delivery	31/08/2019
Deliverable Security Class	Public
Editor(s)	*Konstantinos Fysarakis, Michalis Smyrlis (STS)*
Contributors	ARESS, ATOS, B&B, DANAOS, IBM, ITML, LSE, SEA, STS, TUV
Quality Assurance	*Fulvio Frati (UMIL), Dirk Wortmann (SIMPLAN)*

† *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. *Dirk Wortmann (SIMPLAN)*
2. *Fulvio Frati (UMIL)*

Revisions

Version	Date	By	Overview
3.0	26/08/2018	Editor	Final version
2.0	24/08/2018	Editor	Addressed reviewers' comments
1.0	22/08/2018	Editor	Added reviewers' comments
0.99	01/08/2019	Editor	Updated with smart energy requirements in section 2 – production of review-ready version
0.9	01/08/2019	Editor	New content and edits in Sections 2 & 3, updates and corrections throughout the document, introduction & conclusions
0.41	31/07/2019	Editor	Updated section 3
0.3	30/07/2019	Editor	Formatting and new content on all sections
0.2	22/07/2019	Editor	Updated with received contributions
0.1	04/06/2019	Editor	First Draft

Executive Summary

The main objective of the current document is to deliver the initial version of the market that the THREAT-ARREST project is targeting and the business plan that we are going to follow. This deliverable is the first output of the task "T8.2 – Sustainability management and Business continuity" and provides:

1. An initial version of the market analysis by examining the existing market solutions,
2. An analysis of the training needs and the costs for the THREAT-ARREST pilots,
3. The business plan that will be followed, and
4. The Marketing strategy

A well-defined market analysis will allow the THREAT-ARREST partners to have a clear representation of its structure, its key players and their demands and to develop a strong marketing strategy.

Table of Contents

List of Abbreviations

API Application Programming Interface

ASAP Automated Security Awareness Platform

BCR Binding Corporate Rules

CA Consortium Agreement

CPU Central Processing Unit

CSO Company's Security Officier

CTTP Cyber Threat and Training Preparation

CTTP Cyber Training and Threat Preparation

DFP Data Fabrication Platform

DOD Department of Defence

DPI Deep Packet Inspection

DSP Digital Service Provider

DSV Design-to-Value

DTS Design-to-cost

EEA European Economic Area

EFTA European Free Trade Association

GIG Global Information Grid

GKO Global Key Offering

GRC Governance, Risk and Compliance

GYR Gross Yearly Retribution

GYR Gross Yearly Retribution

ICT Information and Communication Technology

IDS Intrusion Detection System

IoT Internet of Things

IPR Intellectual Property Rights

IPS Intrusion Prevention System

KIPS Kaspersky Interactive Protection Simulation

LE Large Enterprise

MCR Michigan Cyber Range

MSSPs Managed Security Service Providers

NPV Net-Present Value

OES Operator of Essential Services

OSS Open Source Software

P&L Profit & Loss

PEST Political, economic, socio-cultural and technological

R&D Research and Development

SCCG Stakeholder Cybersecurity Certification Group

SLA Service Level Agreement

SME Small-medium Enterprise

SMS Safety Management System

SSH Secure Shell

SSL Secure Socket Layers

SWOT Strengths, Weaknesses, Opportunities, and Threats

TCO Total Cost of Ownership

TSL Transport Socket Layers

VPN Virtual Private Network

List of Tables

List of Figures

1 Introduction

This deliverable aims to give a description of the different technologies that are the objective of the THREAT-ARREST project, a first description of the market that it is targeting and the business plan that we are going to follow.

The scope of this document, as the first output of task "T8.2 – Sustainability management and Business continuity", is to provide a first version of the market analysis of the current market by investigating current solutions and approaches of cyber ranges, including a market segmentation and classification of these solutions that are available as commercial components.
Moreover, the deliverable aims to provide an analysis of the costs and training needs for the project's pilots, as well as the business plan and the market strategy that is going to be followed to achieve the project's goals.
As such, the deliverable is organised as follows: Section 2 presents the Market Analysis, focusing on training needs in general as well as the specific domains and includes an analysis of the current offerings (i.e. the "competitors" of THREAT-ARREST); Section 3 presents the preliminary Business Plan that the consortium intends to follow, covering aspects such as the potential impact, exploitation pricing schemes and PEST/SWOT analyses; Section 4 details the marketing strategy to be followed, including dissemination and communication activities, and; Section 5 concludes the deliverable.

2 Market Analysis

Massive advancements in computing and communication technologies have given rise to the cyber-infrastructure, enabling the acquisition, storage, sharing, integration and processing of data, through distributed software services cutting across organizational and national boundaries. This cyber infrastructure has facilitated the development of complex interconnected cyber systems, supporting an increasing spectrum of every day personal, societal and business activities, making modern society and enterprise increasingly dependent on them (e.g. (Alexandris et al., 2018; Soultatos et al., 2019; Hatzivasilis et al., 2019a; Hatzivasilis et al., 2019b)). Typically, such systems are composed of a large number of highly distributed and heterogeneous software, hardware, network, and sensing components and devices, which are not under a single operational ownership and control and may be provided as products or services from third parties.

The vast levels of data sharing and cyber systems interoperability, as well as their complex compositional structures have also led to increasingly sophisticated, stealthy, targeted, and multi-faceted cyber-attacks. The "cyber-war" against essential infrastructures around the globe has already been underway. Preserving the security of cyber systems is a particularly challenging problem (Fysarakis et al., 2014, Manifavas et al., 2014). This is due to the inherent difficulty of: (i) identifying vulnerabilities in the complex end-to-end compositions of heterogeneous components and devices of such systems, (ii) selecting appropriate security controls for them, and (iii) preserving end-to-end security when dynamic changes occur in the components, the compositional structures and the infra- structures that they deploy.

Moreover, several security breaches today originate from people that have access to a system (i.e., malicious or negligent insiders). Such insiders include employees, temporary employees, contractors or, even, other business partners. The RSA hack in 2011 and the Ukraine Power Hack in 2015 started by a human executing a macro with malware inside an Excel Sheet ((Dark Reading, 2019), (BBC News, 2019)). To be able to fortify a system from insiders and strengthen its security, it is necessary to train insiders to good security practices and increase their awareness to potential attacks, as knowledge about threats and countermeasures influences adherence to good security practices (Siponen, et al., 2014) . However, despite the importance of security training, the initiatives to “educate” enterprise personnel (particularly of SMEs) and make it realize the importance of cyber-security are limited (ENISA, 2019). In a survey conducted by ESET about cyber security in small businesses, 40% of the respondents said they do not provide any cyber-security training or education for employees (ESET, 2019).

Thus, the provision of effective and comprehensive security training in organizations and enterprises is becoming necessary due to the complexity of cyber systems and the need to be secured since cyber-attacks are increasing and become more sophisticated. Today, there is a plethora of tools that may be used for this purpose, including (i) tools that can detect system vulnerabilities by analysing statically their implementation code (e.g., code analysis tools); (ii) tools that can test statically (i.e., prior to system deployment) and/or dynamically (i.e., at runtime) the robustness of the implemented security controls of computer systems (e.g., passive and active penetration testing tools such as configuration testing, SSL/TLS testing, authentication testing, data validation testing); and (iii) tools for monitoring the runtime operation of such systems in order to detect attacks and the effectiveness of the undertaken responses against them (signature and anomaly intrusion detection systems). Tools of these types may operate at different layers of a cyber-system, including its edge devices, network, compute infrastructure, middleware, and software application layers.

A cyber range is a virtual environment/platform that is used for cyber security training and simulation purposes. It provides tools to develop a safe and legal environment for users to

gain cyber skills for developing secure products, so as to help strengthen the stability, security and performance of cyber-infrastructures and IT systems.
It may include actual hardware and software or a combination of actual and virtual components. It also involves simulated traffic and it replicates network services, based on the requirements of the users. Thus, cyber ranges are virtual environments that use actual network equipment, as required. Its goal is to provide:

- performance-based learning and assessment;
- simulated environments improve teamwork and team capabilities;
- real-time feedback;
- simulate on-the-job experience; and
- an environment where new ideas can be tested to solve complex cyber problems.

Cyber range includes a continuous research on cyber threats, a certification/assessment process of the systems against the identified threats and their updates, a continuous education of personnel for new threats and the development of exercises and training material to cover any changes that occur over the time. Figure 1 below depicts the continuous update of cyber range environments.

Figure 1. Cyber range environments

Being virtual environments, cyber ranges are not only restricted to an organization's local network but they can range from single standalone ranges in an organization to replicating ranges through the Internet, so as to be accessed from around the world and be used by either private or public organizations (US Department of Commerce, 2017).

2.1 Training Needs and Costs

2.1.1 Healthcare environment

It's well-known that Healthcare employees must undergo regular and comprehensive training so organizations can better avoid potential data security threats, because of a lack of awareness, mandatory in order to stop preventable cyber incidents.
Left unchecked, these employees are putting their organizations at serious risk of material loss or confidentiality due to a data breach or other cyber incident. The danger of sensitive data of patients or data compromised by a data breach threatens health organizations of all sizes and health sector is one of most profitable for cyber criminals.
The *Cancer Registry*, managed by ARESS, is the Pilot involved in the present project. The registry is a very sensitive environment due to plenty of processed health-related data and to the several actors working with it.
We have three different roles for people working with it:

1) The Director of the Epidemiology Unit (Responsible for the Register in the Local Health Unit), usually a Doctor;
2) The Registry Operators, both Doctors and Paramedics or administration staff;
3) The members of technical staff, composed by personnel from ARESS, InnovaPuglia (In-house provider of the Apulia Region) and by the provider of the management software of the Cancer Registry.

The role of Doctors and operators in cybersecurity is unique. They move through nearly all of Registry's critical-information systems - patient records, test results, surgical monitoring, and more - but their knowledge about threats and danger deriving from misuse of IT tools is very low. So, the training hours on the platform will be directly proportional to their learning needs.
The time spent in training should be dedicated to the following activities:

- Connect to THREAT-ARREST Platform and select the scenario;
- Play the selected scenario;
- Verify results and fill in the gaps, if present;

Instead, technical staff has less training needs than doctors, in consideration of their higher qualification about the threats.
We think that a fair and sufficient amount of training hours is the following:

1) The Director of the Complex Unit => 2 hours monthly;
2) The Register Operators => 2 hours weekly for the first month (crash course); then, 2 hours monthly;
3) The members of technical staff => 2 hours bimonthly.

This training plan was devised in two steps: estimating the total number of hours (*) necessary for the training of personnel, considering the training needs of each role (Director, operators, technical staff) of the Cancer Registry; planning training sessions based on the workload of the personnel.
This number was identified by analysing similar computer training programs promoted by the Puglia Region in the past.

Another figure involved in training program is the Trainer, the IT Manager of ARESS, who is responsible for calling employees and for providing them scenarios and campaign of training and evaluating results and progressions. His effort is described as following:

- He calls the trainees scheduling their training sessions;
- He provides the scenarios and tracks their progression and results;
- He evaluates the levels gained by the trainees.
- We think that a fair and sufficient amount of effort hours is 2 hours monthly.

In relation to the costs concerning the above-mentioned categories of people involved, we have the following scheme:

1) Director of the Epidemiology Unit => €999,12;
2) Registry Operators => €631,80/each;
3) Members of technical staff => €504,72/each;
4) IT Manager => €838,08.

The costs are to be considered annual and are calculated as shown in Table 1:

Table 1 . Costs per type of employee (in details)

Type of employee	Gross Yearly Retribution (GYR)	Social Security Contributions (SSC)			Total cost (GYR + SSC)	Working Hours	Hourly cost (Tot Cost / WH)
		INPS	IRAP	INAIL			
Director of the Epidemiology Unit	€ 52.020,80	€ 14.945,58	€ 4.421,77	€ 208,08	€ 71.596,23	1720	€ 41,63
IT Manager	€ 43.635,80	€ 12.536,57	€ 3.709,04	€ 174,54	€ 60.055,95	1720	€ 34,92
Registry Operators	€ 26.020,41	€ 7.894,59	€ 2.211,73	€ 104,08	€ 36.230,82	1720	€ 21,06
Members of technical staff	€ 26.020,41	€ 7.894,59	€ 2.211,73	€ 104,08	€ 36.230,82	1720	€ 21,06

It should be noted that the GYR (Gross Yearly Retribution) has been divided by 1720 hours, in accordance with the provisions of REG. EU 1303/2013 art. 68 par. 2 (EU, 2017) so if the hourly cost is not useful for the reporting of particular funds, the GYR should be divided not by 1720 but by the hours of contract or in any other way according to the indications that have been provided by those who pay the contribution.
To resume the above detailed activity and costs, Table 2 can shortly explain:

Table 2. Costs per type of employee

Category	Characters	Effort	Total Costs/year
Trainees	Director of the Epidemiology Unity	2 hours/monthly	€999,12
	Registry Operators	2 hours/weekly for the first month; after: 2 hours/monthly	€631,80 each
	Technical Staff	2 hours/bimonthly	€504,72 each

Trainer	IT Manager	2 hours/monthly	€838,08

2.1.2 DANAOS: Shipping Training Pilot

Cyber Security is a new perception in Shipping industry. Protection from sources that put in jeopardy maritime operation is defined and regulated by respective statutory framework. IMO (MSC/FAL.1/Circ.3 - Guidelines On Maritime Cyber Risk Management (ISO, 2015)) stresses the importance of "building a fence" against cyber threats. It becomes mandatory for the shipping entity to ensure that cyber risks are appropriately addressed in safety management systems, no later than the first annual verification of the company's Document of Compliance after 1 January 2021. Training and awareness is the key supporting element to an effective approach to cyber safety and security and should be tailored to the appropriate levels for on-board personnel including the master, officers and crew along with shoreside personnel, who support the management and operation of the ship. DANAOS constitutes a best-fit case to demonstrate how a modern shipping company is managing training needs for both mariners and shore personnel as well as to draft an estimation of budget allocated to training purposes.

DANAOS Assessment and maritime training centre (DATC) was established in 2016 by DANAOS Shipping Co. Ltd. in order to cover the newly arising training needs of the fleet's officers, crew and shore staff employees. The DATC accommodates an on-premise installation, housed at DANAOS Piraeus office in Greece, comprising of the full mission bridge simulator and state-of-the-art training facilities. An integral part of the DATC training curriculum is company's Safety Management System (SMS) as well as feedback and lessons learnt from actual operational fleet experience. DANAOS objective, as any other modern shipping company nowadays, is to provide tailor made in-house training services complying with statutory requirements combining high-technology training means with experienced, qualified, skilled and fully dedicated instructors.

DATC has invested in the requisition of best of breed interactive and customized to company training needs simulators by VSTEP (VSTEP Simulation, 2019) incorporating virtual reality and serious gaming techniques in structuring and performing training activities. Technical infrastructure consists of a NAUTIS full mission Bridge simulator (VSTEP Simulation/ NAUTIS, 2019) and one desktop bridge simulator which are fully compliant with DNV-GL class , a FMBS specification which was based on STCW 1978 including the 2010 Manila amendments (IMO, 2019) , plus an incident Command Simulator (VSTEP RESCUE SIM (VSTEP Simulation/ RescueSim, 2019)) based on shipboard incident management module with unlimited incidents taking place on-board the ships including: Damage Stability, firefighting, evacuation procedures, Flooding, Oil pollution, Hazard Emergencies Handling and many more.

In DATC facilities, DANAOS Shipping conducts regularly seminars and training courses for its crew and employees customized to each personnel skills, experience and responsibilities. During training sessions, seagoing personnel combine theoretical knowledge and practical training enhancing skills and competence by triggering real scenarios as simulating exercises. DATC has been certified and accredited by Lloyd's Register of Shipping and the DMS (Cyprus Government Department of Merchant Shipping) with approved training provider certificate along with ISO 9001:2015 standard certification (ISO/ ISO9001, 2015). Training syllabus and scheduling is shared to trainees by the beginning of each year while courses are mandatory for all staff. Time plan for sessions is flexible and is aligned with the availability of crew on-board. A Key performance indicator of 20 sessions per year has been set as benchmark. In average 1-2 sessions are organized per week accommodating all training needs and be attained both from crew and shore personnel originated from all countries and

recruited by all offices across the company's global network. On top of that, more than 200 courses are conducted yearly for new personnel and junior staff for familiarization with company's procedures and policies. Cost wise training activity in DANAOS reflects mostly expenses related to operation and organization (allowance/expenses coverage for external attendees, consumables, training material, etc.) plus maintenance of simulators and equipment following service level agreement (SLA) with the third-party technology providers. Instructors are mostly associated with the company's personnel considering compensation as part of their standard salary however in some cases external parties are invited for specialized training imposing an extra cost ($/h). Overall training cost is estimated to around 100k Euros per year.

In this context, DANAOS will exploit over the THREAT-ARREST platform so to incorporate cyber security courses to the company's training framework capitalizing on existing infrastructure and training curriculum, thus, not adding significant cost to training budget. IT administrator and company's security officer (CSO) will be assigned with the role of the instructor while attendees should come from all departments and specialties since cyber threat is a common consideration for all personnel. Scope of the company is to explore the possibility to integrate THREAT-ARREST platform with bridge and incident command simulators structuring and offering multi-scale combined training scenarios performed in a relevant to the ship environment. DANAOS is addressing the need for a web-enabled THREAT-ARREST platform allowing synchronous or asynchronous remote access from a single user or multi-users (at the same time), thus, avoiding expenses related to the physical presence of external attendees to the company's main training facility.

2.1.3 Smart Energy

Adequate cybersecurity is becoming increasingly more important in Internet of Things (IoT) deployments. Recent cases of compromised IoT devices show the damage that can occur when for example multiple IoT devices are exploited to launch Distributed Denial of Service (DDos) attacks against online services (Kolias, et al., 2017).

IoT devices are increasingly being targeted by malware, like Mirai (Kolias, et al., 2017). The virus exploits the lack of security usually shipped with IoT devices, which generally contain default passwords, by using a brute force attack (Whitman & Mattord, 2011) and trying a short list of the most common passwords. Once access is gained, the device is added/reported to a bot network which can be controlled by a malicious actor on demand and instructed to attack a particular target.

A recent security report described coin mining as "a modern gold rush" (Corpin, G.C.M. et al., 2018) and with it there has been a rise in exploits that target IoT devices as mining in volume over CPU speed is becoming more popular (Mundo Alguacil, A. et al., 2018). This type of attack on IoT devices can be easily exploited because such devices ship with default credentials that are not changed (Yousuf, et al., 2015) and go unnoticed since such devices in general do not run any malware detection. Coin mining exploits had a particularly big impact on the IoT sector with threats increasing dramatically throughout 2018 (Mundo Alguacil, A. et al., 2018).

The examples above are just two of the scenarios for which a company like Lightsource Labs needs to prepare when deploying IoT enabled products. Employees need to be trained in order to be made aware of such possible threats and equipped with knowledge on how to identify and deal with them appropriately. Without proper training not only can these treats go unnoticed, but employees can become unknowingly negligent and leave systems exposed which may lead to a significant reputational and financial loss for the company.

Currently, we have identified people in three different roles whom would require training:

1. Technicians – responsible for on-site system installations and site visits.
2. Administrators – responsible for day-to-day maintenance of the backend infrastructure and remotely diagnosing installations deployed in the field.
3. Security auditors – responsible for backend infrastructure and edge IoT gateway security.

When it comes to dealing with cybersecurity issues, from the three different roles, technicians are the ones with the least amount of security expertise. But on a day-to-day basis, administrators are the most exposed to threats and the ones most likely to make mistakes since they have privileged access and therefore can cause the most exposure if not trained to handle threats correctly. In contrast, security auditors are considered to have the highest awareness in dealing with cybersecurity threats. The expectation is that individuals in an administrator role will require more hours of training with the THREAT-ARREST platform.
As a result, the expected training hours required per individual per role breaks down as follows:

- Technician
  - 4 hours per week for the first 2 weeks (crash course).
  - 2 hours every 2 months (refresher) or as needed (new product).
- Administrator
  - 2 hours monthly on cyber system security assurance training.
  - 4 hours monthly on cyber-defence, threats and attacks training.
- Security auditor
  - 1 hours monthly on cyber system security assurance training.
  - 2 hours monthly on cyber-defence, threats and attacks training.

Every training exercise requires some input from a trainer. The role of a trainer will be assigned to our most experienced security auditor and will be covered under his/her normal contractual hours. Among other tasks, a trainer needs to assign different training scenarios to individuals, participate as an attacker, evaluating results and scheduling training sessions. With that in mind, a trainer is allocated 5 hours a month toward organising training needs.
Although Lightsource Labs is an Irish based company, its staff and particularly its technicians operate in countries around the globe, therefore, the cost below is an average hourly cost and can vary dramatically from country to country and employment status (full time, part-time, contract).
With all the above taken into consideration, we estimate that the cost per person per role per year breaks down as show in Table 3:

Table 3. LSE - Costs per type of employee

Role	Average hourly rate	Monthly hours	Total Cost / 1 year
Technician	€30	1	€ 600 / each
Administrator	€30	6	€ 2160 / each
Security auditor	€35	3	€ 1260 / each
Trainer	€40	5	€ 2400 / each

2.1.4 Training and Compliance

In a study conducted in 2018, Shred-it, an American information security company, found that employee negligence is the main cause of data breaches. More precisely, the study report shows that 47 percent of business leaders said human error, such as accidental loss of a device or document by an employee, had caused a data breach at their organization (Shred-it, 2019).
Furthermore, IBM, a multinational information technology company, calculated in its "*2019 Cost of a Data Breach Report*" that an average total cost of a data breach amounts to no less than 3.92 million USD (IBM, 2019).
Although the precise cost of an information security incident will depend on numerous factors, the following three major risks help explain why the cost of information security incidents can potentially be so high:

- Regulatory fines for non-compliance with information security obligations continue to rise. An important example in that regard are the fines supervisory authorities can impose for non-compliance with the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"). Depending on which provisions of the GDPR are infringed, administrative fines of up to 10 to 20,000,000 EUR or in the case of undertakings, up to 2% to 4% of global turnover, whichever is higher, can be imposed.
- Organisations can be held to indemnify the victims of the information security incident.
- Information security incidents can cause organisations to suffer considerable brand and reputational damage and, as the case may be, damage related to business interruption.

As a result, it does not come as a surprise that over the course of the last few years, information security has become increasingly important to organisations. Despite the prevalence of technical security measures, individual employees remain the first line - and frequently the weakest link - in organisational defences. Human beings are indeed prone to forget, lose concentration or disregard security policies and procedures. And if that happens, the organisation as a whole can be at risk.
In order to avoid these risks to materialise, training on information security and breach-related obligations is a necessity for any organisation. If employees are properly informed as to what to watch out for, how to prevent, remediate and mitigate incidents, this alone could prevent a lot of potential problems that could affect the infrastructure and the organisation as a whole.
It follows from the foregoing, taking into account what could be at stake, that many organisations will voluntarily provide training on information security and breach-related obligations to their employees. However, in many cases, there will also be compliance reasons for providing such training in the sense that an obligation to provide such training will directly or indirectly follow from a (non-)statutory requirement.
More precisely, some (non-)statutory requirements expressly and explicitly require that training is provided. Other information security and breach-related requirements do not explicitly require training but could only reasonably be met in case the necessary training is provided.
In the section below, some of the most significant (non-)statutory requirements will be discussed. Given that this would exceed the scope of this contribution, (non-)statutory Member State requirements shall not be addressed.
Subsequently, on the basis of one of the scenarios described in the deliverable D3.3, an example of the necessity to provide employees training on information security and breach-related obligations will be provided in subsection 0 of this Deliverable.

(Non-)Statutory requirements to provide employees information security training

In this section, a distinction will be made between statutory requirements (pursuant to the GDPR and the NIS Directive, see paragraph 0) and non-statutory requirements (more

precisely arising from certification, guidance, insurance schemes, contracts and internal policies, see paragraph 0).

Statutory requirements

GDPR

The GDPR is applicable to the processing of personal data. Within the organisations to which the GDPR will very often be applicable, that processing of personal data will in many cases be carried out by employees, or at least they will often play an important part in it. This inevitably brings up the question whether the GDPR actually obliges organisations to provide information security training to their employees.

It might come as a surprise that the GDPR does not contain an explicit general obligation to controllers to provide training to employees with regard to data protection. However, for organisations it will be difficult, if not impossible, to comply with the GDPR in case employees are not acquainted with the obligations the GDPR imposes and are unaware of what exactly is expected of them.

Indeed, the GDPR contains several open provisions which do not explicitly require controllers and processors to provide their employees information security training, but which would be difficult to be complied with in case no adequate training is given.

More precisely, one of the most challenging requirements in the GDPR is for controllers and processors to be able to demonstrate that personal data is processed in accordance with the principles of lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation, and integrity and confidentiality (security) ((General Data Protection Regulation, 2016), art 5(2)). This is called the 'accountability principle'.

Furthermore, in order to be able to demonstrate compliance with the GDPR as a whole, including the aforementioned principles, controllers and processors are required to take the necessary technical and organisational measures ((General Data Protection Regulation, 2016), art. 24(1)). In addition, the GDPR also requires controllers and processors to take appropriate technical and organisational measures which ensure a level of security appropriate to the risk ((General Data Protection Regulation, 2016), art. 32(1)). The GDPR leaves it to the controllers and processors themselves to decide which technical and organisational measures they consider to be appropriate.

The question can be raised how an organisation could possibly meet the abovementioned obligations without providing a certain degree of training to its employees in relation to information security and breach-related obligations.

It can therefore be advocated that the obligation to provide such training can implicitly be derived from, among others, the following provisions of the GDPR (see Table 4), which were already briefly mentioned above.

Table 4. Training obligations deriving from the GDPR

GDPR Provision	Controller/Processor requirement	Comment
Article 5(1) and (2)	To demonstrate that processing is performed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.	Demonstrating that employees were given training on information security, could be one of the manners by which a controller or processor can demonstrate that the processing is performed in a manner that ensures appropriate security of personal data.

Article 24(1)	To implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR.	Providing information security training to employees could be an organisational measure allowing controllers and processors to demonstrate that the processing of personal data is performed in accordance with the GDPR.
Article 32(1)	To implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.	Providing information security training to employees could be an organisational measure which could ensure a level of security appropriate to the risk.

In addition to the abovementioned general principles on the basis of which trainings would be required, some scarce explicit training requirements exist in the field of EU data protection, and in particular:

- Pursuant to Article 39 GDPR, among the tasks of the Data Protection Officer (DPO) the GDPR lists "awareness-raising and training of staff involved in the processing operations."
- Pursuant to Article 47, para. 2(n) GDPR, in relation to the international data transfers based on Binding Corporate Rules (BCRs), the GDPR requires the BCRs to specify "the appropriate data protection training to personnel having permanent or regular access to personal data."
- In the context of international data transfers to the United States to an organisation that commits to comply with the US-EU Privacy Shield Framework, such organisation is notably required to indicate that it has in place procedures for training employees in its implementation, and disciplining them for failure to follow it.

Furthermore, specifically in relation to data breaches, the GDPR requires the notification to the supervisory authorities within 72 hours of "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" ((General Data Protection Regulation, 2016), arts 4(12) and 33).
The breach notification obligation under the GDPR evidently only applies in case of a breach of personal data. It is therefore essential to carefully assess, in the event of an incident, the nature of the data exposed. If such assessment shows that no personal data has been affected, in principle no data breach notification is required under the GDPR.

Therefore, appropriate technical and organisational measures, most notably appropriate employee training, should be implemented to be able to detect promptly whether a personal data breach has taken place and to immediately inform the supervisory (data protection) authority and the affected individuals, if needed ((General Data Protection Regulation, 2016), Recital 87). Indeed, in order for the controller or processor to be able to meet these data breach notification obligations imposed by the GDPR, employee training will most likely be indispensable. Employees should for example be trained on what a data breach is, how to recognise one, how to avoid one, what to do in case one occurs, and how to mitigate any further risks.

NIS Directive

The (minimal harmonisation) Network and Information Security Directive (NISD, 2016) (the "**NIS Directive**" or "**NISD**") was adopted on 6 July 2016 to address the increasing challenges in relation to cybersecurity. This EU legislation aims to cultivate a common approach across

the EU to address any socio-economic damage that may be caused by attacks on the network and information systems of operators of essential services and digital service providers.

Taking into account its nature as a Directive, the NIS Directive had to be implemented by the EU Member States into their national laws by May 2018.[1] It is therefore required to carefully consider the national obligations, which may be particularly relevant to a particular organisation, depending on whether it qualifies as an Operator of Essential Services ("**OES**") or a Digital Service Provider ("**DSP**"), and depending on the sector in which it is active.

More specifically, the distinction between OES and DSP is of particular importance and may be summarised in Table 5:

Table 5. Distinction between OES and DSP

Operators of Essential Services (OES)	Digital Service Providers (DSP)
Article 5 of the NIS Directive defines an essential service as "*a service essential for the maintenance of critical societal and/or economic activities depending on network & information systems, an incident to which would have significant disruptive effects on the service provision*." EU Member States had to identify the operators of essential services established on their territory by 9 November 2018 based on several criteria, and notably whether an incident would have significant disruptive effects on the provision of that service. According to the NISD, operators active in the following sectors may be identified in each Member State: • energy, • transport, • banking, • stock exchange, • healthcare, • utilities, or • Digital infrastructure ((NISD, 2016),Annex II).	A digital service is described as "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*" ((NISD, 2016), art. 4(5)).[2] In contrast with the OES, which are identified by each EU Member State, online businesses must self-assess whether they are targeted by the rules of the NIS Directive, and whether they fall within the following three different types of digital services: • online marketplaces, • online search engines, or • cloud computing services ((NISD, 2016), arts 4(17)-(19)).

In line with what is provided under the GDPR, neither the NIS Directive requires Member States to enact legislation which explicitly obliges OES and DSP to provide training to

[1] Some countries are however late in transposing the requirements of the NISD.

[2] A digital service provider without an establishment in the EU but providing services within the EU must appoint a representative. This representative will need to be established in one of the EU Member States where the digital services concerned are offered. In that case, the digital service provider shall be deemed to be under the jurisdiction of the Member State where the representative is established (NIS Directive, art 18(2)). Micro and small enterprises (as defined in Commission Recommendation 2003/361/EC) do not fall under the scope of the Directive.

employees on information security and breach-related obligations. Instead, it requires OES and DSP to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations ((NISD, 2016), arts 14, 16).
Further to breach notification requirements, the NIS Directive requires OES to notify the national competent authority or the CSIRT, without undue delay, of incidents having a significant impact on the continuity of the essential services they provide ((NISD, 2016), art. 14(3)). Similarly, DSP are required to notify the national competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a digital service offered within the EU ((NISD, 2016), art. 16(3)).

Indeed, also in the framework of the NIS Directive, the question can be raised whether it is possible at all for any OES and DSP to meet these obligations without providing training to employees on information security and breach-related obligations. As a result, we can conclude that, also pursuant to the NIS Directive, there is an implied obligation to provide such training.

Non-statutory requirements

Certification

Training requirements may also flow, directly or indirectly, from certification or standards.
For instance, in the event organisations would choose to obtain the optional ISO/IEC 27001 information security standard (ISO, 2013), information security awareness is an essential and explicit requirement.
More precisely, Article A.7.2.2 of the ISO/IEC 27001 standard requires that *"all employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function*".
Implementation guidance to this Article states that the organisations in question should develop an education and training programme and furthermore clarifies which specific information security and education aspects should be covered during such training.

Guidance

Training on information security and/or dealing with security incidents may also be recommended in guidance from the authorities or other competent bodies.
For instance, with its "*Handbook on Security of Personal Data Processing*", published in December 2017, the European Union Agency for Cybersecurity ("**ENISA**") (ENISA, 2017), aims to help controllers and processors assess security risks and accordingly adopt security measures for the protection of personal data, as is required by the GDPR.
In this Handbook, ENISA recognises that the lack of information security training can be a risk to the processing of personal data. One of the measures proposed by ENISA to mitigate that risk is therefore to provide training to employees, the level of intensity and content of which will depend on the level of risk (i.e. low, medium or high).
A description of those training measures, per level of risk, is shown in Table 6. below:

Table 6. Description of the training measure

Risk Level	Description of the training measure
Low	The organisation should ensure that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the processing of personal data should also be properly informed about relevant data protection requirements and legal obligations

	through regular awareness campaigns.
Medium	The organisation should have structured and regular training programmes for staff, including specific programmes for the induction (to data protection matters) of newcomers.
High	A training plan with defined goals and objectives should be prepared and executed on an annual basis.

Mindful of the importance of cybersecurity training, ENISA furthermore provides extensive content on how to organise a successful training on cybersecurity, including tutorials for teachers, handouts for students, and virtual images to support hands-on activities in training sessions. Besides providing training material, ENISA organises training courses for and trains around 200 cyber security specialists per year.

Insurance schemes

In many cases, an organisation will seek an insurance to cover its cyber risks. In such context, insurers generally impose the implementation of specific security measures and calculate the insurance premium on the basis of the particularities of the company, including its cyber risk and the implemented measures.

Furthermore, in order for the organisation to be able to claim coverage under its cyber insurance in case an incident would arise, it is important that the organisation has acted in accordance with the cyber insurance policy and/or insurance law. This would inevitably require employees to be made aware and trained on the requirements contained therein.

Contracts

Commercial contracts usually include data protection, security and/or incident-related clauses. In such context, depending on the relationship, the qualities of the parties and the subject-matter of the agreement, a contract may impose more or less detailed security requirements. Employees should obviously be made aware and trained regarding these contractual requirements so as to ensure that the organisation can meet its contractual obligations.

Internal policies

In order to effectively comply with its various information security and breach-related obligations, it is necessary for an organisation to ensure that internal rules (policies, standards, procedures, etc.) are adopted and enforced within the organisation.

Such documents may include detailed security measures, both organisational and technical and could as well include the development of an education and training programme with regard to information security and breach-related obligations. Since *pro forma* internal rules are useless in case they are not followed and implemented, it goes without saying that training of employees with regard to these internal policies is essential.

Example of the necessity to provide employees training on information security and breach-related obligations

The deliverable D3.3 includes the first version of the reference Cyber Training and Threat Preparation (CTTP) models and programmes for the three pilots of THREAT-ARREST. In the framework of the Healthcare programmes definition, the following scenario, named "*EHR Leak – Incident Response*", was described:
"*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."

If such scenario would occur in reality, several of the (non-)statutory security and breach-related requirements discussed in section 0 and 0 could be triggered.

More precisely, however subject to further verification, it appears that this scenario concerns a data breach under the GDPR since the EHRs contain personal data. Moreover, considering the sensitive nature of the personal data involved, this data breach may need to be notified in due time to the supervisory authority as well as to the data subjects themselves pursuant to respectively Articles 33 and 34 of the GDPR. Furthermore, given that the hospital could be considered an OES, this incident may also need to be notified to the national competent authority or the CSIRT pursuant to Article 14 of the NIS Directive in case the incident would have a significant impact on the continuity of the essential services the hospital provides.

Apart from the foregoing, it can be imagined that specific requirements are laid down by national law, healthcare sector guidelines, certification mechanisms, insurance schemes, etc., all of which should be addressed and taken into account in case a security incident or breach occurs.

It goes without saying that this requires not only a thorough analysis of the existing (non-)statutory requirements but also the development and implementation of different policies and procedures for employees to be followed, allowing the hospital to be compliant in case of an incident. Once these analyses have been carried out and these policies and procedures developed, employees should then be trained on these (non-)statutory information security and breach-related obligations, as well as on these policies and procedures so that they know what they are expected to do in case an incident occurs. Without such training, the relevant policies and procedures will most likely not be followed in case of an incident, meaning the hospital would most likely be in breach of several (non-)statutory requirements.

2.2 Current Offerings Landscape

2.2.1 Cyber Ranges

Various cyber range approaches have been developed and their structure depends on the approach to design features such as flexibility, scalability, isolation, interoperability, effectiveness, access, service-based access, and risk evaluation.

Based on their purpose of utilization, cyber ranges can be classified into different categories, such as military/defence, education, enterprise/commercial etc. (Davis & Magrath, 2013); the subsections below present these categories and some key products in each.

Military, Defence and Intelligence

Military organizations and government agencies require high security to counter cyber terrorism. Since any kind of weakness or vulnerability is critical to the nation's infrastructure, the Military and Defence implement large-scale cyber ranges, like the Defence Advanced Research Projects Agency (DARPA)'s National Cyber Range (NCR) (National Cyber Range, 2015). NCR development and operation have been funded by the U.S. Department of Defence since 2009 and the targeted user group are U.S. governmental organizations. The NCR enables operational networks to be represented, and interconnected with military command and control systems, with the ability to restore and repeat tests with different variables. NCR uses the military facility to emulate military and adversary networks for the purposes of realistic cyberspace security testing, which was DARPA's primary aim; to replicate large networks for Department of Defence (DOD) weapon systems and operations.

U.S. Army Communications Electronics Command (CECOM) also proposed a cyber range that is capable of developing configurations for supporting multiple environments through the cyber range. It has also been observed to incorporate features, like Cyber Threat characterization and dynamic threat capability (Solivan, 2015).

Education

Certain cloud-based cyber ranges boost the number of trained cyber professionals to offer defensive trainings, mainly to students, so as to be able to impersonate network administrators and study simulated attacks.

The Michigan Cyber Range (MCR) is an example of this type of cyber range that combines teaching, testing and training. It is an unclassified private cloud operated by Merit, a non-profit organization governed by Michigan's public universities in the USA (Community, n.d.). The MCR has offered several services in cyber security education, testing and research since 2012. The MCR Secure Sandbox simulates a real-world network environment with virtual machines that act as web servers, mail servers, and other types of hosts. Users can add preconfigured virtual machines or build their own ones. Access to the Sandbox is provided through a web browser or a VMware client from any location. Alphaville is MCR's virtual training environment specifically designed to test teams' cyber security skills. Alphaville consists of information systems and networks that are found in a typical information ecosystem. Learners can develop and exercise their skills in various hands-on formats, such as defence and offense exercises.

Another cyber range for education is the DETER/DeterLab (Mirkovic, et al., 2010). This project started in 2004 with the goal of advancing cyber security research and education. DETER operates the DeterLab, which is an open facility funded by U.S. sponsors and hosted by the University of Southern California and University of California, Berkeley. It provides hundreds of general-purpose computers and several specialized hosts (e. g., FPGA-based reconfigurable hardware elements) interconnected by a dynamically reconfigurable network. The testbed can be accessed from any machine that runs a web browser and has an SSH client. DETER is based on the Emulab software (Emulab.net, 2019) and has been used is several projects, such as in an integrated experiment management and control environment called SEER (Schwab, et al., 2007), with a set of traffic generators and monitoring tools. It also provides the ability to run a small set of risky experiments in a tightly controlled environment that maximizes research utility and minimizes risk (Wroclawski, et al., 2008). Furthermore, it provides the ability to run large-scale experiments through a federation with other testbeds that run Emulab software, and with facilities that utilize other classes of control software (Faber & Wroclawski, 2009). Lessons learned through the first eight years of operating DETER and an outline of further work is summarized in (Benzel, 2011). The Emulab/Netbed (White, et al., 2002) that is used by DETER is a cluster testbed providing basic functionality for deploying virtual appliances, configuring flexible network topologies and the emulation of various network characteristics. Emulab allocates computing resources for the specified network and instantiates it in a dedicated HW infrastructure. It has been developed since 2000 and there are currently about 30 of its instances or derivatives in use or under construction worldwide (Testbed, 2019). It can be considered to be a prototype of an emulation testbed for research into networking and distributed systems. It provides accurate repeatable results in experiments with moderate network load (Siaterlis, et al., 2013).

EDURange (Weiss, et al., 2017) is a cloud-based framework for designing and instantiating interactive cyber security exercises funded by the U.S. National Science Foundation and developed by Evergreen State College, Olympia, Washington. EDURange is intended for teaching ethical hacking and cyber security analysis skills to undergraduate students. It is an open-source software with a web frontend based on Ruby and backend deploying virtual machines and networks hosted at Amazon Web Services. The exercises are defined by a

YAML-based Scenario Description Language and can be instantiated by the instructor for a selected group of students. EDURange supports Linux machines which can be accessed via SSH. It also has built-in analytics for host-based actions, namely a history of commands executed by students during the exercise.

Enterprise and Commercial

A cyber defence centre is effective if people can operate it and defend enterprises. Enterprises and commercial organizations deploy different cyber ranges to develop games and simulation environments, in order to strengthen cyber security capabilities. These commercial organizations need a superior way to develop ranges so that they are comparable with the rapid growing applications, threats and traffic volumes. The IBM X Force Command Centre is the first ever commercial cyber simulator and uses live malware to test security. It is mainly being used to help companies train their teams on techniques to respond to attacks while simulating real-world conditions of how hackers operate and key strategies to protect business brand and resources (X-Force Command Cyber Tactical Operations Center, 2019).

The Pinecone Cyber range (Pinecone Cyber, n.d.) is another example of a Commercial cyber range that help users harden their defences and train and certify their IT professionals as cyber warriors. Pinecone Cyber provides the ability to create an environment that precisely mirrors the Global Information Grid (GIG); to enable sophisticated simulation of real-world cyber conditions; to optimize and harden the resiliency of next-generation deep packet inspection (DPI) devices, so as to carry out effective lawful intercept programs and related missions; to model and research advanced cyber threats; and to establish centralized command and control to monitor and manage a distributed network of remote cyber ranges.

Another cyber range of this type is the one developed by Cisco that helps users to build skills and experience to handle different cyber incidents. It uses real-world conditions and advanced tools and techniques to mitigate cyber-attacks in a synthetic war gaming environment. This cyber range has four components: i) operations based models to respond to threat scenarios, ii) platform based security tools, iii) simulations for real applications, continuous updating and upgradation, and iv) a cloud hosted environment (Test resource Management Center, 2019). The infrastructure supports wired, wireless and remote access along with a client simulator, a server simulator and an application simulator (Gürtler, 2012). It utilizes five hundred malware samples, ransomware and attack cases to develop more realistic cyber-attack scenarios to be used.

Service Providers

The Cyberbit cyber range is one of the world's leading provider of cybersecurity training. It provides a unified, product suite for threat detection, incident response, and simulated training, across IT and IoT. It creates new business lines by setting up cybersecurity training and simulation centres, in order to ensure advanced training and testing services (Cyberbit, 2016).

SimSpace Cyber Range (Rossey, 2015) is another cyber range of this type, run by a U.S. private company, which enables the realistic presentation of networks, infrastructure, tools and threats. It is offered as a service hosted in public clouds (i.e. Amazon Web Services or Google), at the SimSpace datacentre, or deployed in the customer's infrastructure and premises. The cyber range provides several types of preconfigured networks containing from 15 to 280 hosts, which emulate various environments (generic, military, financial). It is possible to generate traffic emulating enterprise users with host-based agents and run attack scenarios automatically by combining various attacker tasks. All activities can be also monitored at network and scenario level (network traffic, attackers' and defenders' actions, and activities of emulated users at end hosts). The platform is controlled via a web portal that also provides access to the results of an analysis and assessment of monitored activities within the cyber range.

Open Source

Security professionals need practical real-world experience. However, performing dangerous activities on production, personal or work networks may have serious consequences. The Arizona Cyber Warfare Range (Arizona Cyber Warfare Range, n.d.) is a safe environment for learning, hacking, testing, war games, malware practices and real opponent challenges. The range also provides free, Internet accessible and safe environment for novices and experts to test their skills and conduct security practices.

Another cyber range framework is the iCTF (IS Decisions, 2019) that was developed by the University of California, Santa Barbara. The goal of this open-source framework is to provide customizable competitions. The framework creates several virtual machines running vulnerable programs that are accessible over the network. The players' task is to keep these programs functional at all times and patch them so other teams cannot take advantage of the incorporated vulnerabilities. The availability and functionality of these services is constantly tested by a scorebot. Each service contains a flag, a unique string that the competing teams have to steal so that they can demonstrate the successful exploitation of a service. This flag is also updated from time to time by the scorebot.

InCTF (Raj, et al., 2016) is a modification of iCTF that uses Docker containers instead of virtual machines. This enhances the overall game experience and simplifies the organization of attack defence competitions for a larger number of participants. However, it is not possible to monitor network traffic, capture exploits and reverse engineer them to identify new vulnerabilities used in the competition.

Law Enforcement

According to Computer Security Institute (CSI)'s survey, thirty four percent of respondents reported intrusions to law enforcement (De Montfort University Partnered with the Michigan Cyber Security Center (MCC) , 2017). Applications in military and law enforcement are being developed and tested in cyber ranges. This determines their feasibility and effectiveness in practice. The Michigan Cyber Range is one such cyber range. A cyber range environment makes use of a lot of computing devices and every device used increases the vulnerability of a cybercrime. Law enforcement can respond to the resulting cybercrimes. They also ensure technical help with forensics and investigation along with training, victim services and community education (Police Executive Research Forum, 2014).

Other solutions

Locked Shields (Gürtler, 2012) by CCDCOE is the world's largest and most advanced international technical live-fire cyber defence exercise. The setup is based on Blue versus Red team scenarios that include thousands of attacks, a large number of fully virtualized computers, with real-time network and hundreds of participants from all around the globe. This defence exercise has been organised by the NATO Cooperative Cyber Defence Centre of Excellence since 2010, and its main focus is to train for security experts that protect national IT systems.

Cyber Europe (ENISA/ Cyber Europe programme, 2019) is a series of pan-European exercises, held every two years, aimed at testing cybersecurity, business continuity and crisis management capabilities. The security incidents are designed to build up into a crisis at all levels: local, organization, national, European. The exercise is organised for IT security, business continuity and crisis management teams coming from EU and EFTA Member States only and puts the Crisis management procedures of the participants at test. The series of exercises are organised by the European Union Agency for Network and Information Security (ENISA) since 2010.

SANS NetWars (SANS, 2019) is another cyber range that provides hands-on, interactive learning scenarios for information security professionals to help them develop and master real-world, in-depth skills to excel in their field. It currently exists in three different types: i) Core (classic penetration testing), ii) defence, and iii) malware analysis. NetWars main focus is to provide various exercises to help participants learn in a cyber range while working through various challenge levels, in order to master the skills that can be used in their jobs every day.

Another cyber range is KYPO (Vykopal, et al., 2017) that was funded by the Ministry of Interior of the Czech Republic as part of the Security Research Program of the Czech Republic. To be able to create real-world scenarios, KYPO is designed as a modular distributed system and its architecture runs on various computation platforms, such as OpenStack or OpenNebula. This allows it to be flexible and scalable for the creation of the virtual scenarios. The high-level architectural design is based on the following requirements: (i) Flexibility, (ii) Scalability, (iii) Isolation vs. Interoperability, (iv) Cost-effectiveness, (v) Built-In Monitoring, (vi) Easy Access, (vii) Service-Based Access, and (viii) Open Source. With the above requirements, real-world simulated scenarios can be created in a dynamic way. With service-based access, KYPO offers the platform as a service. The platform can provide real-time and historical data for monitoring the overall interoperability of the platform and the individual topologies that the platform can create.

Lightweight Platforms

There are a number of generic testbeds that can be used by cyber range approaches. While some of these evolved from generic testbeds, others were designed based on the cyber security field. The environments are versatile, large-scale infrastructures with state-of-the-art parameters and features, as well as lightweight alternatives with limited scope, functionality and resources. The Australian Department of Defence published an extensive survey of state-of-the-art cyber ranges and testbeds (Davis & Magrath, 2013). The survey lists more than 30 platforms that can be used for cyber security education worldwide. This number is based on publicly available, non-classified information. Below we list some of the lightweight platforms that can be used.

Avatao ((PwC, 2019), (Avatao, 2019)) is an e-learning platform that offers IT security challenges which are created by an open community of security experts and universities. It is developed by an eponymous spin-off company of CrySyS Lab at Budapest University of Technology and Economics, Hungary. It is a cloud-based platform using lightweight containers (such as Docker) instead of a full virtualization. Learners and teachers access these challenges via web browser. Hosts and services within the virtual environment are accessed by common network tools and protocols such as Telnet or SSH.

CTF365 (CFTP, 2019) is a Romanian commercial security training platform with a focus on security professionals, system administrators and web developers. It is an IaaS where users (organized in teams) can build their own hosts and mimic the real Internet. CTF365 provides a web interface for team management, instantiating virtual machines using predefined images and providing credential to access the machines using VPN and SSH. Each team has to defend and attack the virtual infrastructure at the same time. As a defender, a team has to set up a host which runs common Internet services such as mail, web, DB in 24/7 mode. As an attacker, the team has to discover their competitor's vulnerabilities and submit them to the scoring system of the CTF365 portal.

A comparison of some characteristics of the cyber range solutions presented in this section is presented in the Table 7.

Table 7. Cyber Range Comparison

Cyber Ranges	Characteristics

		Evidence Gathering	Evidence Sharing	Analysis	Infrastructure	Application	External CR
Military, Defence and Intelligence	NCR (National Cyber Range, 2015)	N	N	N	N	N	N
	CECOM (Solivan, 2015)	-	-	-	Y	Y	N
Education	MCR (Community, n.d.)	-	-	-	Y	Y	Y
	DETER/Deter Lab (Mirkovic, et al., 2010)	-	-	-	Y	Y	Y
	EDURange (Weiss, et al., 2017)	Y	-	Y	Y	Y	Y
Enterprise and Commercial	Pinecone (Pinecone Cyber, n.d.)	Y	-	-	Y	Y	-
	Cisco (Test resource Management Center, 2019)	Y	Y	Y	Y	N	N
Service Providers	Cyberbit (Cyberbit, 2016)	N	Y	Y	Y	Y	N
	SimSpace (Rossey, 2015)	Y	Y	Y	Y	Y	N
Open Source	Arizona Cyber Warfare Range (Arizona Cyber Warfare Range, n.d.)	-	-	-	Y	N	N
	iCTF (IS Decisions, 2019)	Y	N	N	Y	N	N
	InCTF (Raj, et al., 2016)	Y	N	N	Y	N	N
Law Enforcement	MCC (De Montfort University Partnered with the Michigan Cyber Security Center (MCC), 2017)	Y	Y	N	Y	N	N
Other Solutions	Locked Shields (Gürtler, 2012)	Y	N	Y	Y	N	N
	Cyber Europe (ENISA/ Cyber Europe programme, 2019)	Y	N	N	Y	N	N
	NetWars (SANS, 2019)	-	-	-	Y	N	N

	KYPO (Vykopal, et al., 2017)	N	N	N	Y	N	N
	Avatao (Avatao, 2019)	-	-	-	Y	Y	N
	CTF365 (CFTP, 2019)	-	-	-	Y	Y	N

2.2.2 Serious Games

Free games

The Weakest Link (IS Decisions, 2019) by IS Decisions is a quiz game with the topic of information security awareness and social engineering. It is implemented as a single player online game. During a game, the player is confronted with different security awareness and social engineering scenarios. The player has to select the correct behaviour that prevents a harmful or potential risky outcome of the scenario. The game addresses players without a professional background in information security. Like "The Weakest Link", the serious online game AWARENESS QUEST (see (Beckers, Kristian et. al, 2019), Section 2.2) that will be provided by the THREAT-ARREST platform represents a quiz game. In contrast to The Weakest Link that is a single player game, AWARNESS QUEST will provide several additionally game modes for two players. In these modes two players can play against in each other in different ways. For example, in one of the modes players can challenge each other by selecting questions for the opponent. Compared to The Weakest Link that provides a fixed set of question, AWARNESS QUEST will provide an expandability of the set of questions. In this context, a content management process will be designed that enables the continuous extension of the question set by the continuous consideration of current real-world attacks. Another benefit of AWARENESS QUEST is that its question set can be adjusted to training scenarios for specific target groups (e.g. a certain sector of industry).

The Fugle (Trend Micro, 2019) by Trend Micro is a single player online game. It addresses decision-makers in the field of information security. The game is implemented as an interactive movie. In this movie the player takes the role of the CIO of a global organization who is in charge for the introduction of a new product. The movie is divided into serval sequences. After every sequence, the player is confronted with potential information security issues or information security incidences regarding the new product. The player chooses a strategic action out of a set of actions as a response. Here, each action costs a different amount of money that is withdrawn from the total budget of the player. The following content of the movie depends on which action has been chosen before. The Fugle addresses primary executives in the area of information security. Its learning content focuses on management decisions regarding to information security issues. In contrast to that, the THREAT-ARREST gaming tools AWARENESS QUEST and PROTECT (see (Beckers, Kristian et. al, 2019), Section 2.3) will address the theme of social engineering. In this connection, the standard learning content of these gaming tools will consider social engineering in general, without addressing a particular type of employee. Because the learning content of the gaming tools will be adaptable, it will be also possible to use the gaming tools within training programmes that are designed for specific types of employees (e.g. administrators, reception staff, management personnel, etc.).

Cyber City (Cyber Security Challenge UK, 2019) is a single player game that is provided by the Cyber Security Challenge UK. The game realizes an old-fashioned videogame in form of a point and click adventure. During the game, the player is confronted with different information security issues, like firewall routing, social engineering attacks and law aspects, which he/she has to solve. A limited demo version of the game is implemented as an online game. The full version is only available as a desktop only application. The game addresses

people without a professional information security background. Compared to Cyber City that considers social engineering only partly, the THREAT-ARREST gaming tools AWARNESS QUEST and PROTECT will provide a broad learning content for social engineering. Additionally, the learning content of the gaming tools will be expandable and adjustable. Because Cyber City is implemented as a videogame, for the solution of some exercises a gaming background of the player would be helpful. In comparison, AWARNESS QUEST and PROTECT will be designed for players that have not necessarily a gaming background. In contrast to the full version of Cyber City, AWARENESS QUEST and PROTECT will be implemented as online games.

Elevator (SURF, 2019) is a casual, cooperative and turn based mobile videogame. It is provided by SURF which is the collaborative organisation for ICT in Dutch education and research. ELEVATOR addresses several information securities themes, like (i) fishing, (ii) social media, (iii) passwords and usernames, (iv) secure information exchange, (v) hacking, and more. The game is played by two players who depend on each other. They take the roles of secret agents who shall exploit the information security weaknesses of virtual companies to reach the elevator in each level. In this connection, a player can either choose the role of a hacker or a social engineer. The game addresses people without a professional background in information security. By playing the game, the players shall get an understanding how attackers are acting. For playing the game a formal registration/authorization is necessary. Because Elevator is implemented as a videogame, it would be helpful if the players have any gaming background. In comparison, the THREAT-ARREST gaming tools AWARNESS QUEST and PROTECT are designed for players without any gaming background. Additionally, the gaming tools will provide the ability to extend and adjust its learning content.

The Dogana cards game (Thales, 2018) has been developed by Thales in the context of the research project Dogana (Dogana Project, 2019). It is an educational tabletop board game that can be played by 2 to 6 players who play against each other. In the game, the players take the role of hackers who perform the same mission. The objective of a mission is the compromising of a target system by performing two attacks. The player who accomplishes the mission first wins the game. In a round of the physical card game HATCH (see (Beckers, Kristian et. al, 2019), Section 2.1) that will be provided by THREAT-ARREST every player takes also the role of the attacker at a certain time, whereby the attack of every player is rated by the other players. In contrast to Dogana, every player creates his / her individual attack based on the cards he / she has drawn. Because of the possible combination of cards, the attacks vary from round to round. The learning effect is achieved, because the players deal intensively with the theme of social engineering during the design of their attacks and the discussions in that the players rate the attack of the current attacker.

The Dogana research project also provides also the videogame Phishing Wars (AIT Austrian Institute of Technology GmbH, 2019) that addresses the social engineering attack phishing. Currently, the game can be played for test purposes in the context of a study. Compared to Phishing Wars that considers only one aspect of social engineering in the form of phishing emails, the THREAT-ARREST gaming tools AWARNESS QUEST and PROTECT will provide a broad learning content for social engineering.

Commercial Games

Game of Threats™ (PwC, 2015) by PwC is a head-to-head digital game that simulates the experience of executives in case their company is targeted by a cyber-attack. During the game, participants play both the attackers´ and the defenders´ side, working against a clock and with limited resources in a race to beat their opponents. Its scope is to challenge participants to make quick, high-impact decisions and help them understand the activities that can make the biggest difference and provides valuable insight into emerging cyber threats. In

contrast to Game of Threats™ that considers social engineering only partly, the THREAT-ARREST gaming tools AWARENESS QUEST and PROTECT will provide a broad learning content for the theme of social engineering. Compared to Game of Threats™, the gaming tools will be playable by single players. Additionally, the THREAT-ARREST gaming tools will enable the extension and adjustment of the learning content for specific training scenarios.

The Information security game INFOSEC (XLPro Training Solutions, 2019) by XLPro Training Solutions is an online game that addresses the themes of information security awareness and social engineering. It implements the find-the-error game approach. In this context, the player is shown two different pictures, where one picture always contains violations against information security awareness or indications for social engineering attacks. The other picture represents always the correct behaviour or correct content respectively. For example, one picture shows a phishing mail, while the other picture shows a corresponding mail with the correct content. Depending on the task, the player has to find the erroneous or correct content respectively. The first three levels of the game can be played freely. INFOSEC addresses people without a professional background in information security. Compared to INFOSEC that considers social engineering only partly, the THREAT-ARREST gaming tools AWARNESS QUEST and PROTECT will provide a broad learning content for social engineering.

Match (ERMProtect/ Match, 2019) by ERMProtect is a single player online game in which the player is confronted with several scenarios regarding information security awareness. For each scenario the player has to select the correct behaviour(s) and/or information security countermeasure(s). The game addresses the topics of (i) email security, (ii) smartphone security, (iii) ransomware, (iv) clean desk, and (v) GDPR. Between the solving of scenarios, the player can earn extra points by playing a virtual board game, in which he/she has to create identical combinations of three or more icons to get points. The matching icons disappear from the board and are replaced by new icons. Some icons cause special actions. Match addresses people without a professional background in information security. In contrast to Match that considers primary security awareness aspects that do not include social engineering, the THREAT-ARREST quiz tool AWARNESS QUEST will provide a broad learning content for social engineering. Additionally, the THREAT-ARREST quiz tool AWARNESS QUEST will enable the extension and adjustment of the learning content for specific training scenarios.

Jump (ERMProtect/ Jump, 2019) by ERMProtect addresses the following topics of information security awareness: (i) password security, (ii) smartphone security, (iii) social media, (iv) home office, and (v) personally identifying information (PII). It is implemented as a single player online game in which the player earns points by jumping to and successfully landing on different types of platforms. At a certain type of platform, the player has to answer questions regarding to information security awareness. For correct answers he/she earns points, gets extra lives and/or special powers. Jump addresses people without a professional background in information security. Compared to Jump that considers primary security awareness aspects that do not include social engineering, the THREAT-ARREST quiz tool AWARNESS QUEST will provide a broad learning content for social engineering.

Trivia (ERMProtect/ Trivia, 2019) by ERMProtect is a quiz game regarding to information security awareness. It is implemented as an online game that can be played by a single player or multiple players. Trivia includes the topics (i) insider threat, (ii) physical security, (iii) security on the move, and (iv) web browser. Trivia addresses people without a professional background in information security.

Recall (ERMProject/ Recall, 2019) by ERMProtect is an online game that addresses different topics from the field of social engineering. During the game, *players view an image or video and are then asked one or more questions that relates to what they just saw*. Recall addresses

people without a professional background in information security. Compared to Recall, the THREAT-ARREST quiz tool AWARNESS QUEST will enable the extension and adjustment of the learning content for specific training scenarios.

CIRCADENCE provides the security awareness platform inCyt (CIRCADENCE, 2019) that is mobile accessible. The objective of inCyt is to educate the entire workforce of organizations through concept-driven gameplay reflective of real-world cybersecurity offensive and defensive strategies as well as best practices (cf. (CIRCADENCE, 2019)). The training that is provided by inCyt bases on the guidance in NIST SP 800-16 (NIST, 1998) and NIST SP 800-50 (NIST, 2003) (cf. (CIRCADENCE/ Circadence Wins Silver Award for inCyt from International Serious Play Awards Competition, 2019)) . Additionally, it is informed by the latest threat vectors and cyber security trends (CIRCADENCE/ Circadence Wins Silver Award for inCyt from International Serious Play Awards Competition, 2019). The provided online games are multi-player games. CIRCADENCE addresses people without a professional background in information security. In the form of PROTECT, the THREAT-ARREST platform also provides a single-player game. In contrast to inCyt that considers social engineering only partly, the THREAT-ARREST gaming tools AWARNESS QUEST and PROTECT provide a broad learning content for the theme of social engineering. Compared to inCyt, the THREAT-ARREST gaming tools AWARNESS QUEST and PROTECT will enable the extension and adjustment of the learning content for specific training scenarios.

The Automated Security Awareness Platform (ASAP) (Kaspersky Lab, 2015) by Kaspersky is a training platform for information security awareness. The platform is provided as an online tool that can be processed on computers and mobile devices. ASAP addresses the following topics: (i) email, (ii) web browsing, (iii) passwords, (iv) social networks and messengers, (v) personal computer security, (vi) mobile devices, (v) confidential data, (vi) personal data and GDPR, (vii) social engineering, as well as (viii) security at home and during travel. The platform provides its learning content based on simulation principles showing real life events (cf. (Kaspersky Lab, 2015), p. 5). ASAP sets training objectives and justifies a program in comparison to global benchmarking (cf. (Kaspersky Lab, 2015), p. 2). It also uses automated learning management to adjust the training programs individually for trainees and monitors progress with actionable reporting and analytics (cf. (Kaspersky Lab, 2015), p. 2). The platform addresses people without a professional information security background. In contrast to ASAP, the THREAT-ARREST gaming tools AWARNESS QUEST and PROTECT will enable the extension and adjustment of the learning content regarding to specific training scenarios. Additionally, the THREAT-ARREST platform will provide in the form of AWARENESS QUEST a game with a multi-player mode. Kaspersky Interactive Protection Simulation (KIPS) (Kaspersky Lab, 2018) by Kaspersky is a tabletop game for 4 to 6 players. KIPS addresses business system experts, IT personnel and line managers from enterprises and government departments. The players take the roles of persons responsible for running the business of a fictitious company with the goal to maximize the profit. During the game the company is exposed to cyber security attacks. In this context, the players have to make strategic, managerial and technical decisions in response to already occurred and potential attacks. The English version of the game includes game plans for the following scenarios: (i) corporation, (ii) oil and gas, (iii) power station or water plan, (iv) bank, (v) e-Government, and (vi) transportation. Compared to KIPS that considers different types of cyber security attacks, HATCH focusses on social engineering attacks. In contrast to KIPS where the players react to cyber security attacks, the players of HATCH take also the role of the attacker and planning their own individual attacks based on the cards they have drawn. Because, the players also rate the attack of the current attacker, they also consider social engineering attacks from the view of the attacked.

Finally, Cyber Incident Games (Airbus, 2019) by Airbus are role playing games in which the players take the role of a cyber attacker. A game is played by multiple players. The Cyber

Incident Games reference different IT infrastructures corresponding to various fields of businesses and industries. This includes also a game plan for an industrial production infrastructure. During the game the players receive missions that include each a certain compromising of the IT infrastructure. The players plan appropriate attack scenarios to fulfil the mission. Compared to the Cyber Incident Games that consider cyber security attacks, HATCH focusses on social engineering attacks. In contrast to the Cyber Incident Games where the players only take the roles of attacker, the players of HATCH consider the attacks also from the view of the attacked, because the players rate the attacks of the current attackers.

Summary of comparison for serious games

This section summarizes the results from the subsections 0 and 0. Table 8 represents the comparison of the THREAT-ARREST gaming tools with other tools. The comparison of the physical card game HATCH, which is provided within the THREAT-ARREST project, with other physical serious games is represented in Table 9.

Table 8. Summary of comparison of gaming tools

Feature	TA	WL	TF	CC	EL	PW	IN	MA	JU	TR	RE	IC	AP	GT
Consideration of social engineering	Y	P	N	P	Y	P	P	N	P	Y	Y	P	Y	P
Provision of *single*-player game(s)	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y	N
Provision of *multi*-player game(s)	Y	N	N	N	Y	N	N	N	N	Y	N	Y	N	Y
Extendable and adjustable learning content for specific scenario	Y	N	N	N	N	N	N	Y	Y	Y	Y	N	N	N
Gaming background is *not* necessary	Y	Y	Y	P	P	Y	Y	P	P	Y	Y	Y	Y	Y
Provision as online game	Y	Y	Y	P[3]	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Integration in training platform	Y	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y

{TA= THREAT-ARREST gaming tools, WL= The Weakest Link (IS Decisions, 2019), TF= The Fugle (Trend Micro, 2019), CC= Cyber City (Cyber Security Challenge UK, 2019), EL= Elevator (SURF, 2019), PW= Phishing Wars (AIT Austrian Institute of Technology GmbH, 2019), IN= INFOSEC (XLPro Training Solutions, 2019), MA= Match (ERMProtect/ Match, 2019), JU= Jump (ERMProtect/ Jump, 2019), TR= TRIVIA (ERMProtect/ Trivia, 2019), RE= Recall (ERMProject/ Recall, 2019), IC= inCyt (CIRCADENCE, 2019), AP= Automated Security Awareness Platform (Kaspersky Lab, 2015), GT= Game of Threats (PwC, 2019) | Y= YES, N= NO, P= Partial}

Table 9. Summary of comparison of physical serious games

Feature	TA	DC	KI	CG
Consideration of social engineering	Y	Y	P	P
Multi-player game	Y	Y	Y	Y
Adjustable for specific scenario	Y	N	P	P

[3] Only the limited try-out version is provided as an online game

Feature	TA	DC	KI	CG
Player takes role of attacker	Y	Y	N	Y
Player takes role of attacked/defender	Y	N	Y	N
Attack scenario is composed by player	Y	Y	N	Y

{DC= Dogana card game (Thales, 2018), KI= Kaspersky Interactive Protection Simulation (Kaspersky Lab, 2018), CG= Cyber Incident Games (Airbus, 2019) | Y= YES, N= NO, P= Partial}

2.3 Future developments, products and services (2021-2026)

2.3.1 The future in the Cybersecurity workforce demand

Cybersecurity jobs are in high demand and it does not seem like the need for more security professionals is going anywhere in the foreseeable future. Cyber-attacks are only becoming more common and more harmful, and even though we tend to only hear about the attacks of high-profile entities, no company – or individual for that matter – with an online presence is immune to attacks.

According to the Bureau of Labour Statistics (Bls.gov, 2019), the rate of growth for jobs in information security is projected at 37% until 2022 – that's much faster than the average for all other occupations. Computer science roles are already in high demand as it is; adding in the element of security makes these roles even more critical and sought after.

The Current State of Cybersecurity Training: With so many jobs available, and the need to fill them so dire, more colleges are offering degrees in cybersecurity, though it has yet to become a staple in undergraduate coursework for students majoring in related fields.

For many professionals currently in the cybersecurity field, they learned the necessary skills through certificate programs and in-the-field training versus degree programs. While degree programs may not be as widespread as they should be for the level of demand for cybersecurity roles, they are in fact increasing.

In 1998, the National Security Agency, in response to the President's National Strategy to Secure Cyberspace, developed the National Centres of Academic Excellence in Information program (Nsa.gov, 2019), which sparked the increase in programs.

On the other hand, jobs that require cybersecurity know-how will usually have a range of titles. The most common titles, according to the SANS Institute Cybersecurity Professional Trends survey (Sans.org, 2019), are Security Analyst, Security Engineer or Architect, Security/IT Director or Manager, CISO/CSO, Systems Administrator, Network Architect or Engineer, Forensics Investigator, Auditor, Systems Engineer or Integrator, among quite a few other roles.

Common skills required for cybersecurity job roles are incident handling and response, audit and compliance, firewall/IDS/IPS skills, intrusion detection, analytics and intelligence, SIEM management, access/identity management, application security development, advanced malware prevention, and cloud computing/virtualization. While these are the most common skills, most cybersecurity roles require a handful of these skills plus others.

Based on the SANS survey, the top five industries for cybersecurity professionals are Banking/Finance/Insurance, Information Technology/Management, Government (Defense), Government (Nondefense), and Consulting/Professional Services. Not surprisingly, these top industries all deal with sensitive information, which is commonly targeted by attackers.

2.3.2 The need for Information Security Officers and for Holistic Training frameworks

Currently, about 65 percent of large U.S. companies have a CISO (Chief Information Security Officer) position, up from 50 percent in 2016, according to ISACA, an independent, non-profit, global association. Cybersecurity Ventures predicts that 100 percent of large companies globally will have a CISO position by 2023: they have to. The cybercrime and related workforce shortage are severe – and organizations need security leadership with a solid or dotted line to the CEO in order to remedy the problem. The cybersecurity workforce shortage has left CISOs (Chief Information Security Officers) and corporate IT security teams shorthanded and scrambling for talent while the cyber-attacks are intensifying (Cybercrime Magazine, 2018).

Corporations are responding by placing some or all their IT security into the hands of third parties. Last year, Microsoft estimated that 75 percent of infrastructure will be under third-party control (i.e., cloud providers or Internet Services Providers) by 2020. The Managed Security Service Providers (MSSPs) are a subset of the third parties, and they focus exclusively on security.

Towards this direction, the need for advanced cyber security training modules is evident. Based on the continuously increasing needs in numerous complementary domains, it is expected that after 2020 the tools and products described in Section 2.2 will need to lead to the deployment of thorough software solutions with complementary functionalities that can address the varying challenges of different domains. The need for modular software solutions capable of providing holistic training to employees of different levels and in different domains will drive the development of such products.

In that context, THREAT-ARREST aims to set the basis towards this direction; it envisions to create a complete training solution addressing the challenges of complementary domains (in terms of cybersecurity vulnerabilities, environments, personnel characteristics, etc.) that will set the grounds for complete training software solutions.

3 Business Plan

It should be stated that Section 3 of the D8.3 deliverable has been planned and documented as a "stand-alone" section. Therefore, its structure and contents are quite analytical and include, among other, a project overview and a "business case" / innovation presentation sub-sections.

3.1 Overview

3.1.1 Purpose of Business Plan

The purpose and scope of the present "Business Plan" section comprise of: (i) a brief presentation of the THREAT-ARREST project and its deliverables and (ii) a presentation of the business case, the project's and final product's / solution's aims, objectives, innovation and market potential. The present Plan is not focusing only to the project implementation period (September 2018-August 2021), but also to the "after project" – "product commercialization" period (2021-2024).

3.1.2 The THREAT-ARREST Project

Project details have been analytically documented in:

- the project proposal document (THREAT-ARREST Consortium, 2017)
- the already submitted deliverables (D8.1 – Stakeholder's engagement plan & online channels development, D8.2 – the THREAT-ARREST dissemination plan and D9.1 – the THREAT-ARREST quality assurance plan).

The project in brief:

- THREAT-ARREST is an H2020 project (topic: DS-07-2017)
- Proposal / Project title: "Cyber Security Threats and Threat Actors Training - Assurance Driven Multi-Layer, end-to-end Simulation and Training"
- Type of Action: "IA" (Innovation Action)
- Duration: 36 months (1.9.2018 – 31.8.2021)
- Total Project Budget: 6.45 mil. €

3.1.3 Consortium / Partners

- FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS (FORTH) (Greece)
- SIMPLAN AG (Germany)
- Sphynx Technology Solutions AG (STS) (Switzerland)
- UNIVERSITA' DEGLI STUDI DI MILANO (UMIL) (Italy)
- ATOS SPAIN SA (Spain)
- IBM ISRAEL - SCIENCE AND TECHNOLOGY LTD (Israel)
- Social Engineering Academy (SEA) GmbH (Germany)
- INFORMATION TECHNOLOGY FOR MARKET LEADERSHIP (ITML) (Greece)
- BIRD & BIRD LLP (UK)
- TECHNISCHE UNIVERSITAET BRAUNSCHWEIG (TUBS) (Germany)
- CZ.NIC, ZSPO (Czech Republic)

- DANAOS SHIPPING COMPANY LIMITED (Cyprus)
- TÜV HELLAS (TÜV NORD) S.A. (Greece)
- Lightsource Labs Limited (Ireland)
- Agenzia Regionale Strategica per la Salute ed il Sociale (ARESS)

3.1.4 Project Main Objectives

Main objectives of the THREAT-ARREST project include:

- developing an advanced cyber range platform incorporating emulation, simulation, serious gaming and visualization capabilities
- delivering security training, based on a model driven approach, where CTTP models, specifying the potential attacks, the security controls of cyber systems against them, and the tools that may be used to assess the effectiveness of these controls, will drive the training process, and align it (where possible) with operational cyber system security assurance mechanisms to ensure the relevance of training.
- delivering a platform that will also support trainee performance evaluation and training programme evaluation and adapt training programmes based on them.
- validating he effectiveness of the framework by using a prototype implementation at TRL-7, interconnected with real cyber systems pilots in the area of smart energy, healthcare, and shipping, and from technical, legal, and business perspectives.

3.1.5 Project Milestones

Table 10 below presents the project milestones along with the relevant work packages and their deadlines.

Table 10. Project Milestones

#	Objective	Work Package	Delivery Date
1	Requirements, initial architecture & dissemination / exploitation plans	WP1, WP8	M6
2	1st version of *THREAT-ARREST* components	WPs 2-5	M12
3	Business models, dissemination & exploitation reports	WP8	M18
4	1st version of Integrated training platform	WP6	M20
5	1st pilot execution and platform's evaluation	WP7	M24
6	Final version of *THREAT-ARREST* components	WPs 2-5	M30
7	Final version of Integrated training platform	WP6	M32
8	2nd pilot execution and final platform's evaluation, final business plan, standardisation, dissemination & exploitation reports	WP7, WP8	M36

3.1.6 Legal & Privacy Matters

In terms of legal and privacy matters of the project:

- all related and applicable European Legislation has & will be taken into consideration / adaptation within the THREAT-ARREST project and any potential market commercialization phases/processes
- issues related to Ethics and Human Participation have been addressed (Deliverable D10.1 – delivered on M7)
- matters related to Privacy/Personal Data Protection have been addressed (Deliverable D10.3 regarding collecting and processing personal data – delivered on M7 - and Deliverable D10.2 – list of Partners' nominated Data Protection Officers – delivered on M1).

3.2 Business Case Presentation

3.2.1 Overall Concept: A state-of-the-art Cyber range Platform, utilizing Model - Driven Emulation, Simulation and Gamification - based Training

THREAT-ARREST will develop an advanced cyber range training platform incorporating (THREAT-ARREST Consortium, 2017):

- *Simulation,*
- *Emulation,*
- *Data Fabrication,*
- *Serious Gaming and*
- *Visualisation Capabilities*

The platform's aim is to adequately train / prepare stakeholders of:

- Various market segments / "industries" and
- with different types of responsibility & levels of expertise

in defending high-risk cyber systems and organizations to counter advanced, known and new cyber-attacks.

The THREAT-ARREST platform's ***unique*** *and* ***innovative proposition*** is that:

- it will deliver security training, based on ***a model-driven approach***, where ***CTTP models***, specifying the potential attacks, the security controls of cyber systems against them, and the tools that may be used to assess the effectiveness of these controls, will drive the training process, and align it (where possible) with operational cyber system security assurance mechanisms to ensure the relevance of training
- it will support ***trainee performance and training programmes evaluation*** and will be able ***adapt the training programmes*** based on these evaluations.

The effectiveness of the platform and overall framework will be validated using a prototype implementation, interconnected with real cyber systems pilots in the areas of:

- ***Smart Energy,***
- ***Healthcare,***
- ***Smart Shipping***

Validation will comprise technical, legal and business perspectives. Following on this, the platform's own security and privacy/personal data protection capabilities will form an integral part of the project ("security & privacy-by-design").

3.2.2 CTTP Models & Platform Tools presentation

CTTP Models & Programmes

A ***CTTP model*** will define the structure and automate the development of a ***CTTP programme*** by determining (THREAT-ARREST Consortium, 2017):

- the components of a cyber-system, their relations and the cyber threats covered by the CTTP programme
- the ways in which these components should be simulated and emulated
- the ways in which cyber-attacks against the cyber system may manifest themselves
- the actions that trainees are expected to take against these attacks and the tools that may be used for this purpose
- targets regarding the preparedness and effectiveness level that the trainees targeted by a CTTP programme are expected to achieve and how these levels may be measured in different stages of the delivery of the programme

A CTTP model covers two key layers in the implementation of the THREAT-ARREST platform's "cyber system", i.e.:

- the *software* architecture layer (SAL, PAL)
- the *physical* architecture layer (Physical Infrastructure)
- it also covers *dependencies* between components in SAL, PAL and Physical

The CTTP model includes also specifications of two more important aspects that are necessary for the delivery of a ***CTTP programme***. These are:

- a *deployment* model, specifying the allocation of the software (SAL) components of the cyber system onto its physical components
- an *assurance* model, specifying known threats that may affect the physical or software components of the system; assumptions regarding the external environment of the cyber system and the behaviour of agents (human- or system-agents) related to it that can affect it (i.e., prevent or enable threats); and security controls used to mitigate the risks arising from the threats

The CTTP models will function as the central "core" of the whole platform and will "drive" / interact with the platform's technical tools, as presented in next page's Figure 2 and Figure 3.

The CTTP models will also enable training scenarios based on ***"hybrid" combinations of simulation and emulation training***. In these scenarios, some of the components of the cyber system will be emulated and the rest will be simulated. Overall, the training scenarios that will be supported by THREAT-ARREST will vary with respect to the:

- extent of "coverage" of the cyber system under consideration
- types of attacks (e.g. historic or live attacks unfolding as a scenario is simulated by the platform)
- type of response required by the trainee
- a trainee's profile

The allowed forms of variability along the above factors will be defined as part of scenarios forming a CTTP programme.

Finally, it should be noted that evaluating the performance of individual trainees and the adequacy of CTTP programmes as a whole will be an important part of THREAT-ARREST.

The effectiveness and quality of the security training programmes will be evaluated based on validated international techniques/guidelines and will be in terms of:

- trainee's satisfaction
- completeness of the training material
- amount and quality of skills obtained by each trainee
- change of the trainees' behaviour as a group towards security issues and
- Return-On-Investment (ROI)

Platform & Tools

Figure 2 and Figure 3 below present the overall THREAT-ARREST platform tools and architecture (THREAT-ARREST Consortium, 2017) & (THREAT-ARREST Consortium, 28.2.2019).

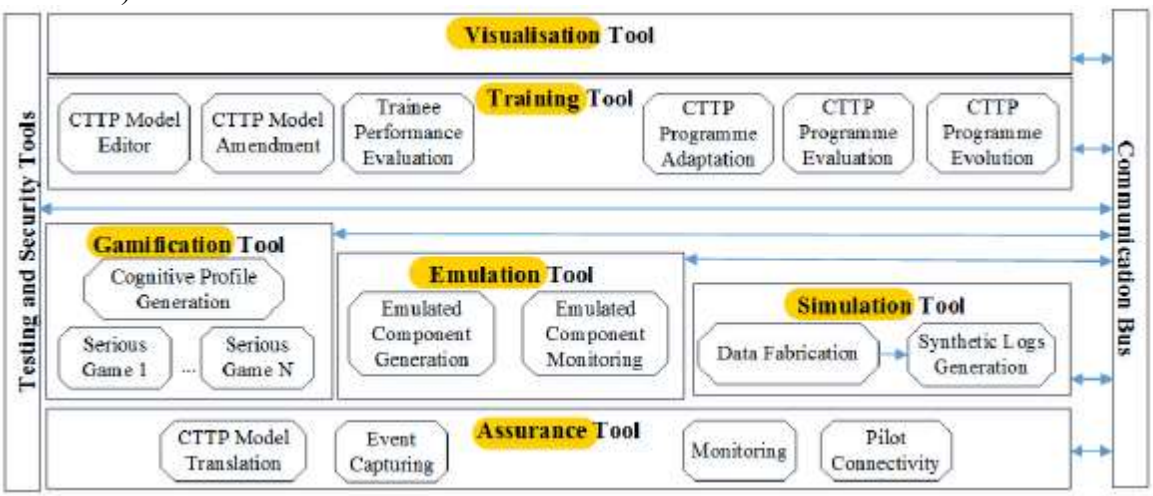

Figure 2. THREAT-ARREST - Platform overall conceptualization

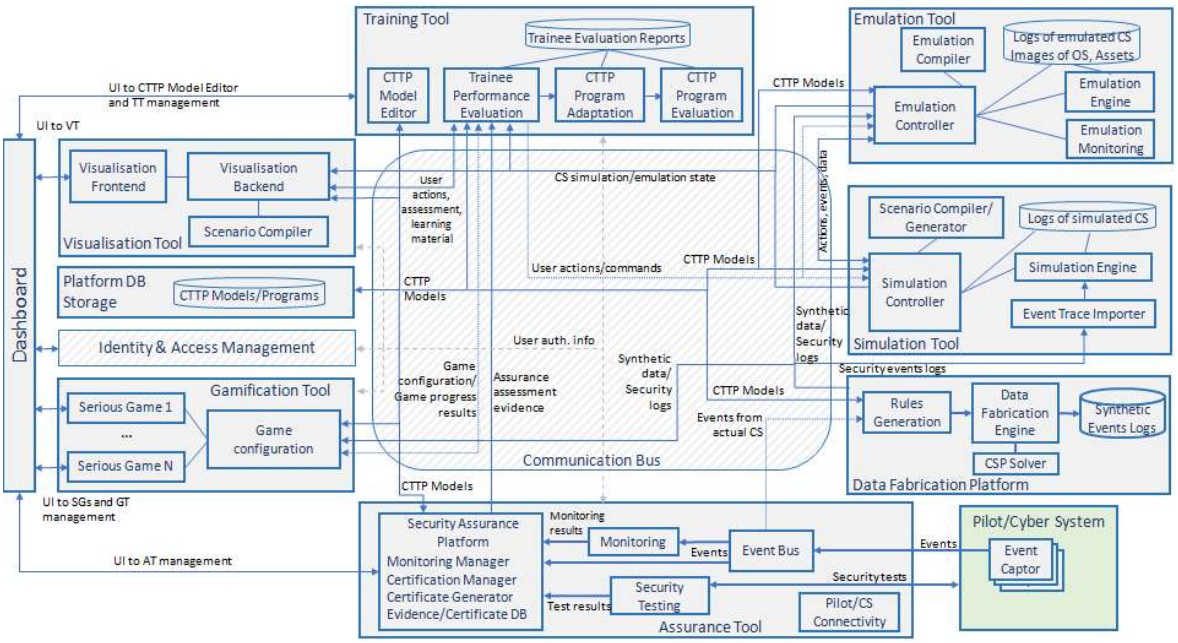

Figure 3. THREAT-ARREST- Platform - logical "integration" layout

Training tool & Dashboard (ITML). The **training** tool supports the definition of CTTP models and programmes, the presentation of learning materials/exercises of CTTP programmes, enable trainee actions in response to cyber threats, interactions with simulated

and/or emulated cyber system components, trainee performance evaluation, CTTP programme evaluation and adaptation. The **Dashboard** will act as the main "interface" with the platform user (trainee/trainer), also interfacing with the other platform tools. The Dashboard will first "initialize" the platform tools for a training scenario.

Gamification / Serious Games tools (SEA). These tools host various serious games, scenarios and training evaluation mechanisms, which enable trainees to develop skills in being resilient to and preventing social engineering attacks (e.g. phishing, impersonation attacks, etc.). The provided games are driven by the threats and assumptions specified in CTTP models (security assurance).

Simulation tool (SIMPLAN). The **jasima®-Java Simulator** tool simulates individual cyber system components and networks of such components to enable the simulation of entire training scenarios defined in CTTP programmes.

Visualization tool (SIMPLAN). The visualization platform enables the visualization of simulations and the effect of training actions on simulated systems. The platform facilitates the creation, parameterization and interaction with the simulation and training platforms. The tool enables users to parameterize scenarios, trigger simulations, and view their outcomes.

Emulation tool (ITML). The emulation platform provides the automated generation of emulated cyber-system components, in the form of interconnected virtual machines (VMs) equipped with the appropriate software stack, as well as their interconnections in Physical and/or Software Architecture Layers (PAL/SAL) of a cyber system.

Security assurance tool (STS). This tool supports the continuous assessment of the security of the cyber system through the combination of runtime monitoring and dynamic testing in order to provide information about the status of the actual cyber system. It also collects runtime system events and generates alerts that provide the basis for setting up realistic simulations. Furthermore, it enables the configuration of security assessment, reporting and certification to the needs of different stakeholders ranging from senior management to external auditors and regulators below summarizes the key tools and technologies that will be integrated in the THREAT-ARREST platform.

Data Fabrication Platform (DFP) tool (IBM). The DFP supports the generation of synthetic logs. In the ordinary operation under THREAT-ARREST, DFP gets input from the abovementioned assurance tool regarding the *actual* logs of the examined pilot system. Then, based on statistical analysis, the platform produces *realistic synthetic* log files and computational/networking events. These outcomes are later parsed by the simulation/emulation/gamification tools in an attempt to provide training under realistic conditions and enhance the overall learning process.

3.2.3 THREAT-ARREST Application / Pilots

Details regarding the three Pilots' requirements, set-up and evaluations have been/will be included in the following Deliverables (see Table 11).

Table 11. Pilots Requirements

Deliverable	Title	Delivery Date
D1.2	The platform's system requirements analysis report"	M4 *(already submitted)*
D7.1	THREAT-ARREST Evaluation Framework and	M20

	Pilot Set Up Guidelines	
D7.2 – D7.4	Health / Energy / Maritime Sectors pilots reports v1	M24
D7.5 - D7.7	Health / Energy / Maritime Sectors pilots reports v2	M34
D7.8	Final THREAT-ARREST evaluation report	M34

Additionally, details regarding specific training needs are included in the present report's subsection 2.1.

3.2.4 The THREAT-ARREST's Innovation Proposition

Overall Innovation Potential

THREAT-ARREST, through its cyber range / cybersecurity training platform, aims to bring innovation in cybersecurity by providing the basis towards the establishment of a European Cybersecurity Academy - through a network of national cybersecurity "academies" - in order to provide multi-disciplinary curricula and training recognized at European level against advanced cyber threats in multiple domains. The envisioned platform can be directly linked to certified studies in advanced cyber threats mitigation; thus, building an ecosystem of large enterprises (LEs) as well as small-medium entities (SMEs) that comprise critical infrastructures in various fields of operation and on top of multiple technologies, will maximise innovation potential and may assist towards the vision of the aforementioned European Cybersecurity Academy.

Examining the current landscape, as formulated by the leading solutions available today *(see present report's Section 2),* we can identify innovations that THREAT-ARREST will bring to the market:

- THREAT-ARREST will bring to the market a ***complete cyber range solution***, comprising innovations & advances in numerous technologies and fields (models-driven, security assurance testing and monitoring, visualisation, serious games, simulation, emulation and hybrid training)
- THREAT-ARREST will be capable of an ***overall training process modelling***, the ***real-time assessment of the security features*** for an examined system and the ***continuous evaluation of the trainees***
- The THREAT-ARREST platform ***will not be industry-specific***; it will be validated in 3 different, complementary industrial pilots with different security requirements and will be ***applicable and adjustable to any other industrial field***
- THREAT-ARREST, building on top of existing solutions, aims to ***form the basis for the definition of the cyber security training value chain***
- THREAT-ARREST will as well focus on the ***creation of a Cybersecurity ecosystem, engaging complementary stakeholders from various fields***

Furthermore, THREAT-ARREST is expected to:

- develop advanced education and training methods and skills for high-risk and vulnerable industries in multiple scenarios and increase their effectiveness and efficiency of evidence analysis and final decision making, in terms of both detection time and response time
- increase society's resilience to advanced cyber security threats in terms of (i) ensuring significant coverage of such threats through multiple and diverse training scenarios and

providing means of mitigation and (ii) maximising the society's engagement to the envisioned training platform by developing a cybersecurity ecosystem

- provide a holistic training experience, covering a wide range of automatically adjustable difficulty levels and scenarios, significantly improving the capability of those charged with defending ICT systems to deal with advanced threats.
- support the development of disruptive innovation in the field of cyber security awareness training; it will provide innovative technologies, solutions and services to high risk industries
- directly enhance innovation capacity to three critical industry fields (Energy, Shipping and Health)
- significantly contribute to the growth of SMEs providing security-related services; enable SMEs to enhance their products and strengthen their position in the market
- minimise risks associated with digital business initiatives and thus support the development of competitive start-ups and spin-offs
- provide significant added value to services provided by companies in the Energy, Shipping and Health sector
- contribute to existing standards / regulations / certifications, based on the significant expertise of specific Partners
- enhance the trust and engagement of individuals and enterprises to critical ICT systems
- improve quality of life and the feeling of security and safety for the citizens through advanced and more safe services in at least 3 critical domains (Shipping, Energy and Health)
- boost markets related to critical infrastructures and ICT systems, leading to increased employment rates in multiple fields
- contribute towards enhanced cyber security and risk management in the smart energy domain and facilitate the smooth transition to energy- and cost-efficient, as well as environmentally friendly infrastructures

The Platform's specific Technologies: Innovation & Advancements

Innovations and Advancements regarding the Platform's Tools & Technologies are presented in Table 12.

Table 12. THREAT-ARREST Platform & Tools Innovation / Advancements

Area / Technology	Innovation / Advancement
Simulation	Provision of a cyber system simulation tool, driven by security assurance models. The tool will be able to simulate not only a network (as most of the current simulation tools do) but also components of all layers in the implementation stack of a cyber system, their processing behaviour and security properties.
Emulation	Providing an emulation tool, able to automate the process of a full-scale physical cyber system emulation, based on well-defined architecture and security assurance models. The parts comprising this emulated cyber system will be able to interact with simulated entities towards exchange of data and information.
Visualization	Building on existing techniques, following an approach using a 2D symbolic visualization and a post-process animation of simulation events. Enhancing existing tools by incorporating advanced interactive capabilities and real-time analytics in terms

Area / Technology	Innovation / Advancement
	of performance assessment, scenarios' reconfiguration and parameters' adjustment.
e-Training	Providing additional capabilities in terms of parsing CTTP models and driving the operation of the system's emulated and simulated components. The envisioned e-training environment will also support high level of interactivity with the trainees in terms of (i) real-time assessment and (ii) automated scenarios' adjustment. It will also provide advanced trainee performance evaluation capabilities including comparisons between actions on simulated/emulated and the real system components.
Serious Games	Exploiting current solutions in serious games applied in the cyber security field, and advancing them by incorporating to them advanced visualisation tools as well as sophisticated training modules offering automated scenarios' and levels' configuration based on real-time assessment techniques. A key advancement in THREAT-ARREST will be the delivery of model-driven gaming focused on assumptions set by security assurance models and combined with simulation and emulation in hybrid CTTP programmes.
Data Fabrication	Provide realistic logs and networking events based on the actual traces of the examined pilot system. Thus, the organization's personnel will be trained under more realistic conditions and will face the same operational conditions as if the real system is used. This hands-on experience would enhance further the training outcome.
Security assurance	Connecting continuous security assurance with cyber security training and developing a platform based on synergies between the two. In particular, the vision is to articulate training (CTTP programmes) on security assurance schemes, to use evidence collected from continuous assurance assessment in order to create realistic simulations for CTTP programmes and use continuous monitoring of assurance schemes to measure the performance of trainees following training.
Security monitoring	Deploying the monitoring capabilities of the assurance tool (which will be incorporated in the platform) and extend them with event capturing and analysis capabilities at the emulation and simulation levels (e.g., user actions, emulated component responses etc.). Carrying out statistical profiling of monitoring events (these capabilities are important for realising the overall innovative vision of THREAT-ARREST, although they do not by themselves constitute a significant advancement in the state-of-the-art in monitoring.
Security Testing	Coming up with new threat and vulnerability models to represent the IT/OT interface in CPSs, in order to generate test plans specific for each industrial domain. At the OT interface, the relative importance of detecting specific vulnerabilities is related to the target devices; THREAT-ARREST envisions a scanner with a lower detection rate that will be more effective in cases where the vulnerabilities it detects are individually more severe in the damage their exploits may do.

Sustaining innovation

In order to sustain Innovation, THREAT-ARREST aims to form the ground towards a cybersecurity ecosystem that will interlink clusters and initiatives in order to create value for many stakeholders including researchers, experimenters, SMEs, policy makers, universities and students etc. Innovation clustering initiatives are viewed as a key abstraction for creating the appropriate ecosystem, however these are often characterised and constrained by their regional nature. Therefore, a European-wide initiative is the key towards sustaining innovation in cybersecurity (THREAT-ARREST targeted Stakeholders are identified in detail in section 3.4.2 of the present report).

3.3 Standardization & Intellectual Property

3.3.1 Contribution to Standards and Regulations

Standards play a key role in improving cyber defence and cyber security across different geographical regions and communities. Standardizing processes and procedures is also essential to achieve effective cooperation in cross-border and cross-community environments. The number of standards-developing organizations (SDOs) and the number of published information security standards have increased in recent years, creating a significant challenge.

Following on the above, the issue of the fragmented nature of the EU security market (lack of harmonized certification procedures and standards) still remains and has a negative impact on both the supply side (industry) and the demand side (public and private purchasers of security technologies), leading to barriers to market entry and makes true "economies of scale" difficult. To this extent, THREAT-ARREST will be closely monitoring the recent developments in the EU legislative/regulative cybersecurity context (*see in the following).*

As Figure 4 below shows, the THREAT-ARREST Consortium has identified the following EU Strategies and International/European Standardization / Certifications Bodies that will be closely monitored during and after the project lifetime, while for some of them, specific contributions are envisaged to be provided (ITU, 2018):

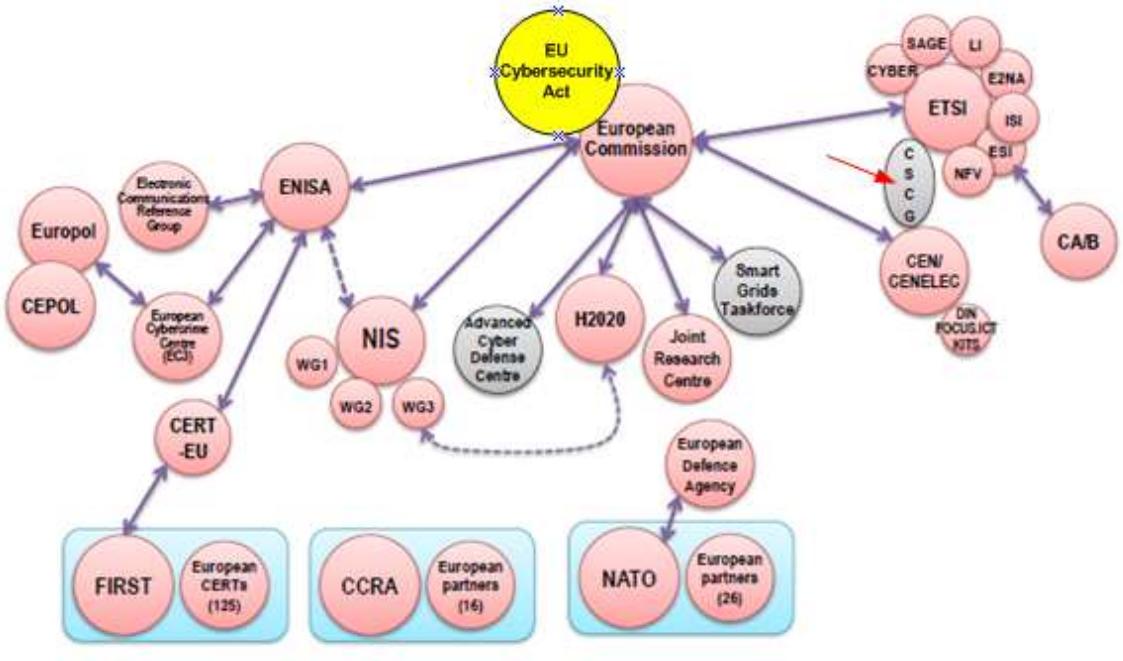

Figure 4. European Cybersecurity Ecosystem (ITU)

1. **The EU Cyber Security Strategy (EU CSS)** (2013), with its ongoing review and the recent (27/6/2019) **EU Cybersecurity Act** (EU Cybersecurity Act, 2019) / **EU certification framework** for ICT digital products, services and processes. The European cybersecurity certification framework will enable the creation of tailored and risk-based EU certification schemes. **ENISA** will play a pivotal role in this, while the **Stakeholder Cybersecurity Certification Group (SCCG)** will be responsible for advising the Commission and ENISA on strategic issues regarding cybersecurity certification. The EC Cybersecurity strategy includes the **Directive (EU) 2016/1148 on Network and**

Information Security (NIS), which requires Member States (MS) to have minimum NIS capabilities in place, and cooperate and exchange information within a dedicated network, and demand the private sector to adopt NIS enhancing actions. Towards this direction, THREAT-ARREST, as an innovative cyber range platform, will be able to be appropriately disseminated and standardized in order to be more widely used (see Figure 5).

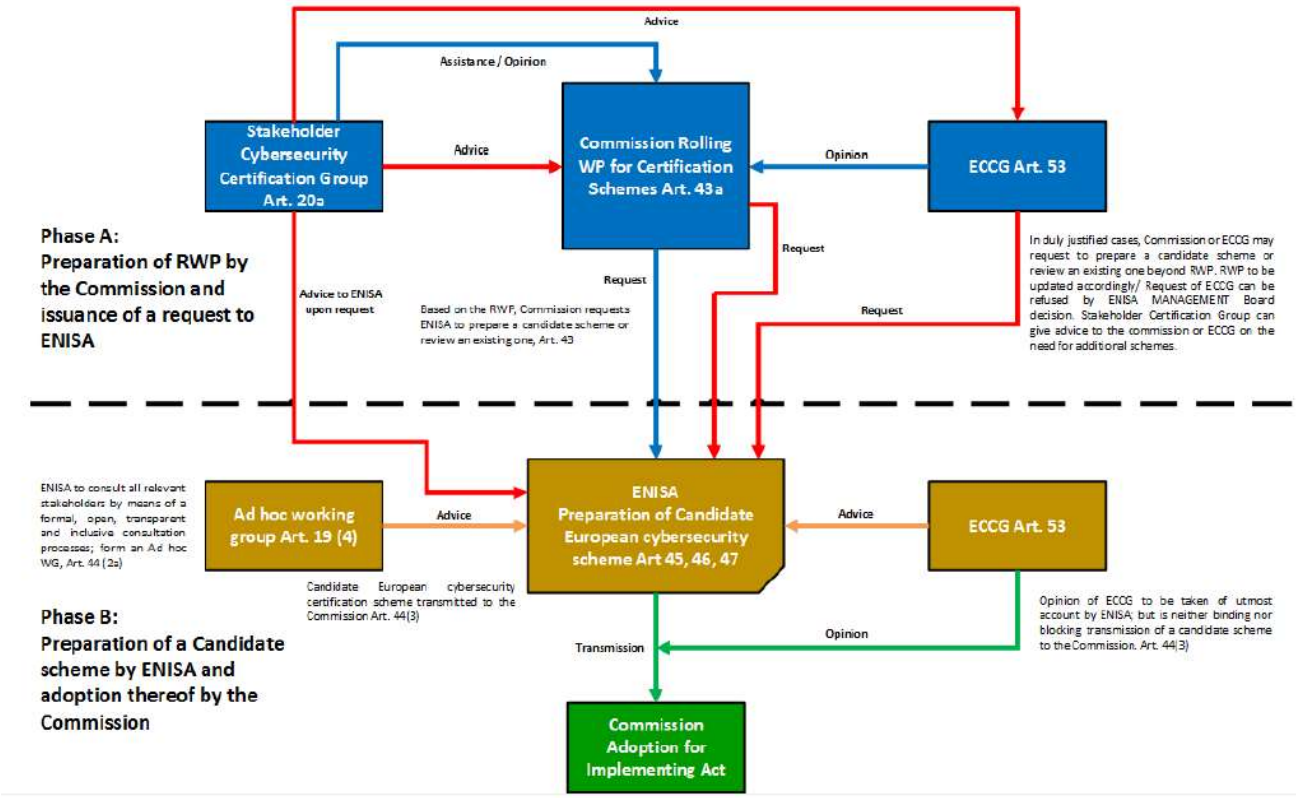

Figure 5. Cybersecurity Certification Framework & ENISA (ENISA / Dr. Steve Purser, 21.1.19)

2. **ENISA** has established working collaborations with Standards Developing Organizations (SDOs) and specific working groups (WG), such as **ISO SC27, ETSI, CEN / CENELEC and ITU SG17** *(see* Figure 6,Figure 7 *and* Figure 8*).*
3. The **European Cyber Security Organisation** (**ECSO**) (ECSO - European Cyber Security Organisation, 2019), who represents the industry-led contractual counterpart to the European Commission for the implementation of the Cyber Security Contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations, countries part of the European Economic Area (EEA) and the European Free Trade Association (EFTA) and H2020 associated countries. ECSO's main objective is to support all types of initiatives or projects that aim to develop, promote, and encourage European cybersecurity. The following ECSO's working groups will play a pivotal role:
    a. **Working Group 5 (WG5)**: Education, awareness, training, cyber ranges) and
    b. **Sub-group SWG5.1:** Cyber range environnements and technical exercises (ECSO-WG5, Nov.2018)

4. **The EU Cloud Strategy**: EC published its cloud strategy, entitled 'Unleashing the Potential of Cloud Computing in Europe.' The strategy aims to improve the adoption of cloud computing in Europe so as to drive innovation and reduce costs in the EU's digital market. Given that the THREAT-ARREST framework is targeted to any SMEs/enterprises/organizations in multiple sectors, adherence with this strategy will be supported, while produced white papers on behalf of the THREAT-ARREST consortium can provide valuable information with regards to evolution of such a strategy.
5. **THREAT-ARREST** will pursue close collaboration and networking with the European Reference Network for Critical Infrastructure Protection (**ERNCIP**) in order to keep up with as well as contribute to the progress of harmonization of test protocols throughout Europe. In particular, THREAT-ARREST aims to collaborate closely with ERNCIP's Thematic Group on "**IACS** Cybersecurity Certification Framework", which focuses on the establishment of the European IACS Components Cyber-Security Compliance and Certification Scheme.
6. **ETSI Cyber Security Technical Committee (TC CYBER)**: TC CYBER is working closely with relevant stakeholders to develop appropriate standards to increase privacy and security for organisations and citizens across Europe. THREAT-ARREST mechanisms are going to be disseminated to TC CYBER.
7. **CEN-CENELEC-ETSI** (as SDOs) and the **'Cyber Security Coordination Group' (CSCG)** (Focus Group on Cybersecurity): The group aims to provide strategic advice in the field of IT security, Network and Information Security (NIS), and cyber security (CS). Contribution from THREAT-ARREST can be used towards the preparation of set of advices.
8. **ISO/IEC JTC1/SC27 Working Groups**, who work in the fields of Information security, cybersecurity and privacy protection Standardization.

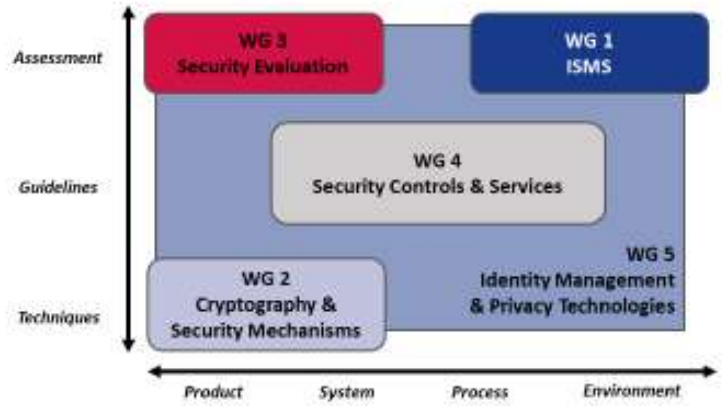

Figure 6. ISO/IEC JTC1/SC27 WCs (ENISA, Dec.2018)

9. **Current *International*** and developing ***European*** **schemes** on Information and ***Cybersecurity Professionals Certifications***: Capitalizing on its innovative capabilities regarding cybersecurity professionals' training evaluation / certification, THREAT-ARREST can also play a significant role in the cybersecurity professionals certification field, including:

   → ***International*** schemes (ISACA-CISA/CISM, $(ISC)^2$-CISSP, CSA-Cloud Security, SNAS-GIAC, etc.

→ ***European*** schemes under development (ref. e-CF European e-Competence Framework 3.0) ((ECSO-WG5, Nov.2018)

Table 13 below presents the most important Certification schemes.

Table 13. Cybersecurity Professionals' Certification Schemes (ECSO-WG5, Nov.2018)

Cybersecurity Professional - Certification Provider	Country	Certificates
e-CF	European	e-CF (EN 16234-1 based)
National European schemes	European Countries	EITCI, ANSSI / PASSI, NCSC UK schemes et al.
ISO schemes (IAF / IRCA / ANSI / AFNOR etc.)	International / many Countries	ISO/IEC 27001 Lead Auditor & similar
$(ISC)^2$	USA	CISSP, SSCP, CCSP
ISACA	USA	CISA, CISM, CRISC, CGEIT
GIAC	USA	GSLC, GSNA, GISP, GSTRT
CompTIA	USA	CASP, CSA+, Security+
EC-Council	USA	CEH
NIST NICE Cybersecurity Workforce Framework (NCWF)	USA	(specialty areas certifications)
NIST NSCP Program	USA	NIST Cyber Security Professional (NCSP) (NIST Cyber Security Professional (NCSP), 2019)

The THREAT-ARREST consortium will be in constant communication with ENISA regarding the development of the European Cybersecurity Professionals Certifications.

3.3.2 Standardization and Open Source Engagement

Cybersecurity open source software (OSS), like all manner of OSS development and usage, is an irreversible trend and, indeed, open source is driving Innovation everywhere. Today, open source code is so effective and cost efficient that it is used in more than 90 percent of all commercially available software (securitymagazine / K.Bergelt, 10.4.19). Market reviews predict that open source will play an even larger role in Cybersecurity (VMWare / D.Hohndel, 13.12.17).

It should be noted that, although the Intellectual Property Rights (IPRs) and Standardization systems both aim to support and incentivize innovation and technological progress, the intersection of these two mechanisms may give rise to various tensions and conflicts. The standardization system is based on the assumption of commonalities, creating an even playing field for competition by granting stakeholders equal access to innovative solutions. Conversely, the IPRs system is based on the award of temporary monopolies borne of IPR holders' ability to exclude others from implementing protected technologies. The contrasting principles of the inclusivity of standards and exclusivity of IPR do not meet without complexity ("uneasy reconciliation" of two aspects of Open / Interoperability standards: that

they should both incorporate leading-edge technology as well as be generally available and accessible for implementation) (Mair, 2012).

Regarding Open Source, and based on each Partner's "background" technology / experience, but also following on the project's development, the following guidelines will be followed:

- Partners may be using Open Source components - tools (e.g. OpenStack, Messaging tools, etc.) or code in their deliverables or be contributing their deliverables to Open Source communities.
- Alternatively, some of the Partners may be contributing to Standards *(see previous Sect. 3.3.1)*, whether these are open standards or other.

Details concerning open source code use and contributions to standards have already been addressed in the Consortium Agreement (CA). Further on, during the course of the project, open source matters will be finalized / agreed upon in more detail – if needed.

Regarding the project's results, the THREAT-ARREST knowledge management and protection strategy aims to be as open as possible, in order to achieve maximum impact of the project results, so the default ruling is that results will be public. This ruling will be different where this is explicitly required by the legitimate explicit interests of THREAT-ARREST partners. In particular, for what concerns IPR developed *within* the THREAT-ARREST experiments, the following pattern will be followed as part of each of the experiments:

- delivering *public* reports (deliverable of type "R, PU") about the requirements, KPIs, principle solutions, as well as lessons learned for each of the pilots; and
- performing *confidential* piloting activities (deliverable of type "DEM, CO"), to ensure IPR protection, while offering controlled release of IPR and knowledge as part of the aforementioned public reports.

In terms of the policy, if and when Open Source is used:

- permissive free software type license (Apache 2.0 license or a similar) will be the minimum expectation
- viral / copyleft licenses (GNU/GPL or similar) will be explicitly forbidden since they dramatically restrict the uptake of open source by commercial parties which will be extremely influential for THREAT-ARREST

According to project development, Open Source and "Commercial/Licensing" Business Models may co-exist.

THREAT-ARREST's orientation is towards Open Interfaces & Specifications, so Open Source is simply seen as "one of many" implementation environments which are down to Partners and subsequent practitioners to choose.

3.3.3 Intellectual Property, Licensing, Open Access & Data Management strategy

The cybersecurity industry has the potential to be a significant driver of innovation and protection for the global economy. However, unlike other areas of the information technology industry, cybersecurity is a relatively young and fast developing segment where an IP/Licensing culture has not yet taken hold. Once dominated by several enterprise and consumer-focused companies, today thousands of cybersecurity software vendors exist, as well as more than 60 open source software security platforms hosted on GitHub. With the industry's growing market size, many aggressive entrants and an open source software model that is fast becoming the standard way of moving innovation forward, there is a potential for established vendors to look to impair these growth drivers through the use of intellectual property (securitymagazine / K.Bergelt, 10.4.19). Additionally, the expected growth in the

cybersecurity software industry has the potential to be significantly disrupted and its innovation impaired by patent lawsuits.

On the other hand, cybersecurity open source software (OSS) projects, like all manner of OSS development and usage, is an irreversible trend. Today, open source code is so effective and cost efficient that it is used in more than 90 percent of all commercially available software.

Aiming to address and take advantage of the above scheme, THREAT-ARREST has already and will continue to improve on its Intellectual Property (IPR) strategy. Main IPR management goals are:

- fostering a focused project approach towards generating IPR as one of the main drivers of the project and the project's deliverables work;
- evaluating project results to identify opportunities for IPR protection; and
- avoiding premature disclosure, which could compromise the ability to secure patents or other IP rights (this process will be managed by monitoring external publication or disclosure of project results)

All THREAT-ARREST Partners have and will have an active interest in the dissemination and exploitation of the obtained results - *throughout* and *after* the project - something which is also required in order to create a strong impact of the proposed concepts at a European level.

IPR management, handling of potential legal issues and the basic guidelines/policies for the management of knowledge, intellectual property and innovation have already been defined in the Consortium Agreement (CA). Overall, the IPR strategy is focused and clear, in order to best protect innovations developed within the timeframe of the project from attacks by competitors.

IPR matters will be continuously monitored by the Steering Committee and be amended if any improvements can be introduced. The Steering Committee, in collaboration with the Project Management team, will be the main responsible for the management of IPR and for the resolution of any IPR problems that occur.

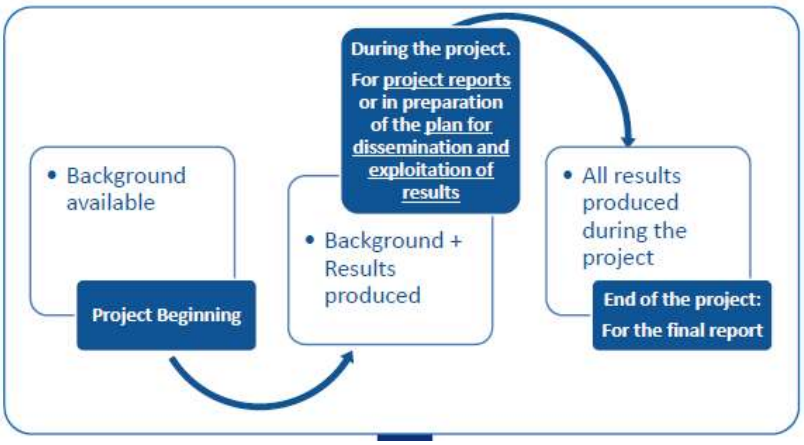

Figure 7. Timing of THREAT-ARREST IP Reviews

The overall THREAT-ARREST Consortium IPR policy handles the following issues and sets the following policies:

(a) protects *pre-existing* know-how and information related to the use of knowledge owned by individual partners from work carried *independently of* the THREAT-ARREST project. It

is important to guarantee confidentiality on any information disclosed by the partners during the project development.

(b) protects IPR of any knowledge gained *within* the THREAT-ARREST project:

- if an invention has been the work of a single Partner, then this Partner will be the sole owner of this knowledge, subject to granting access rights to other partners whenever necessary.
- if an invention has been the work of a more than one partner, they will all have shared ownership of this knowledge (shared IP ownership matters will be further clarified in the course of the project, if such need arises).
- access to the knowledge generated *within the project* will be granted royalty-free to the THREAT-ARREST partners for the execution of the project. Agreements for the preferential or at market conditions for *use* of this knowledge outside the scope of the project shall take place by the relevant partners *(see* Table 14 *below)*.

Table 14. Granting of Access & Use Rights ((European IPR HelpDesk / J. Scherer, 17.4.18), (European IPR HelpDesk, 2019))

	Access to Background	Access to project Results
During project implementation	• Royalty-free	• Royalty-free
Use of project results	• Royalty-free (requested / granted for up to 1 year after project completion)	• on "fair & reasonable conditions" (which in cases *could* also be royalty-free) *(to be discussed / finalized during the course of the project)*

(c) defines the ***exploitation strategy of the obtained results***. It is very important to maintain a balance between IPR agreements and the dissemination and exploitation strategy. The necessary steps to ensure the protection of IPRs have already been taken. Therefore, during the course of the project, partners who own the rights of specific knowledge developed within the project will further decide on exploiting these results (through Licensing, Patents, Copyright or any other suitable form of IP protection – see Figure 8).

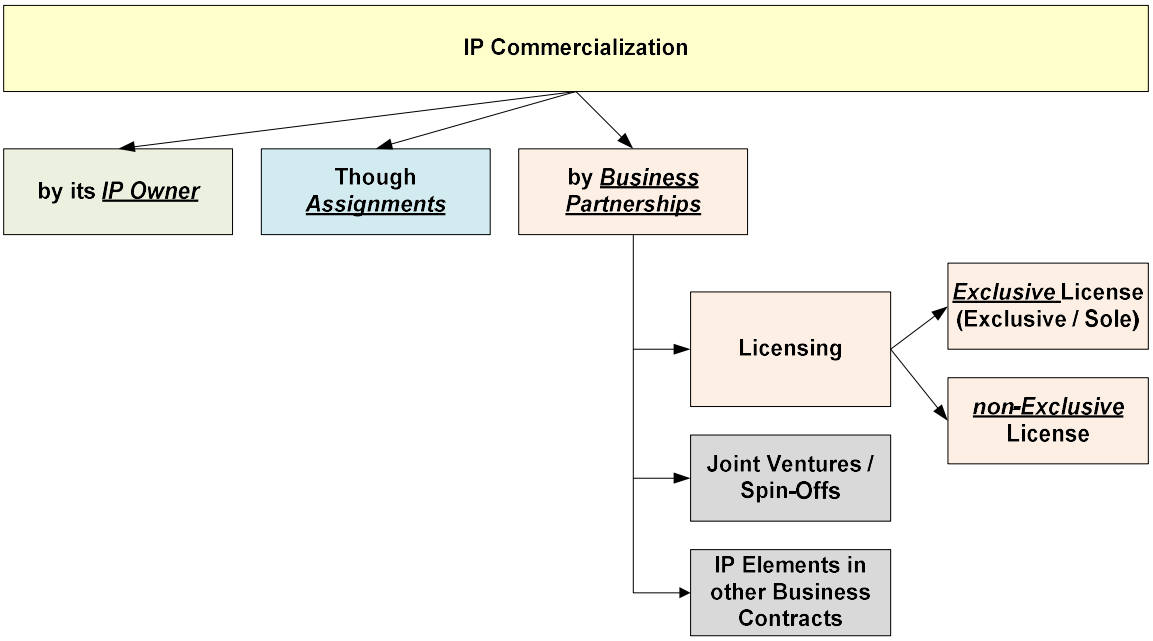

Figure 8. IP "Commercialization" scenarios (European IPR HelpDesk, 2015)

Table 15 below presents potential forms/modes of Project Results IPRs Protection, especially for the "after-project" commercialization period (cases directly relayed to THREAT-ARREST are marked yellow).

Table 15. Potential forms/modes of Project Results IP Protection / Exploitation ((European IPR HelpDesk / J. Scherer, 17.4.18), (European IPR HelpDesk, 2019), (European IPR HelpDesk, 2015))

Subject Matter	**IP.1. Patent**	**IP.2. Utility Model**	**IP.3. Industrial Design**	**IP.4. Copyright**	**IP.5. Database Rights**	**IP.6. Trademark**	**IP.7. (Trade Secret)**
Invention	☑	☑			☑		☑
SW	☑			☑	☑		☑
Scientific Article				☑			
Design of Product			☑	☑	☑	☑	
Name of Product / Service						☑	
Know-How							☑
website			☑	☑		☑	

Sectors of "interest" to THREAT-ARREST marked yellow. It should be noted that the relationship between the Licensing of IPR and competition law in the EU is well summarised in the preamble of the Technology Transfer Guidelines issued by the EC (OECD , 2019).

(d) defines a ***contingency plan*** to ensure the access to knowledge crucial to the project development if a partner with specific IPRs leaves the consortium. Policies for the partial or full transfer of ownership of results between partners should be defined.

(e) regarding ***Open Access***, the Consortium will fully address the European Commission's requirements through the support of open access for published articles. All scientific

publications of project's results will be granted open access according to publisher and law regulations as set out in the Grant Agreement. Depending on the nature of the publication, the articles will be made available immediately through open access publishing ('gold' open access) (e.g. by an open access journal) or within a period of 6 months through self-archiving ('green' open access). THREAT-ARREST partners have already established various Open Access policies: supporting authors in retaining their rights to provide access to published articles, providing official repositories, and making the bibliographic metadata that identify the deposited publication available to OpenAIRE (OpenAIRE, 2019). Other means include finding suitable repositories via OpenAIRE, the Registry of Open Access Repositories (Roar.eprints.org, 2019) and the Directory of Open Access Repositories (Opendoar.org, 2019).

(f) if needed, during the course of the project, a Data Management Plan will be prepared.

3.4 Business Model & Exploitation

The business model of THREAT-ARREST is considered to be a multi-sided one, meaning that there is more than one type of customers that have interest on the service provided. As already stated, and since THREAT-ARREST is a case of several Partners developing several "tech bricks", there is a need for an "integrated" business model / business plan. The overall Business Plan and Business Model will further "unfold" during the course of the project and will rely on knowledge generated within the project, at least partially.

The overall exploitation strategy will also be based on the IPR strategy for the "after project" period - which will be decided/agreed between Partners during the course of the project. As a general rule, there will be a balance between open and closed dissemination for the project deliverables. The possible option of "Open" dissemination (enabling other players in the THREAT-ARREST ecosystem) may also be discussed among Partners.

As presented in subsection 3.3.3, each Partner will define his own IP exploitation strategy, however ***an integrated IP strategy is also required***. During the course of the project, the potential case of a specific Partner taking over responsibility for implementing the exploitation plan for the integrated system, for the after-project period, will also be discussed. In view of all the above, the Consortium will hold, in good time, a dedicated Workshop on Business Planning & Exploitation.

3.4.1 Product / Solution Positioning

Positioning within the cPPP perspective

Figure 9 below shows the positioning of the *THREAT-ARREST,* as an ***innovative cyber range platform***, and its anticipated enhancements with respect to the ***cPPP perspective on Products, Services and relationships with application domains and Secure ICT infrastructures***, as presented in the European Cybersecurity Strategic Research and Innovation Agenda for contractual Public-Private Partnership (PPP) (ECSO, June 2016); as shown, *THREAT-ARREST* covers at least the:

- energy, transport, health and critical infrastructure domains
- IoT, Mobile and cloud secure ICT infrastructures
- almost all related products & services

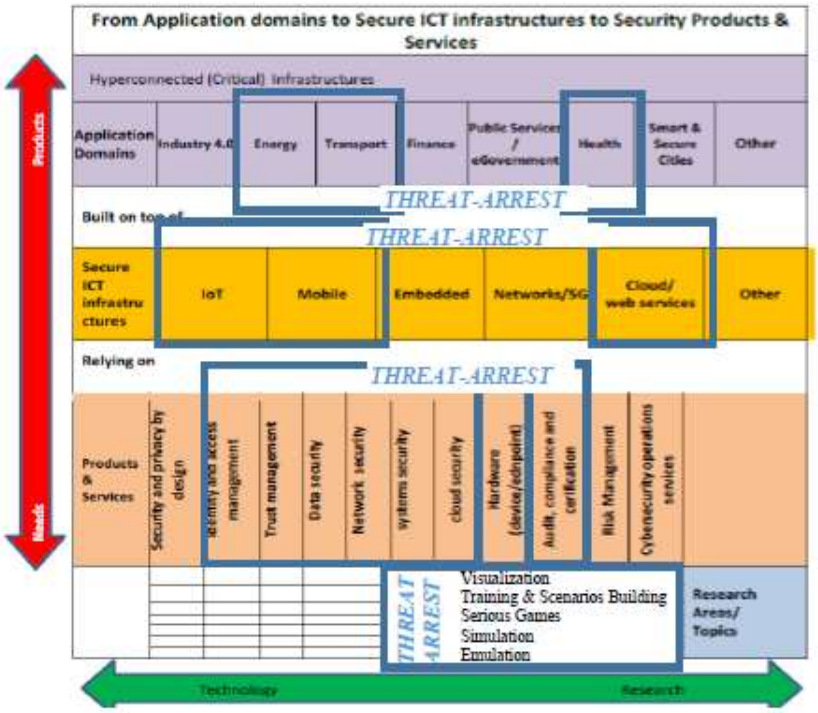

Figure 9. THREAT-ARREST positioning with respect to the cPPP perspective on Products, Services and relationships with application domains and Secure ICT infrastructures

Positioning within the Cyber Ranges / Cyber-Training Platforms Market

As an innovative cyber range platform, THREAT-ARREST will be positioned within the cyber ranges / cyber-training platforms market *(see section 2 on Market Analysis)*.
Expressed industry need / interest on utilizing cyber range / cyber-training platform services is definite, and the overall related Market is rapidly evolving.
The THREAT-ARREST platform can be positioned based on specific critical parameters. The following Figure 10 shows *potential* market segments that the THREAT-ARREST will be able to address and position itself within.
The Consortium will decide and design, during the course of the project, the final "commerciable" platform / solution / services characteristics and specifications. Therefore, *focused* / *exact* positioning of the THREAT-ARREST within the cyber ranges market is not feasible at this point.

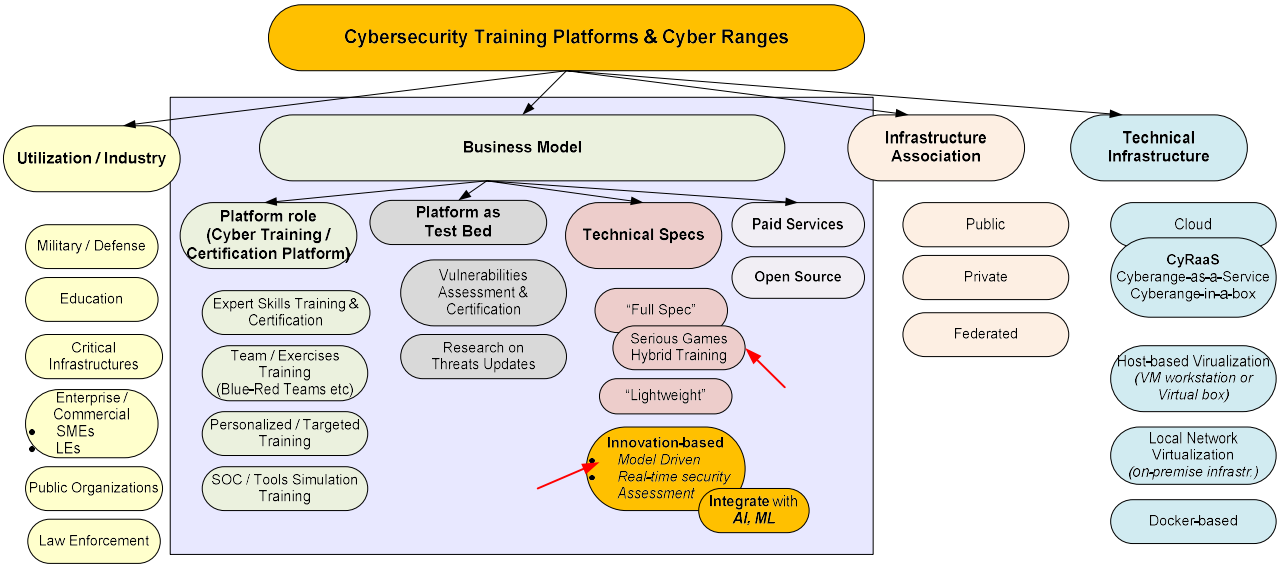

Figure 10. Training Platforms / Cyber ranges segmentation

An overall positioning of THREAT-ARREST could be based on:

- a "product / solution - oriented" segmentation *(see* Figure 10 above)
- a "Stakeholder/Customers-oriented" segmentation *(*see Table 16)

Based on these, the THREAT-ARREST platform could target market subsegments like the "innovation-based platform", or the "Full spec / Serious Games / Hybrid Training" subsegment *(*see above Figure 10 – red arrows), based on:

- the learning content and the adaptability of the training scenarios of THREAT-ARREST platform (scenarios can be easily adapted and extended based on the model-driven approach)
- the provision of Serious Games that can even address Customers / Trainees who do not possess any information security background (these games can also be played on mobile devices)

3.4.2 Targeted Stakeholders/Customers

THREAT-ARREST is envisaged as a participatory project and will engage with numerous relevant actors across the EU. Identification of Stakeholders/Target Groups has started at the planning / proposal stage of the project and it will be continued throughout the course of the project. Stakeholders can be seen / grouped based on:

(a) the ecosystem defined in the ECSO / European Cyber Security cPPP Strategic Research & Innovation Agenda (ECSO, June 2016) & (ECSO-WG3 / G. Rizzo, 10.10.18) (*see* Figure 11*)*

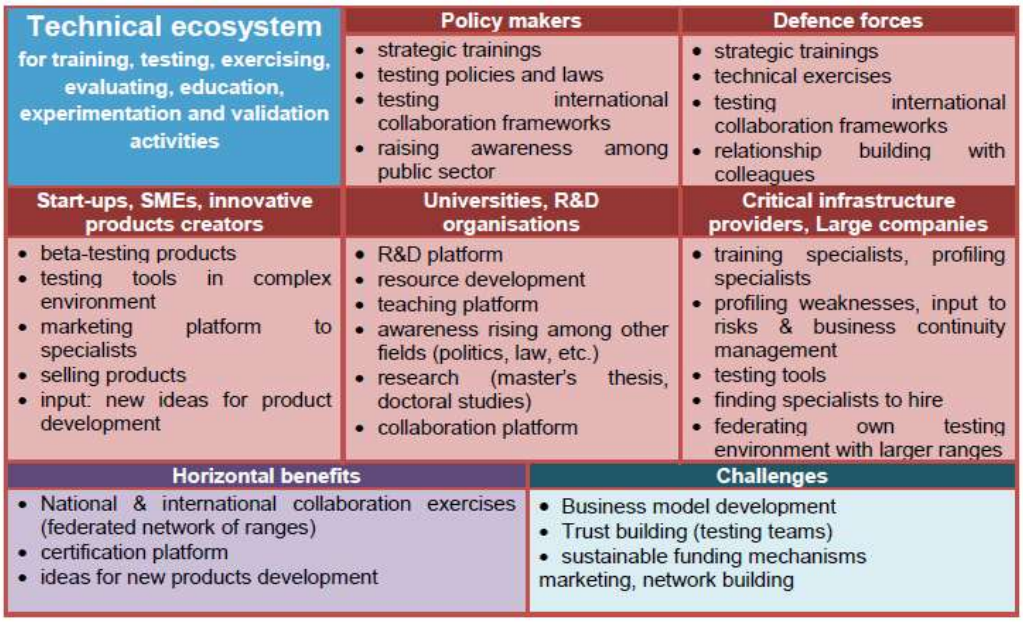

Figure 11. ECSO / cPPP Ecosystem (ECSO, June 2016)

(b) an "Active / Enabling / Internal" Stakeholder perspective (see Figure *12*)

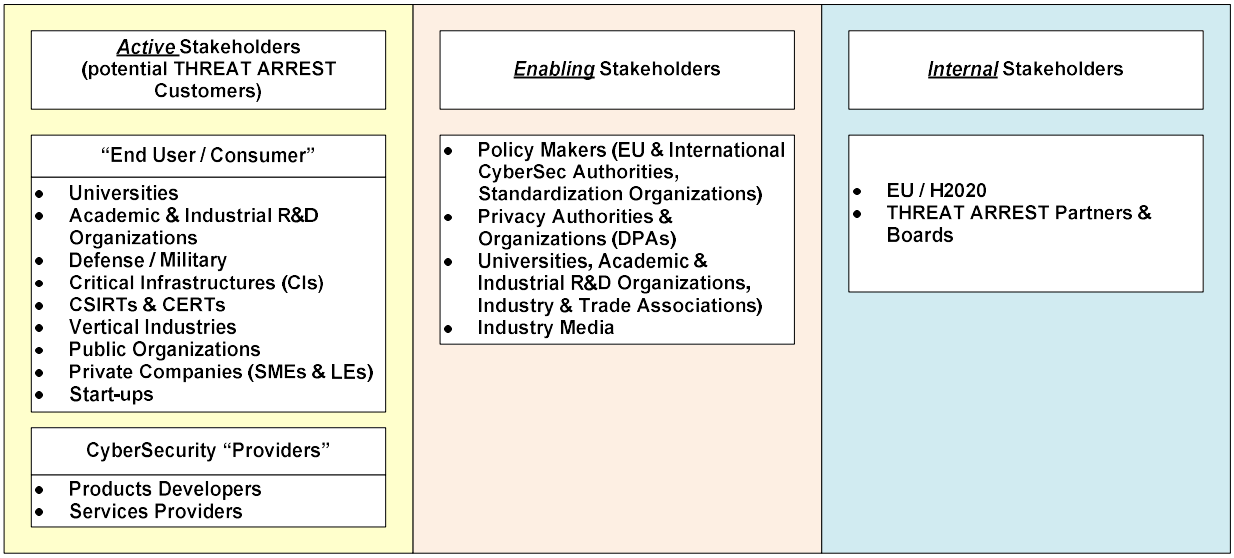

Figure 12. Stakeholders Analysis

Table 16 consolidates all the above:

Table 16. THREAT-ARREST potential Stakeholders / Customers targets Matrix

Group	"Customers" within each Group						Group size	Training & other Needs – cyber-range specs	Reach Strategy
							("tbc" → to be further elaborated/ completed during course of project)		
	Network Operators & Managers	**Security Professionals / Managers**	**Security Designers**	**R&D Community Staff**	**Law Enforcement Staff**	**Non-Technical Staff**			
1.Universities	☑	☑	☑	☑		☑	(tbc)	(tbc)	make them aware of the project results / convince to potentially incorporate it as part of a more complex/complete solution or product
2.R&D Organizations			☑	☑		☑	(tbc)	(tbc)	
3.Defense / Military	☑	☑				☑	(tbc)	(tbc)	help them understand the additional capabilities offered by THREAT-ARREST with respect to existing solutions
4.Critical & High-Risk Infrastructures (CIs)	☑	☑				☑	(tbc)	(tbc)	
5.CSIRTs / CERTs	☑	☑				☑	(tbc)	(tbc)	
6.Vertical Industries	☑	☑				☑	(tbc)	*(see sections 2.1.1-2.1.3 on training needs for Health care, Smart Energy & Smart Shipping)*	
7.Public Organizations	☑	☑				☑	(tbc)	(tbc)	
8.SMEs	☑	☑				☑	(tbc)	(tbc)	
9.SMEs - *specific business cases*									
10.LEs	☑	☑				☑	(tbc)	(tbc)	
11.Start-Ups	☑	☑	☑			☑	(tbc)	(tbc)	
12.Products Developers			☑			☑	(tbc)	(tbc)	convince them to potentially incorporate THREAT-ARREST as

Group	"Customers" within each Group						Group size	Training & other Needs – cyber-range specs	Reach Strategy
							("tbc" → to be further elaborated/ completed during course of project)		
13.Services providers			☑			☑	(tbc)	(tbc)	part of a more complex/complete solution / product / service
14.Policy Makers / Authorities					☑	☑		(tbc)	
15.Privacy / PII Authorities / DPAs					☑	☑		(tbc)	make them aware of the project results & potential implementation to Law Enforcement (technical Audits)
16.Standardization Organizations (SDOs)								(tbc)	cooperate to include THREAT-ARREST-based training as part of their BOK / training Sessions
17.Industry & Trade Associations								(tbc)	help them understand the innovations / additional capabilities offered by THREAT-ARREST
18.Industry Media								(tbc)	

According to cPPP/ECSO – WG3 working group (ECSO-WG3 / G. Rizzo, 10.10.18), "Users & Operators" (Vertical Industries) can be further classified as in Figure 13. cPPP/ECSO Vertical Industries classification below (the THREAT-ARREST-related validation pilots sectors are marked with yellow).

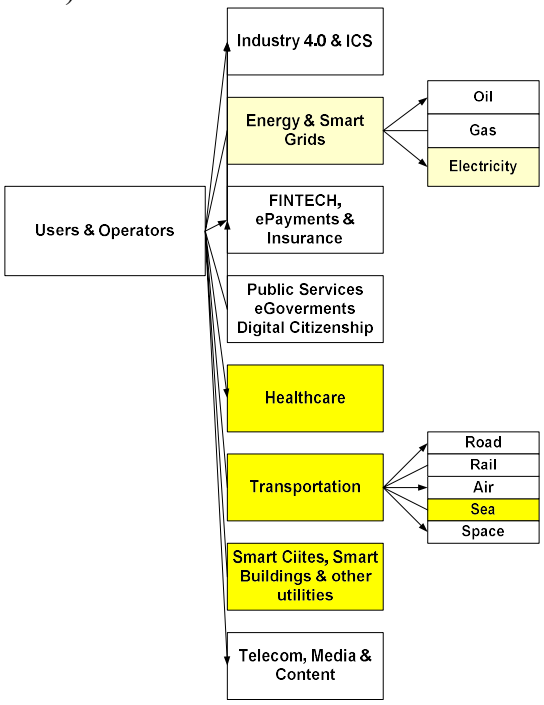

Figure 13. cPPP/ECSO Vertical Industries classification

As already explained, it is too early at this stage to clearly focus & position THREAT ARREST within the above Stakeholders / Customers segments. In the context of the previous subsection 3.4.1.2, an initial positioning of THREAT-ARREST could target segments as:

- Large Enterprises (LEs) / Organizations within high-risk sectors, and/or Critical Infrastructure Organizations that need training programs with tailored-made, in-depth training scenarios.
- Educational institutions / Universities / R&D Organizations
- SMEs with "usual" business cases, for which fixed training programs are sufficient.
- SMEs with more "specific" business cases, for which adaptable training programs are needed.
- Companies of all sizes that need "testbed" services (perform tests / vulnerability assessments of their emulated / simulated cyber systems)

Based on all the above:

- Engagement of different Stakeholders will be initiated and further developed, during the course of the project, by suggestions coming from the different Partners after analysing the relevance of their contact network members to the project as well as an ad-hoc identification process.
- Stakeholders will be invited to take part in the THREAT-ARREST community and participate in the workshops of the project. Some of the stakeholders' groups will also take part in the pilots.
- According to the Project's Dissemination Plan (THREAT-ARREST Deliverable D8.2), an intensive dissemination activity will be developed by the different Partners, through

general and more specific communication activities, for showing the objectives of the project and to attract the attention of further relevant actors.

Apart from the aforementioned stakeholders, THREAT-ARRESST will build strong collaborations with other PPPs and related initiatives as pointed out in the ***European Cyber Security cPPP Strategic Research & Innovation Agenda***, exploiting:

- each Partners' memberships (FORTH is part of the cPPP ECSO and is also involved in the Security WG of the 5G-PPP; ATOS is part of the ECSO, BDVA, FI-PPP and AIOTI; IBM is part of BDVA, 5G, Future Internet (from Haifa), HPC (from Zurich), Cybersecurity (from UK); and TUB is a member of the Photonics and Robotics PPPs) and
- each Partners' existing active involvement in ongoing projects within such initiatives (ITML is exploitation manager in I-MECH project and member of the Productive4.0 project under ECSEL JU)

Furthermore, the THREAT-ARREST consortium will look into potential exploitation of the project results, by assessing the ***potential of further exploiting results within another H2020 (or other) R&I project.*** Cyber range-related Innovation Projects have already been included in the following H2020 Actions (H2020 portalgate / reporting on Actions & Proposals, 2019):

- DS-07-2017 (Addressing Advanced Cyber Security Threats and Threat Actors) – THREAT-ARREST is in fact a part of it
- SU-DS01-2018 (Cybersecurity Preparedness – Cyber Range, Simulation and Economics)

Cybersecurity Training and Cyber Ranges are certain to be pivotal and be included in all further funded projects / RIAs in the near future (*see also* ENISA recommendations – "Analysis of the European R&D priorities in cybersecurity", December 2018*)* (ENISA / Dr. F.Di Franco, Dec.2018) and the present reports subsection 2.1.4. "Training & Compliance")

3.4.3 Competition

For a detailed analysis on the products and services potentially competing with THREAT-ARREST, please refer to the present report's section 2.2 on Market Analysis – Current Offerings Landscape.

Based on the market analysis / offerings data presented in subsection 2.2, and also based on the presentation of the THREAT-ARREST platforms specifications & innovations (see subsections 3.2.1 and 3.2.4), an initial qualitative comparison, between THREAT ARREST and competing Products / Solutions is given in Table 17.

Table 17. Comparison between THREAT ARREST and other Cybersecurity Training Platforms

Feature	TA	BO	KA	CSX	CB	OT
Multi-Layer Modelling	Y	P	Y	Y	Y	P
Continuous Security Assurance	Y	N	N	Y	Y	N
Automatic Security Vulnerability analysis of pilot system	Y	N	N	N	N	N
Realistic Simulation of Cyber systems	Y	P	Y	Y	Y	N
Combination of emulated & real equipment	Y	N	P	Y	N	N
Serious Gaming	Y	N	Y	Y	N	P
Programme Runtime Evaluation	Y	N	N	Y	Y	Y
Programme Runtime Adaptation	Y	N	Y	Y	N	P

{TA= THREAT-ARREST, BO = BeOne (BeOne Development, 2019), KA= Kaspersky (Kaspersky, 2019) , CSX = ISACA CSX (Cybersecurity.isaca.org, 2019), CB = CyberBit (CyberBit, 2016), OT=online training platform | Y = YES, N = NO, P= Partial}

3.4.4 Product / Services Bundles

Specific Product / Solution / Services "bundles", related to the THREAT-ARREST commercialization period, will be further discussed and defined, among Partners, during the course of the project. At this stage, it is too early to present such detailed "commercialized" product/solution specifications.

3.4.5 Business Canvas

Based on the previous sections, a "Business Canvas" has been updated for the THREAT-ARREST Business Plan, as shown in Figure 14.

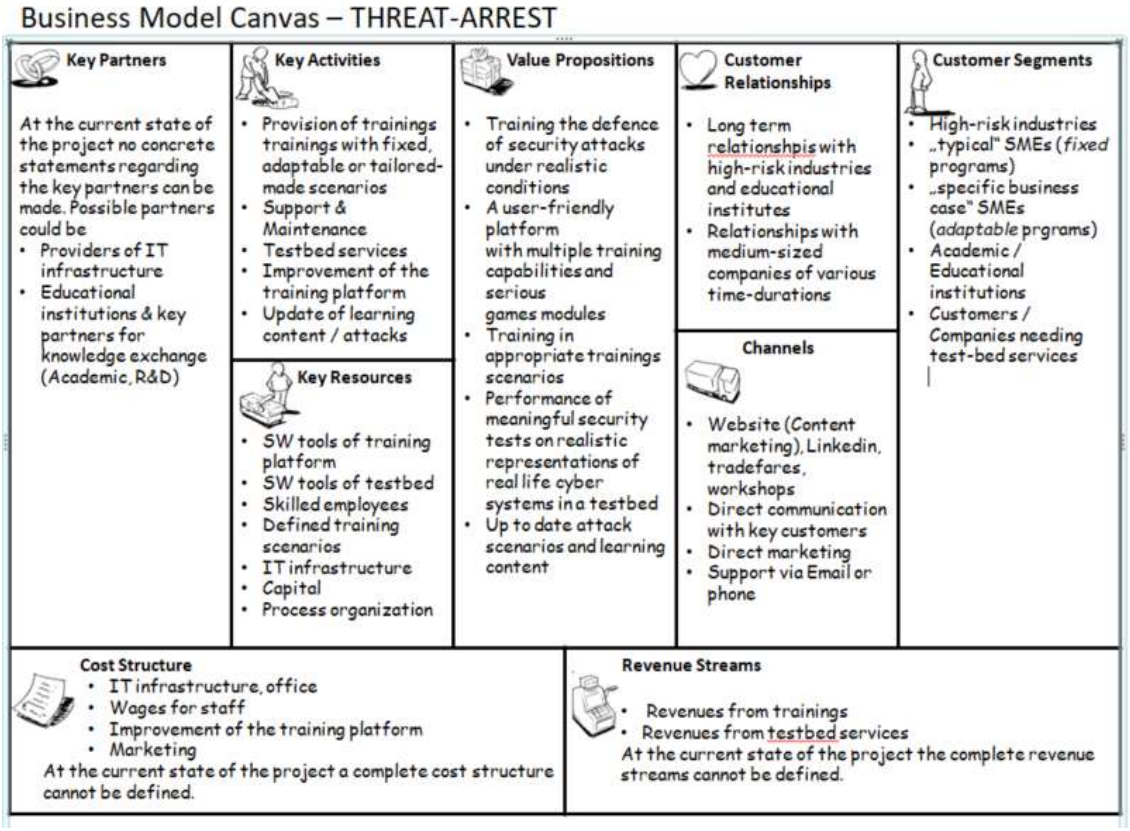

Figure 14. THREAT-ARREST Business Model Canvas

3.4.6 Pricing Mix –Strategy / Revenues Structure

At the moment of documenting the present plan, many of the project development details are not yet defined. Therefore, the final and detailed THREAT-ARREST product/service positioning and the related pricing / revenue strategies cannot, consequently, defined at this stage. The THREAT-ARREST Consortium will look and discuss / decide, during the project course / coming months, upon realistic "commercial" product / service positioning and strategies.

Revenue Streams: these could be generated from:

- **Platform:** Directly (e.g. through selling the training platform's licenses)

- **Platform**: Indirectly (e.g. by selling training services / sessions for the users of the platform, or by using the platform as a "testbed" tool)
- **Partners**: Direct revenue streams: Consulting, SW customization, Training, implementation of additional services, etc.

Based on the overall THREAT-ARREST platform specifications and positioning so far, *potential s*cenarios for Revenues Streams are shown in Table 18.

Table 18. THREAT-ARREST potential revenue streams

	Integrated Platform	**Individual Partners**
One-Time Revenues		
• per specific Training Session	☑	☑
• Consulting		☑
• SW Customization		☑
• Risks Assessment Services	☑	
• Other Additional Services	☑	☑
Recurring Revenues		
• Service Subscription / Contract	☑	☑
• Licensing	☑	☑

In terms of potential pricing schemes to be used, Training Services Pricing could include three different options that the consortium has identified. The first possible option is *Scenario 1: "Charge Everything"*, show in Table 19.

Table 19. Pricing scheme Scenario 1 ("Charge Everything")

#	**Costing / Pricing scheme Charge Everything**	**Level 1 (Basic)**	**Level 2 (Silver / Intermediate)**	**Level 3 (Golden / Advanced)**	**Level 4 (Premium / Advanced)**
1	CTTP Model-driven / Simulation-based Training	€	€	€	€
2	CTTP Model-driven / Emulation & Simulation-based Training		€	€	€
3	CTTP Model-driven / Emulation, Simulation & Serious Games-based Training			€	€
4	CTTP Model-driven / Emulation, Simulation, Serious Games & Data Fabrication-based Training			€	€
5	Fixed-Scenarios Training & Evaluation	€	€	€	€
6	Adaptable-Scenarios Training & Evaluation		€	€	€
7	Tailored-made, in-depth Training Programs (including ICT customizations				€
8	Other added-value, case-based training services				€
9	"Support & Maintenance" contract services			€	€
10	Other (non-Training) Services (e.g. Risk Modelling/Assessment – "Testbed" Services				

(Note: the € symbol means "service included - priced")

Another *possible* Training Services scenario is *Scenario 2: "Freemium"* model-based Pricing (HBR / V.Kumar, 2014) & (EU / L.Probst et.al., 10.2015), shown in Table 20

Table 20. Pricing scheme Scenario 2 ("Freemium")

#	Costing / Pricing scheme Freemium based	Level 1 (Basic)	Level 2 (Silver / Intermediate)	Level 3 (Golden / Advanced)	Level 4 (Premium / Advanced)
1	CTTP Model-driven / Simulation-based Training	free	free	free	free
2	CTTP Model-driven / Emulation & Simulation-based Training		€	€	€
3	CTTP Model-driven / Emulation, Simulation & Serious Games-based Training			€	€
4	CTTP Model-driven / Emulation, Simulation, Serious Games & Data Fabrication-based Training			€	€
5	Fixed-Scenarios Training & Evaluation	free	free	free	free
6	Adaptable-Scenarios Training & Evaluation		€	€	€
7	Tailored-made, in-depth Training Programs (including ICT customizations				€
8	Other added-value, case-based services				€
9	"Support& Maintenance" contract services			€	€
10	Other (non-Training) Services (e.g. Risks Modelling/Assessment – "Testbed" Services				

Finally, a third p*ossible* Training Services scenario identified is ***Scenario 3: "Target Group"-based Pricing*** (e.g. R&D-Education / SMEs & LEs / Public Bodies / Critical Infrastructures etc. (also could be applying the "Charge Everything" or "Freemium" models), as shown in Table 21.

Table 21. Pricing scheme Scenario 3 ("Target Group-based Pricing")

#	Costing / Pricing scheme "Charge Everything" or "Freemium"-based	R&D Education	SMEs	LEs	CIs	Public
1	CTTP Model-driven / Simulation-based Training	€	€	€	€	€
2	CTTP Model-driven / Emulation & Simulation-based Training	€	€	€	€	€
3	CTTP Model-driven / Emulation, Simulation & Serious Games-based Training	€	€	€	€	€
4	CTTP Model-driven / Emulation, Simulation, Serious Games & Data Fabrication-based Training	€	€	€	€	€
5	Fixed-Scenarios Training & Evaluation	€	€	€	€	€
6	Adaptable-Scenarios Training & Evaluation	€		€	€	€
7	Tailored-made, in-depth Training Programs (including ICT customizations			€	€	
8	Other added-value, case-based services			€	€	
9	"Support& Maintenance" contract services	€	€	€	€	€
10	Other (non-Training) Services (e.g. Risks Modelling/Assessment – "Testbed" Services	€	€	€	€	€

(Note: the € symbol means "service included - priced")

3.4.7 Roadmap

The proposed roadmap is split in two sections:

(a) *individual Partners'* roadmap

(b) the *integrated product's (commercialization*) roadmap

Regarding the *integrated product's* roadmap (*section 0 below*), this will be further analyzed, agreed and detailed during the course of the project. Regarding the *individual Partners'* exploitation / roadmap, details are shown in the following section 0.

Individual Partners Exploitation / "From Prototype to Product" Roadmap

Table 22 presents the roadmap for the development of different components of the THREAT-ARREST platform for the individual partners:

Table 22. THREAT-ARREST Partners' Roadmap

Tool / Partner	Current TRL	Advancements by THREAT-ARREST	Final TRL	Roadmap
Training & Dashboard [ITML]	TRL6	Translation of simulation specifications in CTTP models and statistical profiles into DFP rules to enable synthetic event generation for the purposes of THREAT-ASSET	TRL7	ITML aims to exploit the outcomes of THREAT-ARREST, to enhance its market position with respect to intelligent management of advanced security threats, as well as on providing training services in multiple domains. Moreover, ITML's vision through THREAT-ARREST is to exploit the advanced visualisation, gamification and training tools on the basis of the project's findings, which can be used to enhance its current products. Last, ITML will exploit the project's findings in enhancing and strengthening its positioning within the EU market and research domain, establishing partnerships and agreements for further collaborations with the large corporations participating in THREAT-ARREST
Gamification / Serious Games [SEA]	TRL4	Serious Games will be enhanced with (i) advanced scenarios of cyber threats' mitigation and (ii) new visualisation components	TRL7	SEA will gain expertise and create scenarios for our existing games to address the needs of a wider audience of stakeholders from e.g. the energy domain. Moreover, SAE will create new serious games, trainings and tailor them to achieve standard compliance domain-specific standards such as NERC CIP (energy domain), ISO 27799 (health care domain), etc. Furthermore, participating in the case studies of this project will allow us to expand its work for evaluating the efficiency and effectiveness of cyber-security training programs. In the future, SEA will launch a new service to support customer in evaluation their internal or external training programs using the criteria customer satisfaction, learning, attitude towards security, flow, planned behaviour and overall security

Tool / Partner	Current TRL	Advancements by THREAT-ARREST	Final TRL	Roadmap
				impact of the training. Measurable results include new serious games, reasoning for their compliance to the training demands of domain-specific security standards, new evaluation methods for cyber-security trainings, presentation of these artefacts on exhibitions
Simulation [SIMPLAN]	TRL7	The Jasima simulator will be configured and adopted in order to meet the needs of the *THREAT-ARREST* training platform (i.e., simulation of different layers in the cyber systems implementation stack.	TRL7	The THREAT-ARREST project will allow SIMPLAN to enter new fields of application with its simulation expertise. With the simulation engine Jasima, SIMPLAN will build upon existing background. This engine will be substantially extended to match requirements for network security simulations. These extensions and the knowledge generated in the project will allow SIMPLAN to enter promising new markets for simulation in the field of cyber-security. As a side-effect, the simulation engine and the visualization components will also be strengthened for the markets where SIMPLAN is already active. Necessary resources to develop the THREAT-ARREST solution from prototype/demonstrator to product will be financed by SIMPLAN's own funds. Deploying simulation solutions to new markets is a challenging task. However, SIMPLAN has done that successfully with new solutions and new markets in the past. By experience, solutions like the one targeted with the THREAT-ARREST project will enable SIMPLAN to find 1-2 new customers per year with a potential of 100-200 k€ additional annual revenue equalling 1 or 2 additional workplaces.
Visualization [SIMPLAN]	TRL5	Jasima will be extended by visualization layers (Web, Mobile Device, Windows Client) for *THREAT-ARREST* based on existing technology but as required for presenting the outcomes of simulation/emulation of cyber system components in the project	TRL7	
		The visualization platform will include serious gaming elements in order to increase learning motivation for small and medium groups		
Emulation [UMIL]	TRL8	The capabilities of the emulation will be combined and expanded to achieve the automated generation and interconnection of emulated cyber system components. These components will be equipped with the appropriate	TRL8	Participation to THREAT-ARREST project will be exploited by UMIL/SESAR Lab to: (a) further establish itself as a major player in the security and trustworthiness of ICT, including IoT platforms and cloud infrastructures, starting new educational endeavours at postgraduate level; (b) use the project outcome to develop its activities at the doctoral levels, such as the French-Italian doctoral college on Secure Collaborative Knowledge Management co-organized with INSA; and (c) set up training sessions organized for security administrators

Tool / Partner	Current TRL	Advancements by THREAT-ARREST	Final TRL	Roadmap
		software stack, enabling the trainees to perform security mitigation tasks. The emulated tool of THREAT-ARREST will also select cyber system components and attacks based on CTTP models. (Final TRL: TRL7, the TRL of other capabilities of used tools will remain as is)		and skilled users in the framework of its program for continuing education. In addition, SESAR Lab at UMIL is a major technology transfer centre operating in conjunction with a number of European industrial partners in the context of cloud computing, and service/software assurance for embedded, telecommunication, and mobile systems. Based on these partnerships, UMIL regularly holds information days, workshop, and courses on emerging technologies and methodologies. UMIL will therefore be in a unique position to set–up a program of basic and advanced courses to complement the handbook in presenting THREAT-ARREST techniques and methodologies to engineers and designers working in the industry as well as in academia.
Data Fabrication (DFP) [IBM]	TRL6	To support the Threat-Arrest requirements, IBM Data Fabrication Platform is being enhanced with the ability to generate sequences of simulated cyber-events in general, and, in particular, synthetic security events log files.	TRL7	IBM research plans to exploit the outcomes of the Threat Arrest project internally to enhance the security and quality of IBM products and externally as part of the IBM security offerings or as a cloud service on any IBM platform. We will ensure that relevant IBM business units which are involved with developing the company's relevant products and services are aware of the technologies developed in the Threat Arrest project and will consider them for inclusion in products, as well as in factoring the project innovation into the overall IBM product strategy.
Security assurance [STS]	TRL6	Offering customizable security data analytics applied to data-at-rest and live, streaming data. The analytics and intelligence capability utilizes off-the-shelf hardware components coupled with custom software engine to provide a clear upgrade path, without vendor-specific lock-in. (Final TRL: TRL7). Development of mechanisms to support the connectivity and use of the platform as part of a cyber threat	TRL7	STS will use the outcomes of THREAT-ARREST for strengthening its service and product portfolio. STS plan is to augment the capabilities of its security assurance and certification platform in ways that will enable it to support the delivery of cyber security training programmes (e.g., providing monitoring and dynamic testing for CTTP models and programmes, establishing interoperability with emulation and simulation environments, etc.) and, therefore, be used as a tool for this purpose. From a technical perspective, the strategy of STS for achieving this exploitation route will be to develop mechanisms supporting the implementation of continuous assurance by executing the assurance sub model of CTTP models, and developing appropriate APIs for its platform to provide access to the monitoring/testing evidence and checks required as part of CTTP programmes. Another key enabler of this plan will be to make the STS platform interoperable

Tool / Partner	Current TRL	Advancements by THREAT-ARREST	Final TRL	Roadmap
		training framework. These will require mechanisms supporting the implementation of continuous assurance by executing the assurance sub model of CTTP models, APIs for monitoring/testing evidence and checks reporting etc.		with simulation and emulation tools that would enable it explore what-if scenarios in specifying assurance models. From a business perspective, STS's strategy will be to explore ways of making use of its platform as a training tool for security auditors and for increasing the security awareness of end-users and system administrators of cyber systems of private and public organisations in the healthcare and telecoms sectors which are the focus markets of the company. STS will also seek to develop consultancy services in setting up training programmes for establishing cyber security assurance assessment schemes, based on the outcomes of THREAT-ARREST.
FORTH				The results of the THREAT-ARREST project will be exploited by the established mechanisms of FORTH. Those include the PRAXI network5 and the Science and Technology Park of Crete (STEP-C). PRAXI Network is an established technology transfer organization with long-standing experience in assisting SMEs and research organisations throughout Greece. The other initiative of FORTH, the Science and Technology Park of Crete (STEP-C), offers, in addition to incubating facilities and services to start-up companies with new and emerging technologies, specialized professional services that are difficult to find under one roof and geared to assisting and guiding companies in various aspects such as transfer of technological advancements into the manufacturing of innovative products and services and unleashing their potential through innovation.
ATOS				THREAT-ARREST is in line with ATOS priorities. ATOS foresees different exploitation lines for THREAT-ARREST: Horizontal exploitation: positioning THREAT-ARREST outcomes within ATOS technology services offering. This has a two-pronged approach: i) the improvement of existing products in the Global Key offering (GKO) portfolio by incorporating partial results from THREAT-ARREST to existing solutions, or ii) by offering THREAT-ARREST as a standalone product based on the final platform. In particular, taking into account THREAT-ARREST advances in the field of serious gaming there are three lines to explore: the GKO on cyber-security, the Cyber Threat

Tool / Partner	Current TRL	Advancements by THREAT-ARREST	Final TRL	Roadmap
				Management Services within the Managed Services portfolio, and the Governance, Risk and Compliance (GRC) offering. Moreover, ATOS will exploit THREAT-ARREST results through strategic R&D&I consulting and Technology Watch, applying the latest research results to opportunities where clients need solutions that go beyond markets. Increased possibilities to undertake research and innovation projects, outreaching to key players in the innovation sector (research institutes, universities, etc.). ATOS Research & Innovation department (ARI) is the mechanism used by ATOS for R&D projects, technology transfer activities and inside-out promotion of technology. ARI counts with different IT Labs which leverage research activities in conjunction with robust partnerships or start-ups. THREAT-ARREST will be carried out by the ARI Cybersecurity Lab, which ensures a wide experience on security topics through its continuous investigation in THREAT-ARREST topics, before, during and after the project.
TUBS				In line with the strategy of TUBS to exploit research results, project THREAT- ARREST will serve as a multiplier by producing new technologies and exploiting synergies with other running projects. In particular, TUBS is already developing technology to allow vehicular and space platforms to undergo dynamic change in their software configurations without having to undergo verification, validation or certification (DFG Project CCC: Controlling Concurrent Change) as well as the H2020 project SHARCS which aims to further end-to-end security by developing mechanism that can operate at all levels of the execution stack. In both projects, the research effort concentrated on run-time policy enforcement, i.e. observing the behaviour of a software component and ensuring that it stays within its operational profile. The technologies that will be produced by THREAT-ARREST are complimentary to the SHARCS and CCC efforts and related research projects. Moreover, in cooperation with its technology transfer agency SympTA/S (SYMTAVISION), TUBS will transfer software prototypes into industrial practice. Other lines of exploitation reflect the educational nature of TUBS and foresee the application of SHARCS results for teaching

Tool / Partner	Current TRL	Advancements by THREAT-ARREST	Final TRL	Roadmap
				activities at TUBS, in terms of lectures, laboratories and disseminating results over scientific channels.
CZ.NIC				As a national CSIRT of the Czech Republic, CZ.NIC will integrate the project outputs into national awareness activities and cooperation. CSIRT.CZ is a leading national cybersecurity stakeholders' group with more than 100 members (government representative, critical information infrastructure protection operators, IT companies). In regard to the implementation of the NIS Directive, the project outputs should be specially targeted to the Digital Service Providers, who will be in the CSIRT.CZ constituency. Last but not least, project outputs should be used also within the Safer Internet project, especially for increasing cyber security maturity level of schools and other educational institutions and therefore to demonstrate the cooperation among H2020 and Connecting Europe Facility (CEF).
DANAOS				DANAOS, as a leading owner in container sea transportation, chartering out ships to major shipping liners will exploit on innovative solution of THREAT-ARREST in order to: (i) train and familiarize company's crew and personnel to potential cyber-threats that might face in everyday operational activities as well as the mitigation action to take; (ii) strengthen DANAOS security plan against these threats and assist company for the adoption of the ideal and most effective technology framework for protection and (iii) enhance DANAOS leading position and reputation in maritime trade by ensuring that charterers interests and data protection remains a priority.
LSE				LSE expects to get systematic assurance and possible certification for end-to-end security of its smart home monitoring system, usage defending systems for high-risk threats across its portfolio, specification of potential attacks which can be prevented via security control mechanisms and all the above could be used for internal training services for preparation against future cyber-attacks.
ARESS				ARES exploitation strategy of THREAT-ARREST results identifies two major exploitation objectives, to be achieved respectively in the short and medium term. The short-term exploitation objective, to be achieved during the project lifetime, consists in

Tool / Partner	Current TRL	Advancements by THREAT-ARREST	Final TRL	Roadmap
				carrying out the evaluation of cybersecurity training and simulation as part of an innovative security management model for healthcare. Setting up the training and simulation experiments for THREAT-ARREST in the healthcare sector will be an important step toward achieving this goal and will expand ARES scope to non-medical technologies like ICT for healthcare. The long-term exploitation objective consists in releasing a cybersecurity training approach customizable to different types of healthcare operators, based on THREAT-ARREST results and focused on the practical needs of healthcare sector in Apulia. This objective will be achieved in two steps. During the project lifetime, testing in collaboration with healthcare operators will allow to identify early adopters and build a success story. After the project end, guidelines and tools for the entire Apulian healthcare sector will be released and updated.
TÜV				TÜV HELLAS expects that, using the THREAT-ARREST "outcomes" (overall Framework / platforms and mainly the Training Platform) will enable them, as a Certification Body & Training Organization, to offer new, specialized Training Services within the CyberSecurity domain. Such specialized Auditors' Training & Evaluation services are anticipated to be of high demand in the immediate & near future, as they will satisfy the needs both of specialized technical training as well as of covering / satisfying the changing European Legislation landscape requirements (new NIS Directive, new GDPR Regulation etc.). The exploitation potential of TÜV HELLAS is significant, as the Company is part of the TÜV NORD group (a global technical services group, with core activities in Industrial Services, Mobility, Training, Natural Resources, Aerospace and IT, covering more than 70 Countries, with more than 14,000 Employees). TÜV HELLAS already possess a considerable experience in offering IT and IT security related Training services and has a strong presence in the South-Eastern Mediterranean region. Based on the above, there exists a strong potential for all TÜV NORD Group regions, with emphasis in EU market Countries.

Tool / Partner	Current TRL	Advancements by THREAT-ARREST	Final TRL	Roadmap
B&B				In the context of its work within the THREAT-ARREST project, B&B is able to keep abreast of the many legal and regulatory changes. It is also able to position itself on the legal market as a market leader by researching the most innovative legal issues and providing legal advice in relation thereto, with a practical and business mind. Not only does this provide to B&B a competitive advantage and enables it to position itself towards its international clients, but it also gives B&B the ability to showcase its first-hand knowledge and expertise and to get involved in EU policy making. Business development opportunities are expected by leveraging on the research results and the practical know-how gained during the project. This should hopefully allow enlarging B&B's current work in relation to its targets and reduce investments in relation to the research of novel legal issues. For instance, in relation to privacy, the research performed on the application of new obligations under the GDPR can be re-used in other contexts and for an array of targets in various sectors.

Commercialization Roadmap: Integrated Platform

As far as the ***Integrated THREAT-ARREST Platform*** is considered:
More specific plans will be deployed during the project, and as per the Consortium Partner's discussions / agreements on the total Business Model
A final product / solution "Commercialization path" will be drafted and followed
The "Commercialization path" will include:

- the *individual Partners'* plans (updates on the previous subsection's 0 data)
- a *collective strategy / path for the integrated product*

An integrated product commercialization path is in Figure 15.

Figure 15 Commercialization phases will start after the project's final deliverable - "Prototype Build" (TRL7) - phase 2 as above (31.8.2021).

Maximizing the project's overall impact

Measures to maximize the project's overall impact include and will be based on:

- an **External Advisory Board**. The External Advisory Board (EAB) is comprised by leaders of industry, standardization, and policy to ensure that *THREAT-ARREST* solutions not only address the requirements of the explored domains via the *THREAT-ARREST* pilots (maritime, health and energy) but also from other industrial sectors
- **Standardization Activities** *(see previous subsection 3.3.2)*
- designing, documenting and implementing detailed ***Dissemination & Exploitation Plans,*** in the context of WP8 (part of which is the present deliverable D8.3); see Table 23.

Table 23. Deliverables for the Work Package 8

Deliverable		Delivery Date
D8.1	Stakeholders' engagement plan and online channels development	M3 (*submitted)*
D8.2	THREAT-ARREST dissemination plan	M3 *(submitted)*
D8.3	THREAT-ARREST market analysis, business & marketing plan v.1	M12 *(present report)*
D8.4	Stakeholders' engagement & online channels report v.1	M18
D8.5	THREAT-ARREST dissemination and exploitation report v.1	M18
D8.6	THREAT-ARREST market analysis, business & marketing plan v.2	M30
D8.7	Stakeholders' engagement & online channels report v.2	M36
D8.8	THREAT-ARREST dissemination and exploitation report v.2	M36

3.4.8 PEST & SWOT Analysis

PEST & SWOT analysis are presented in Table 24 and

Table 25.

Table 24. PEST Analysis

Factor	Potential Benefit / Impact	THREAT-ARREST Strategy

Factor	Potential Benefit / Impact	THREAT-ARREST Strategy
Socio--Economic & Environmental	A probable future increase of budgeting / spending by European Governments & EU for training in cyber security, could lead to a further growth of the market for cybersecurity training platforms. This would especially concern the innovation proposition (model-driven, serious games, etc.) provided of the THREAT-ARREST platform, being able to address a larger group of potential users	Developing a successful prototype and successfully commercialize a final innovative & differentiated product on-time and in order to capitalize on the opportunities
	Economic crisis / market recession could force Companies / Organizations to reduce their budgets for training their employees on cybersecurity	This is the "opposite side" of the previous impact. Strategy remains the same (innovative / differentiated product-solution & services, well-thought-off pricing strategy)
Technological / Commercial	Awareness regarding the importance of cybersecurity has been increasing in large segments of EU users / citizens. An "easier" market acceptance of the THREAT-ARREST training platform by its Stakeholders / users could be expected.	Promote - emphasize the platform's innovative character (e.g. parts of trainings are implemented by serious games that enable trainees to obtain knowledge within a "pleasant" context)
	The platform's innovative model-based approach promotes a straight-forward and" holistic" reproduction of customer-specific training scenarios	The platform will be able to successfully "address" Customers / Organizations with more specific needs
	Interfacing / communication between the different components / tools of the THREAT-ARREST training platform will be implemented with open standards and technologies in a decoupled way.	Possible future "extensions" of the platform would be feasible - concentrate on assessing value / developing them
	The platform's gaming tools are browser-based and can be played on mobile devices. This will enable a playing of the games "on-the-go"	Concentrate to successfully address a wider training customers' base
	Competitor solutions that rely on their own IT infrastructure and have a bigger market presence / power could provide similar products at lower prices. This could lead to a stronger competitors' market position and potential THREAT-ARREST customers could prefer their offerings.	Concentrate on successfully developing and promoting the THREAT-ARREST's unique & innovative features. Concentrate on competitive product / solution offerings & pricing
	Existing competitive products on the market have a higher degree of maturity	Gain all possible "experience" and "maturity" form the project's real-life Pilot programmes, in order to "build maturity" into the commercial product

Factor	Potential Benefit / Impact	THREAT-ARREST Strategy
	Gap between research and market: when performing R&D on new technologies, it is often very difficult for the EU-based security industry to predict whether there will be, in the end, a final market uptake. While this is a widespread problem that can be found across many industrial sectors, it is particularly pertinent for the security industry, which is mostly "faced" with an institutional market.	A detailed commercialization "go-to-market" strategy will be further developed during the course of the project and will be implemented. A detailed Business Plan, including a market and competitive analysis as well as operational, financial, marketing, growth, and contingency plans has already been prepared and will be further improved during the course of the project. End users' feedback and findings during the validation of the platform in real operating conditions (during the pilots' execution) will also be taken into account. Additionally, THREAT-ARREST will pursue active involvement of all relevant stakeholder groups.
	Lack of engagement of relevant stakeholders may eliminate the prospect of building a sustainable cyber security strategy.	It is of utmost importance to ensure the involvement of relevant stakeholder groups. THREAT-ARREST aims to raise awareness and engagement through a number of initiatives, including among others pursuing synergies, organising showcases, workshops and campaigns, as well as other communication and dissemination activities.
Legal & Regulatory	The THREAT-ARREST platform has to "integrate & implement" the data protection laws of different countries (i.e. not only European - GDPR). This could make the platform's implementation more complex	Standardize the process of reviewing, coding and "embedding" all applicable legal / privacy requirements within the Product and related training services (a successful "privacy-by-design" principle)
	Similarly, THREAT-ARREST will have to take into consideration and "apply" country-specific (e.g. Germany) legislation relating to legal / ethical use of cybersecurity / training technical tools ("ethical hacking" scenario)	Similar strategy as above
	Changes in the legislative / regulative status in EU Countries could lead to "export controls" for cyber security tools like THREAT-ARREST	Watching closely and following-up on all related legislation / regulation developments
	Lack of interoperable solutions (technical standards) and practices (process standards) are affecting the single market in cyber security.	THREAT-ARREST will closely monitor all developments regarding (a) EU legislative / regulative context (b) relevant SDOs and as well as keep up with emerging technologies / risks, so as to ensure that (a) product development process complies with related standards and (b) any new requirements that may arise will be timely and effectively addressed.

Factor	Potential Benefit / Impact	THREAT-ARREST Strategy
	The highly fragmented nature of the EU security market, e.g. the lack of harmonized certification procedures and standards, has a negative impact on both the supply side (industry) and the demand side (public and private purchasers of security technologies), leads to barriers to market entry and makes true economies of scale very difficult.	THREAT-ARREST will pursue close collaboration and networking with all the Policy & Standards-producing Organizations / Bodies, both European and International *(see details in section 3.3.2)*

Table 25. SWOT Analysis

	Internal Analysis	
	Helpful for achievement of the goal	**Harmful** for achievement of the goal
Internal Analysis	**Strengths** • Model-based, innovative cybersecurity training platform approach • Can address different cybersecurity services segments / needs (cyber range, gamification, testbed) • Provision of trainings services / scenarios for niche ("specific needs") markets • Adaptability to the training needs / scenarios of varied domains / market segments • Gaming tools are browser-based and can be played on mobile devices "on-the-way", while requiring no complex introduction and no trainee gaming / info security background	**Weaknesses** • The "Funding / adequate Resources" theme, regarding a successful commercialization • Potential Platform Integration issues (comprises many separate tools & technologies) • Potential IP / Licensing issues for the commercial product (many Partners involved)
External Analysis	**Opportunities** • Rapidly expanding cybersecurity training services market • Increasing market & users' awareness of the value of cybersecurity platform-based training • Evolving EU cybersecurity "Products & People "Certification context	**Threats** • Competition by similar products / solutions already established in market / "easily" available. • Competitors with greater market power develop similar products with a higher degree of maturity and for a lower price. • "Next-generation" / more sophisticated competitive Products of established competitors (e.g. utilizing AI or ML) • Standardization issues

3.5 Sales / Costs / P&L / Resources / Funding

3.5.1 Market Size Estimation

THREAT-ARREST and related services offerings can address several segments of the Cybersecurity services industry *(see previous sections 3.4.1 and 3.4.2).* Nevertheless, it is not feasible, at this point of the project, to accurately estimate specific market segments sizes and related THREAT-ARREST targets in terms of market share. Bellow can be found data regarding *overall* markets size estimation:

(a) independent market reports estimate the Global Cybersecurity market size at 167 Bn. $ for year 2019 (MarketsandMarkets / TC 3485, Sep.2018) – see Figure 16.

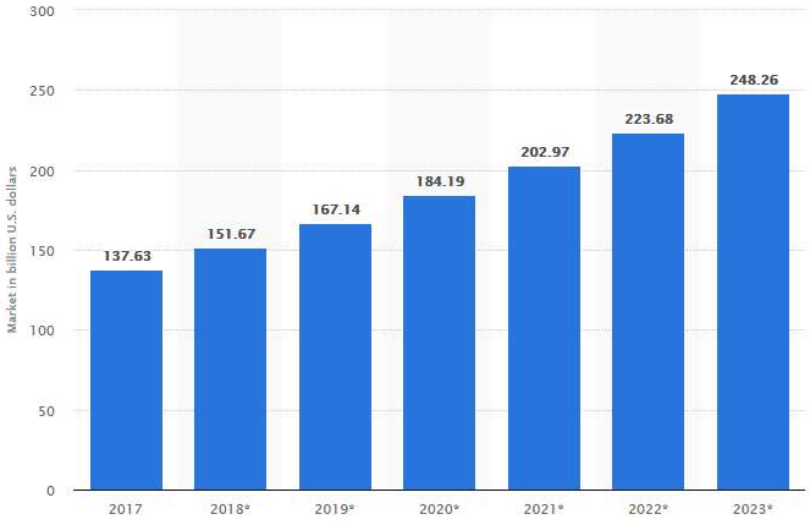

Figure 16. Global Cybersecurity Market size (MarketsandMarkets / TC 3485, Sep.2018)

(b) according to Gartner (Gartner, 2018), worldwide spending on information security products and services was more than $114 billion in 2018, an increase of 12.4 percent from 2017. For 2019, Gartner estimates that the market will grow 8.7 percent to $124 billion. It is important her to stretch that it is estimated that the ***cybersecurity services*** sector is estimated to represent at least 50% of the total market.

(c) "cybersecurity ventures" (cybersecurityventures / St. Morgan, 10.2019) estimates that, between 2017 and 2021, more than $1 trillion will have been cumulatively spent on cyber security products and services.

(d) ECSO / CIMA Analysis (ECSO - EUNITY, 24.1.19) estimates an average 17% increase in cybersecurity "sales" annually. The European market is estimated at 25% of the Global market

(e) all above market reports agree on the size of the Cybersecurity Training & Education sub-market, which is estimated at 3.5 Bn. $ (with the European equivalent market estimated between 0.5 and 0.83 Bn. $ - 2018-year estimates - and at an average annual grow between 5 and 8%). Figure 17 below shows the European Cybersecurity Market (ECSO - EUNITY, 24.1.19). It can be seen that, yet, the "Training& Education" sub-segment occupies a small overall share.

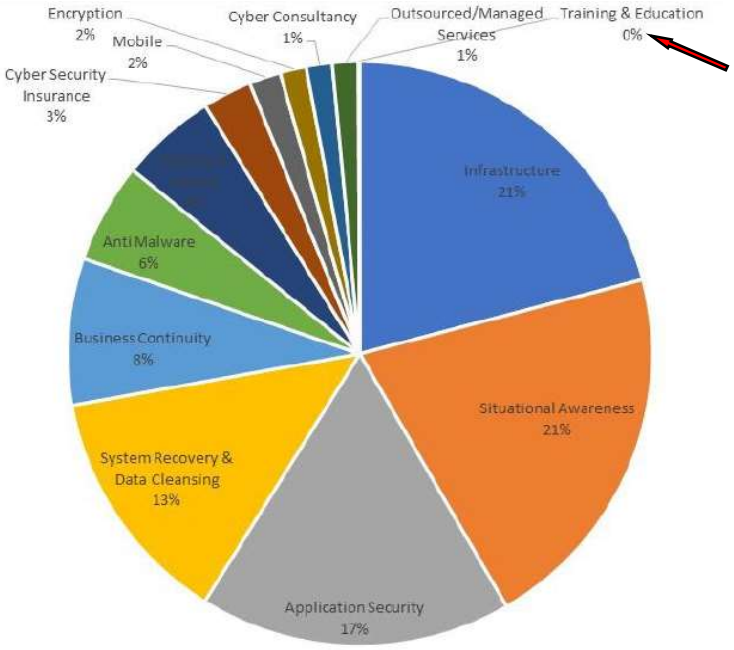

Figure 17. European Cybersecurity Market break-down

Figure 18 below shows the Global & European Cybersecurity training & education market sub-segment sizes and trends (MarketsandMarkets / TC 3485, Sep.2018)

Market potential

49% of the organization plan to spend more on Training (EY information security survey 2016).

Cyber security Training and education market size by Region, 2014-2019 ($Billion)

Region	2014	2015	2016	2017	2018	2019	CAGR (2014-2016)
NorthAm	1.13	1.19	1.27	1.35	1.44	1.55	6.4%
EU	0.69	0.71	0.75	0.78	0.83	0.89	5.2%
APAC	0.47	0.52	0.57	0.64	0.72	0.82	12%
EMEA	0.19	0.21	0.24	0.26	0.30	0.34	11.6%
LatAm	0.15	0.17	0.19	0.22	0.25	0.30	15.4%
Total	2.63	2.80	3.01	3.25	3.55	3.90	8.2%

Source: *MarketsandMarkets Analysis*

Figure 18. Global Cybersecurity-Training Market potential

(f) Figure 19 below shows market positioning related to the Security-Awareness Computer-Based Training Market (Gartner / KnowBe4, 2019):

Figure 19. Magic Quadrant for Security-Awareness Training Providers (Gartner / KnowBe4, 2019)

(g) Table 26 below presents a projection of the ***cybersecurity training*** markets size (2021-2025 period), based on all previously shown market reports data:

Table 26. Cybersecurity training markets size projection (2021-2025)

Market size (*Bn. €*) →	**2021**	**2022**	**2023**	**2024**	**2025**
Market segment					
Global Security ***Training & Education*** Market (avg. annual growth 8 %)	4.5	5	5.4	5.8	6.3
European Security ***Training & Education*** Market (avg. annual growth 5%)	1	1.05	1.1	1.15	1.2

However, above estimations/projections contain uncertainty, and the market size could finally be increasing much more rapidly during the 2021-2025 period. For instance, Gartner (Gartner, 5.3.18) predicts that, by 2022, 15% of large enterprises will be using cyber ranges to develop the skills of their security teams, up from less than 1% in 2018. If we take the number of large enterprises (LEs) in the EU-28 area – estimated at 46,500 (EU, Nov.2018) - we can come up to a projection that, by 2020, a pool of around 6,000 large European enterprises will need cyber range services – an impressive figure that will be further elaborated during the course of the project.

3.5.2 Costs & Pricing structure

The THREAT-ARREST final Costing / Pricing will be based on the corresponding final Business Model. Please note that, at this point of the project, exact data is not provided as it would, at this stage, be purely based on rough estimates - essential figures like total cost of ownership (TCO), etc. are still unknown.

According to the current Business Model *(see subsection 3.4.5 on Business Canvas)*, THREAT-ARREST incurred costs to operate the business model include costs for the:

- ✓ deployment in IT / Infrastructure management
- ✓ SW / tools / Platform development and maintenance
- ✓ Staff wages / salaries
- ✓ Marketing / promotion expenses
- ✓ Financial expenses

Table 27 below presents possible costing scenarios (PwC, 2015).

Table 27. Costing scenarios

Business Model	Cost-Driven DTC (Bottom-Line Growth)	Value-Driven DTV (Top-Line Growth)	DTC + DTV "in parallel"
Cost Structure Attributes			
Fixed Costs	☑	☑	☑
Variable Costs	☑	☑	☑
Focus on *costs / service value optimization*	☑		☑
Focus on *Premium service value / personalized service proposition*		☑	☑
Economies of *scale*	☑	☑	☑
Economies of *scope*	☑	☑	☑

3.5.3 Sales – P&L - ROI projections

At this point of the project, such projections are not possible with an acceptable degree of accuracy.
Figures and best estimates on P&L data, Return On Investment (ROI), net-present value (NPV) and alike will be provided during the project within the final exploitation and innovation phase / plans.

3.5.4 Resources/Funding

Similarly, it is considered as too early at this point to define/design final product market positioning and related Resourcing/Funding schemes and amounts.

4 Marketing Strategy

Marketing term describes *any activity that involves the creation and sharing of media and publishing content in order to acquire and retain customers*. Moreover, the methodological approach to the communication activities considers three cumulative levels of activity, which incrementally increase both the proximity to the audience and the depth of information (see Table 28).

Table 28. Levels of communication activity

Category	Purpose
INFORM	Raise a basic level of awareness of the project's goals, team and activities, and convey a general understanding of the purpose and benefits of the action.
ENLIGHTEN	Answer in detail key questions about the project's activities, its methodologies, the timing of its milestone and its results.
ENGAGE	Involve the audience in the project's activities and maintain awareness over the course of the project (and beyond). This could take the form of a simple subscription to the project's newsletter, interactive but asynchronous means such as questionnaires, or fully-fledged person-to-person interaction such as inviting participation in workshops, focus groups or other project events. From a commercial perspective, engagement entails the development of a customer-supplier relationship and is usually termed customer retention.

Each communication action will be aimed at reaching one or more of the above levels across the different audiences, through the tools, channels and activities detailed in the Deliverable *D8.1 The THREAT-ARREST Dissemination Plan* (THREAT-ARREST consortium/ D8.2, 2018) and the Deliverable *D8.2 The stakeholders' engagement plan & online channels development* (THREAT-ARREST consortium/ D8.1, 2018). Dissemination and Communication activities are aimed mainly at Informing and Enlightening the target audiences, whilst Marketing has the end goal of Engaging audiences. Thus, the project marketing addresses the objective of **identifying and engaging with potential future customers** of the THREAT-ARREST services.

4.1 Overall Strategy

The marketing approach followed by THREAT-ARREST is directly linked to the communication activities but also to the dissemination and exploitation ones. Marketing, treated as a special case of the communication effort, is aimed at the target consumers of the THREAT-ARREST services and designed specifically to create a convincing case for the THREAT-ARREST services' **viability**, **competitiveness**, and **added-value** with respect to the alternatives available on the market, to engage and retain customers, and thereby ultimately to generate revenue.

THREAT-ARREST needs to move from **being a project to a commercial service**, and the communication, dissemination and marketing activities should reflect this. The aim of the THREAT-ARREST platform is to deliver security training, based on a model driven approach where cyber threat and training preparation (CTTP) models. As with the launch of any new product or service onto the market, a strategic approach governing its presentation to the outside world is required. Such an approach relies on a **solid understanding of the target audiences and the objectives of the communications** aimed at them. Consequently, the approach to communication must be **tailored** to take advantage of their specificities for

maximum effect; **selected messages** must be delivered using the **correct means**, and the **timing** of communication activities should be designed for maximum impact.
Hence, the marketing strategy of the THREAT-ARREST project targets to a variety of stakeholders that can be interested in the THREAT-ARREST platform. These stakeholders will be approached using a variety of **channels** (including online media and traditional formats) and also by exploiting the usage of two different Content Marketing types (STRATEGIC consortium, 2017), **Outbound Marketing** and **Inbound marketing**.
Outbound Marketing or *Interruption* marketing is a pejorative term that refers to promoting a product through continued advertising, promotions, public relations and sales.
Inbound Marketing is the promoting a company or a product through blogs, webinars, video, blogs, newsletters, whitepapers, Search Engine Optimization (SEO), physical products, social media marketing, and other forms of content marketing which serve to attract customers through the different stages of the purchase funnel. Inbound Marketing is about "potential customers seeking you out, rather than you are chasing them down" (EvidenceN, 2019).
During the project duration, THREAT-ARREST invested on mostly on *inbound marketing* by creating or distributing content that customers want to read, view or listen. The key messages in any marketing campaign will be centred around the particular benefits offered by THREAT-ARREST to public bodies, businesses and citizens, in response to certain business or societal objectives. Thus, the THREAT-ARREST marketing campaign will be initially based on traditional channels, such as newspaper, advertisements, television commercials, web page, social media, webinars, blogs, banners, etc. Additionally, more target-oriented marketing paths, like advertisements in branch publications and participation in events, exhibitions and conferences, will be adopted.

4.2 Dissemination

As mentioned above, Dissemination and Communication activities are aimed mainly at **Informing and Enlightening the target audiences**. Hence, awareness raising, and knowledge diffusion are listed as priorities for THREAT-ARREST dissemination strategic approach. More specifically, the purpose of *THREAT-ARREST's* dissemination efforts will be to influence stakeholders' view, so that they will become aware of the project's new ideas, services and results, and ultimately adopt it.
Three categories of dissemination channels (online dissemination, scientific publications and organization of international scientific events) will be established, as defined in the Deliverable D8.1. This combined approach ensures efficient dissemination of the technical activities of THREAT-ARREST based on the target audience's needs and involvement (THREAT-ARREST consortium/ D8.2, 2018) .
The THREAT-ARREST dissemination approach will be implemented at both the consortium and individual partners' level and will target all possible stakeholders, whereas it will be conceptually divided in two phases, based on the project's results.

1. During the early stage of the project, where solid results will not be yet available, THREAT-ARREST will follow a content related dissemination approach, employing various dissemination channels and material for communicating messages to the identified stakeholder groups.
2. The second phase will be based more on a result-oriented approach, where emphasis will be put in the outputs of the THREAT-ARREST project, and dissemination and communication will be more focused in the actual outcomes of the project.

All dissemination channels and metrics to measure the impact are detailed in the deliverables D8.1 and D8.2 ((THREAT-ARREST consortium/ D8.1, 2018), (THREAT-ARREST consortium/ D8.2, 2018)).

4.3 Communication

Communication is meant to be a dynamic, rather than static process for showing the objectives of the project and to attract the attention of further relevant actors. As such, it is meant to take into account the various opportunities, as well as the profile of the targeted stakeholders. To this end, the consortium has established and retained mechanisms for getting feedback from the latter and will utilize this feedback to regularly review and update the communication strategy on the basis of the stakeholders' needs and requirements. Moreover, the consortium will constantly refine the strategy, according to the progress of the project, to focus on efficiently promoting and communicating the results at each stage and on progressively building buzz around the **THREAT-ARREST** offering. This way, communication activities will be fine-tuned or modified in response to changing situations and to the needs of the stakeholders targeted.

All communication channels and metrics to measure the impact are detailed in the Deliverables D8.1 and D8.2 ((THREAT-ARREST consortium/ D8.1, 2018), (THREAT-ARREST consortium/ D8.2, 2018)).

4.4 "Go-to-Market" Strategy

The main target is to **advertise the benefits offered by THREAT-ARREST**. To start, the development of a **brand identity** should begin early, and continuity should be evident in the shift from project-based to commercial activities. This brand identify reflects the content and purpose of the THREAT-ARREST services, following the market research activities to be carried out under the exploitation task of WP8. A complete graphic identity to communicate the main concepts of the THREAT-ARREST project has been designed. This simple, useful and consistent graphic identity helps the consortium to communicate the project messages more effectively and is the base for communicating towards the outside world. Graphic identity involves the use of logos, type fonts and colours to create an image easy to recognize by the audience. All material that will be developed will follow this graphical identify. Consistent graphic identities allow the target audience to easily identify and recognize the THREAT-ARREST project. For this reason, it is essential that all material distributed by the project partners maintain the project's identity.

A second underlying topic concerns the question of **partnerships**. This inevitably ties together with the work to be undertaken under the exploitation task of WP8 but should also be examined in the context of its impact on the communication activities. The commercial services of THREAT-ARREST could gain a great deal from being offered as part of a partnership with an existing commercial provider of similar or complementary services. The options need to be identified and fully fleshed out before a coherent strategy can be constructed around them, but this issue is considered strategically important for the success of the communication strategy as a whole.

A third major strategic issue is **regionalisation**. The THREAT-ARREST project is geared towards targeting three pilot scenarios in different countries, and promotional and communication materials will be translated into the local languages by project partners and customised in each case to highlight the specific benefits to stakeholders in the respective countries. The pilot partners will have a direct role in acquiring local 'intelligence' in order to inform the most effective strategies for communication and marketing.

5 Conclusions

This deliverable ("D8.3 – The THREAT-ARREST market analysis, business and marketing plan v.1"), being the first output of the task "T8.2 – Sustainability management and Business continuity", presented the first iteration of the THREAT-ARREST market analysis, business and marketing plan. As such, the deliverable presented aspects such as the training needs and costs, the current landscape of the relevant market, future developments, products and services, the business plan and business model, and overall market strategy.

The above were analysed based on the current knowledge and the limitations (considering the early implementation phase of the project) of the consortium. As the implementation progresses and a minimum viable product can be presented to stakeholders and potential end users, the plan will be revised to more accurately depict the needs and targeting of the THREAT-ARREST platform at the end of the project.

Therefore, this first version of the market analysis, business and marketing plan of the project will be updated as the project matures; the result of this process will be presented in the final version of this deliverable, i.e. in deliverable "D8.6 – The THREAT-ARREST market analysis, business and marketing plan v.2", which is due in M30.

6 References

[1] Airbus, 2019. *Cyber Incident Games.* [Online]
Available at: https://airbus-cyber-security.com/products-and-services/consultancy/cyber-incident-games/#scroll1

[2] AIT Austrian Institute of Technology GmbH, 2019. *PHISHING WARS.* [Online]
Available at: https://spielengegenphishing.tech-experience.at/#

[3] Alexandris, G., et al., 2018. Blockchains as enablers for auditing cooperative circular economy networks. 23rd IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD 2018), IEEE, Barcelona, Spain, 17-19 September 2018, pp. 1-7.

[4] Arizona Cyber Warfare Range, n.d. *Arizona Cyber Warfare Range.* [Online]
Available at: https://www.azcwr.org

[5] Avatao, 2019. *Avatao.* [Online]
Available at: https://avatao.com

[6] BBC News, 2019. *Ukraine hacks 'could happen to UK'.* [Online]
Available at: http://www.bbc.com/news/technology-35686493

[7] Beckers, Kristian et. al, 2019. *THREAT-ARREST serious games v1,* s.l.: s.n.

[8] Benzel, T., 2011. *The Science of Cyber-Security Experimentation: The DETER Project.* Orlando,Florida, Annual Computer Security Applications Conference (ACSAC '11).

[9] BeOne Development, 2019. *Security Awareness Training in the Context of Everyday Working Activities.* [Online]
Available at: https://www.beonedevelopment.com/en/security-awareness

[10] Bls.gov, 2019. *Information Security Analysts : Occupational Outlook Handbook: : U.S. Bureau of Labor Statistics.* [Online]
Available at: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

[11] CFTP, 2019. *CFTP.* [Online]
Available at: https://ctf365.com

[12] CIRCADENCE/ Circadence Wins Silver Award for inCyt from International Serious Play Awards Competition, 2019. *Circadence Wins Silver Award for inCyt from International Serious Play Awards Competition.* [Online]
Available at: https://www.prlog.org/12780007-circadence-wins-silver-award-for-incyt-from-international-serious-play-awards-competition.html

[13] CIRCADENCE, 2019. *inCyt.* [Online]
Available at: https://www.circadence.com/products/inCyt

[14] Community, M. N. S., n.d. [Online]
Available at: https://www.merit.edu/cyberrange/

[15] Corpin, G.C.M. et al., 2018. *(23) Internet Security Threat Report.* [Online]
Available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

[16] Cyber Security Challenge UK, 2019. *Cyber City.* [Online]
Available at: https://www.cybergamesuk.com/

[17] Cyberbit, 2016. *Cybershield Training and Simulation, Live training for cyber-security professionals.* [Online]
Available at: https://www.cyberbit.com/wp-content/uploads/2016/09/CB-TnS-Print.pdf

[18] CyberBit, 2016. *www.cyberbit.com.* [Online]
Available at: https://www.cyberbit.com/wp-content/uploads/2016/09/CB-TnS-Print.pdf

[19] Cybercrime Magazine, 2018. *Cybersecurity Jobs Report 2018-2021.* [Online]
Available at: https://cybersecurityventures.com/jobs/

[20] Cybersecurity.isaca.org, 2019. *CSX Training Platform.* [Online]
Available at: https://cybersecurity.isaca.org/csx-certifications/csx-training-platform

[21] cybersecurityventures / St. Morgan, 10.2019. *htpps://cybersecurityventures.com.* [Online]
Available at: htpps://cybersecurityventures.com/cybersecurity-market-report

[22] Dark Reading, 2019. *The 7 Best Social Engineering Attacks Ever.* [Online]
Available at: http://www.darkreading.com/the-7-best-social-engineering-attacks-ever/d/d-id/1319411?_mc=RSS_DR_EDT&piddl_msgorder=&image_number=3

[23] Davis, J. & Magrath, S., 2013. *A survey of Cyber Ranges and Testbeds,* Australian Government Department of Defence: Cyber and Electronic Warfare Division Defence Science and Technology Organisation.

[24] Davis, J. & Magrath, S., 2013. *A Survey of Cyber Ranges and Testbeds,* s.l.: s.n.

[25] De Montfort University Partnered with the Michigan Cyber Security Center (MCC) , 2017. *Standing up a Cyber Range Capability in Michigan Centre for Secure Computing (CSC),* s.l.: s.n.

[26] Dogana Project, 2019. *DOGANA at Bluff City 2018. How to assess Social Engineering 2.0 attacks using SDVAs.* [Online]
Available at: https://www.dogana-project.eu/

[27] ECSO - EUNITY, 24.1.19. *CIMA 2019 / Cybersecurity Industry Analysis (ECSO EUNITY Workshop),* s.l.: LSEC / ECSO.

[28] ECSO - European Cyber Security Organisation, 2019. *ECSO - European Cyber Security Organisation.* [Online]
Available at: https://www.ecs-org.eu/

[29] ECSO, June 2016. *ECSO – SRIA for a contractual Public-Private Partnership (cPPP),* s.l.: ECSO.

[30] ECSO-WG3 / G. Rizzo, 10.10.18. *European Cybersecurity cPPP and ECSO,* s.l.: ECSO.

[31] ECSO-WG5, Nov.2018. *ECSO – WG5: Information & CyberSecurity Professional Certification (EHR4CYBER),* s.l.: s.n.

[32] Emulab.net, 2019. *Emulab.Net - Emulab.* [Online]
Available at: http://www.emulab.net

[33] ENISA / Dr. F.Di Franco, Dec.2018. *ENISA recommendations – Analysis of the European R&D priorities in cybersecurity,* s.l.: ENISA.

[34] ENISA / Dr. Steve Purser, 21.1.19. *"ENISA in the EU Cybersecurity Certification Framework" - Cybersecurity Standardization Conference – Brussels 21.1.2019),* s.l.: s.n.

[35] ENISA/ Cyber Europe programme, 2019. *Cyber Europe programme.* [Online]
Available at: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme

[36] ENISA, 2017. *Handbook on Security of Personal Data Processing.* [Online]
Available at: https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

[37] ENISA, 2019. *A Users' Guide: How to Raise Information Security Awareness.* [Online]
Available at:
https://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/A%20Users%20Guide%20How%20to%20Raise%20Information%20Security%20Awareness.pdf

[38] ENISA, Dec.2017. *ENISA - Priorities for EU research – Analysis of ECSO's SRIA,* s.l.: s.n.

[39] ENISA, Dec.2018. *ENISA: "Guidance and Gaps analysis for European Sstandardization",* s.l.: s.n.

[40] ERMProject/ Recall, 2019. *Recall.* [Online]
Available at: https://ermprotect.com/security-awareness-training/course-library/

[41] ERMProject/ Recall, 2019. *Recall.* [Online]
Available at: https://ermprotect.com/security-awareness-training/course-library/

[42] ERMProtect/ Jump, 2019. *Jump.* [Online]
Available at: https://ermprotect.com/security-awareness-training/course-library/

[43] ERMProtect/ Match, 2019. *Match.* [Online]
Available at: https://ermprotect.com/security-awareness-training/course-library/

[44] ERMProtect/ Trivia, 2019. *Trivia.* [Online]
Available at: https://ermprotect.com/security-awareness-training/course-library/

[45] ESET, 2019. *ESET.* [Online]
Available at: https://www.eset.com/us/about/newsroom/

[46] EU / L.Probst et.al., 10.2015. *New Business Models - Freemium,* s.l.: EU.

[47] EU Cybersecurity Act, 2019. *EU Cybersecurity Act - Regulation (EU) 2019/881 (https://eur-lex.europa.eu/eli/reg/2019/881/oj),* s.l.: s.n.

[48] EU, 2017. *REGULATION (EU) No 1303/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.* [Online]
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32013R1303&from=EN

[49] EU, Nov.2018. *European Union report: "Annual Report on European SMEs 2017/2018",* s.l.: EU.

[50] European IPR HelpDesk / J. Scherer, 17.4.18. *The Basics of successful IP management in H2020,* s.l.: European IPR HelpDesk.

[51] European IPR HelpDesk, 2015. *How to manage IP in H2020: Project implementation & conclusion,* s.l.: European IPR HelpDesk.

[52] European IPR HelpDesk, 2019. *Your Guide to IP Commercialization,* s.l.: European IPR HelpDesk.

[53] EvidenceN, 2019. *What Is Digital Marketing.* [Online]
Available at: https://evidencen.com/what-is-digital-marketing/#.XTXO8vIzbDc

[54] Faber, T. & Wroclawski, T., 2009. *A Federated Experiment Environment for Emulab-based Testbeds.* s.l., Tridentcom.

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

[56] Gartner / KnowBe4, 2019. *https://info.knowbe4.com.* [Online]
Available at: https://info.knowbe4.com/gartner-magic-quadrant-security-awareness-cbt-partner

[57] Gartner, 2018. *www.gartner.com.* [Online]
Available at: www.gartner.com/newsroom/press-release/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019

[58] Gartner, 5.3.18. *https://www.gartner.com.* [Online]
Available at: Boost Resilience and Deliver Digital Dexterity With Cyber Ranges"
https://www.gartner.com/doc/reprints?__hstc=260811986.a32de8aca956d48d6f8186d84ff7f166.1565937063723.1565937063724.1565937063724.1&__hssc=260811986.4.1565937063729&id=1-6QJJ8DH&c

[59] General Data Protection Regulation, G., 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[60] Gürtler, M., 2012. *NATO Cooperative Cyber Defence Centre of Excellence.* [Online]
Available at: https://www.enisa.europa.eu/events/cyber-exercise-conference/presentations/7.%20Conf%20Paris%20-June%202012%20-%20-%20M.%20GURTLER%20-NATO-CCDCOE.pdf

[61] H2020 portalgate / reporting on Actions & Proposals, 2019. *https://webgate.ec.europa.eu/dashboard/hub/stream/aaec8d41-5201-43ab-809f-3063750dfafd.* [Online].

[62] Hatzivasilis, G., et al., 2019a. MobileTrust: Secure Knowledge Integration in VANETs. ACM Transactions on Cyber-Physical Systems – Special Issue on User-Centric Security and Safety for Cyber-Physical Systems, ACM, vol. 4, issue 3, Article no. 33, pp. 1-15.

[63] Hatzivasilis, G., et al., 2019b. The CE-IoT Framework for Green ICT Organizations. 1st International Workshop on Smart Circular Economy (SmaCE), Santorini Island, Greece, 30 May 2019, IEEE, pp. 1-7..

[64] HBR / V.Kumar, 2014. *https://hbr.org.* [Online]
Available at: https://hbr.org/2014/05/making-freemium-work

[65] IBM, 2019. *Cost of a Data Breach Study.* [Online]
Available at: https://www.ibm.com/security/data-breach

[66] IMO, 2019. *STCW Convention.* [Online]
Available at:
http://www.imo.org/en/OurWork/HumanElement/TrainingCertification/Pages/STCW-Convention.aspx

[67] IS Decisions, 2019. *THE WEAKEST LINK.* [Online]
Available at: https://www.isdecisions.com/user-security-awareness-game/

[68] ISO/ ISO9001, 2015. *ISO 9001:2015.* [Online]
Available at: https://www.iso.org/standard/62085.html

[69] ISO, 2013. *ISO/IEC 27001:2013.* [Online]
Available at: https://www.iso.org/standard/54534.html

[70] ISO, 2015. *ISO 9001:2015.* [Online]
Available at: https://www.iso.org/standard/62085.html

[71] ITU, 2018. *Cybersecurity Ecosystem (https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2018/05_Kiev/ITU%20Seminar%2015.05.18%20-%20Oleksandr%20Potii.pdf),* s.l.: ITU.

[72] Kaspersky Lab, 2015. *Kaspersky ASAP: Automated Security Awareness Platform Efficiency and ease of management for organizations of any size,* s.l.: s.n.

[73] Kaspersky Lab, 2018. *Kaspersky Interactive Protection Simulation An effective way of building cybersecurity awareness among top managers and decision makers,* s.l.: s.n.

[74] Kaspersky, 2019. *Kaspersky.com.* [Online]
Available at: https://www.kaspersky.com/

[75] Kolias, C., Kambourakis, G., Stavrou, A. & Voas, J., 2017. DDoS in the IoT: Mirai and other botnets. *Computer,* Volume 50, pp. 80-84.

[76] Mair, C., 2012. *Openness, Intellectual Property and Standardization in the European ICT Sector.* s.l.:Maurer School of Law.

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

[78] MarketsandMarkets / TC 3485, Sep.2018. *www.marketsandmarkets.com.* [Online] Available at: https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html

[79] Mirkovic, J. et al., 2010. *The DETER Project: Advancing the Science of Cyber Security Experimentation and Test.* Waltham, Massachusetts, 2010 IEEE International Conference on Technologies for Homeland Security (HST '10).

[80] Mundo Alguacil, A. et al., 2018. *McAfee Labs Threats Report.* [Online] Available at: https: //www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf

[81] National Cyber Range, T. r. M. C. D. o. D., 2015. *National Cyber Range, Test resource Management Center, Department of Defense.* [Online] Available at: https://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf

[82] NISD, 2016. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[83] NIST Cyber Security Professional (NCSP), 2019. *APMG International.* [Online] Available at: https://apmg-international.com/product/nist-cyber-security-professional-ncsp

[84] NIST, 1998. *NIST SP 800-16 Information Technology Security Training Requirements: a Role- and Performance-Based Model, National Institute of Standards and Technology,* s.l.: s.n.

[85] NIST, 2003. *NIST SP 800-50 Building an Information Technology Security Awareness and Training Program, National Institute of Standards and Technology,* s.l.: s.n.

[86] Nsa.gov, 2019. *National Centers of Academic Excellence.* [Online] Available at: https://www.nsa.gov/resources/students-educators/centers-academic-excellence/

[87] OECD , 2019. *Licensing of IP rights & Competition Law_note by EU (DAF/COMPWD(2019)52,* s.l.: OECD.

[88] OpenAIRE, 2019. *OpenAIRE.* [Online] Available at: https://www.openaire.eu

[89] Opendoar.org, 2019. *Directory of Open Access Repositories - v2.sherpa.* [Online] Available at: http://www.opendoar.org

[90] Pinecone Cyber, n.d. *Cyber Range and Cyber Testing - Cyber Range.* [Online] Available at: https://www.pinecone-cyber.com/index.php/solutions/security-solutions/cyber-range-and-cyber-testing/137-cyber-range-and-cyber-testing

[91] Police Executive Research Forum, 2014. *The Role of Local Law Enforcement Agencies In Preventing and Investigating Cybercrime,* https://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf: s.n.

[92] PwC, 2015. *Strategic Product Value Management,* s.l.: PwC.

[93] PwC, 2019. *Game of Threats.* [Online] Available at: https://www.pwc.co.uk/issues/cyber-security-data-privacy/services/game-of-threats.html

[94] Raj, A., Alangot, B., Prabhu, S. & Achuthan, K., 2016. *Scalable and Lightweight CTF Infrastructures Using Application Containers.* Austin, TX, 2016 USENIX Workshop on Advances in Security Education (ASE 16).

[95] Roar.eprints.org, 2019. *Welcome to the Registry of Open Access Repositories - Registry of Open Access Repositories.* [Online] Available at: http://roar.eprints.org

[96] Rossey, L., 2015. Panel: Cyber Experimentation of the Future (CEF): Catalyzing a New Generation of Experimental Cybersecurity Research. *SimSpace Cyber Range,* Issue ACSAC.

[97] Sans.org, 2019. *SANS Institute: Reading Room - Analyst Papers.* [Online] Available at: https://www.sans.org/reading-room/whitepapers/analyst/membership/34615

[98] SANS, 2019. *NetWars.* [Online] Available at: https://www.sans.org/netwars/

[99] Schwab, S., Wilson, B., Ko, C. & Hussain, A., 2007. SEER: a security experimentation EnviRonment for DETER. In: *Proceedings of the DETER Community Workshop on Cyber Security Experimentation and Test on DETER Community Workshop on Cyber Security Experimentation and Test 2007.* Boston, MA: s.n., pp. 2-2.

[100] SECTRICITY, 2019. *Security Awareness Training Games.* [Online] Available at: https://sectricity.com/en/security-awareness-en/security-awareness-training-games/

[101] securitymagazine / K.Bergelt, 10.4.19. *www.securitymagazine.com.* [Online] Available at: https://www.securitymagazine.com/articles/90106-cybersecurity-innovation-and-the-patent-landscape

[102] Shred-it, 2019. *Shred-it Study Exposes Employee Negligence | Shred-it United State.* [Online] Available at: https://www.shredit.com/en-us/about/press-room/press-releases/sacking-employees-for-data-breach-negligence

[103] Siaterlis, S., Genge, B. & Hohenadel , M., 2013. EPIC, A testbed for scientifically rigorous cyber-physical security experimentation. In: s.l.:IEEE Transactions on Emerging Topics in Computing, p. 319–330.

[104] Siponen, M., Seppo, P. & Mahmood, M., 2014. "Employees' adherence to information security policies: An exploratory field study. *Information & management,* Volume 51, pp. 217-224 .

[105] Solivan, D., 2015. *Communications-Electronics Command cyber training range launches.* [Online]
Available at:
https://www.army.mil/article/150996/communications_electronics_command_cyber_training_range_launches

[106] Soultatos, O., et al., 2019. Pattern-Driven Security, Privacy, Dependability and Interoperability Management of IoT Environments. 24th IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD 2019), IEEE, Limassol, Cyprus, 11-13 September 2019, pp. 1-6.

[107] STRATEGIC consortium, 2017. *D8.3b_SustainabilityBusiness Marketing and Financial Plans_v1.1,* s.l.: s.n.

[108] SURF, 2019. *ELEVATOR.* [Online]
Available at: https://www.elevatorgame.nl/en

[109] Test resource Management Center, D. o. D., 2019. *National Cyber Range Overview.* [Online]
Available at: https://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf

[110] Testbed, E., 2019. *Emulab Testbed.* [Online]
Available at: http://www.emulab.net

[111] Thales, 2018. *Awareness through play: DOGANA cards game.* [Online]
Available at: https://www.dogana-project.eu/index.php/social-engineering-blog/11-social-engineering/90-cardsgame

[112] THREAT-ARREST consortium/ D8.1, 2018. *D8.1 The stakeholders' engagement plan & online channels development,* s.l.: s.n.

[113] THREAT-ARREST consortium/ D8.2, 2018. *D8.2 The THREAT-ARREST dissemination plan,* s.l.: s.n.

[114] THREAT-ARREST Consortium, 2017. *THREAT-ARREST proposal,* s.l.: s.n.

[115] THREAT-ARREST Consortium, 28.2.2019. *Deliverable D1.3 (Platform's initial reference architecture),* s.l.: s.n.

[116] Trend Micro, 2019. *The Fugle.* [Online]
Available at: http://targetedattacks.trendmicro.com/about-the-game.html

[117] US Department of Commerce, 2017. *National initiative for Cybersecurity Education, Cyber Ranges, National Institute of Standards and Technology (NIST),* s.l.: s.n.

[118] VMWare / D.Hohndel, 13.12.17. *www.vmware.com.* [Online]
Available at: https://www.vmware.com/radius/2018-predictions-five-things-watch-open-source/

[119] VSTEP Simulation/ NAUTIS, 2019. *NAUTIS Maritime Simulator - VSTEP Simulation.* [Online]
Available at: https://www.vstepsimulation.com/nautis-simulator/nautis-maritime-simulator/

[120] VSTEP Simulation/ RescueSim, 2019. *RescueSim Advanced Fire Fighting Simulators for Greece - VSTEP Simulation.* [Online]
Available at: https://www.vstepsimulation.com/rs-news/rescuesim-advanced-fire-fighting-simulators-for-greece/

[121] VSTEP Simulation, 2019. *VSTEP Simulation.* [Online]
Available at: https://www.vstepsimulation.com/

[122] Vykopal, J. et al., 2017. *KYPO Cyber Range: Design and Use Cases.* s.l., ICSOFT.

[123] Weiss, R., Turbak, F., Mache, J. & Locasto, M. E., 2017. Cybersecurity education and assessment in EDURange. In: s.l.:IEEE Security & Privac, pp. 90-95.

[124] White, B. et al., 2002. An Integrated Experimental Environment for Distributed Systems and Networks. *ACM SIGOPS Operating Systems Review,* SI(ACM), pp. 255-270.

[125] Whitman, M. & Mattord, H., 2011. *Principles of Information Security.* [Online]
Available at: http://bedford-computing.co.uk/learning/wp-content/uploads/2016/08/Principles-of-Information-Security-4th-ed.-Michael-E.-Whitman.pdf

[126] Wroclawski, J., Mirkovic, J., Faber, S. & Schwab, S., 2008. *A Two-Constraint Approach to Risky Cybersecurity Experiment Management.* s.l., Invited paper at the Sarnoff Symposium.

[127] X-Force Command Cyber Tactical Operations Center, 2019. *Ibm.com.* [Online]
Available at: https://www.ibm.com/security/services/managed-security-services/xforce-command-cyber-tactical-operations-center

[128] XLPro Training Solutions, 2019. *Information security game INFOSEC.* [Online]
Available at: https://playxlpro.com/portfolio1/games/html/infosec/

[129] Yousuf, T., Mahmoud, R., Aloul, F. & Zualkernan, I., 2015. Internet of Things (IoT) Security: Current status, challenges and countermeasures. *International Journal for Information Security Research (IJISR),* Volume 5, pp. 608-616.