



City Research Online

City, University of London Institutional Repository

Citation: Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Hildebrandt, T., Tsakirakis, G., Oikonomou, F., Leftheriotis, G. & et al (2020). Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. *Applied Sciences*, 10(16), 5702. doi: 10.3390/app10165702

This is the published version of the paper.

This version of the publication may differ from the final published version.

Permanent repository link: <https://openaccess.city.ac.uk/id/eprint/25035/>

Link to published version: <https://doi.org/10.3390/app10165702>

Copyright: City Research Online aims to make research outputs of City, University of London available to a wider audience. Copyright and Moral Rights remain with the author(s) and/or copyright holders. URLs from City Research Online may be freely distributed and linked to.

Reuse: Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

City Research Online:

<http://openaccess.city.ac.uk/>

publications@city.ac.uk

Article

Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees

George Hatzivasilis ^{1,2,*}, Sotiris Ioannidis ^{1,3}, Michail Smyrlis ^{4,5}, George Spanoudakis ⁵, Fulvio Frati ⁶, Ludger Goeke ⁷, Torsten Hildebrandt ⁸, George Tsakirakis ⁹, Fotis Oikonomou ¹⁰, George Leftheriotis ¹¹ and Hristo Koshutanski ¹²

¹ Foundation for Research and Technology–Hellas, Institute of Computer Science, Vassilika Vouton, 70013 Heraklion, Greece; sotiris@ics.forth.gr

² Department of Electrical and Computer Engineering, Hellenic Mediterranean University (HMU), Estavromenos, 71410 Heraklion, Greece

³ Department of Electrical and Computer Engineering, Technical University of Crete, 73100 Chania, Greece

⁴ Innovation Department, Sphynx Technology Solutions AG, 6300 Zug, Switzerland; smyrlis@sphynx.ch

⁵ Research Centre for Adaptive Computing Systems (CeNACS), City, University of London, London EC1V 0HB, UK; g.e.spanoudakis@city.ac.uk

⁶ Department of Computer Science, University of Milan, 20122 Milano, Italy; fulvio.frati@unimi.it

⁷ Innovation Department, Social Engineering Academy, 60322 Frankfurt, Germany; ludger.goeke@social-engineering.academy

⁸ Research Department, SimPlan, 63452 Hanau, Germany; torsten.hildebrandt@simplan.de

⁹ Research and Development Department, ITML, 11525 Athens GR, Greece; gtsa@itml.gr

¹⁰ Applied Research Department, DANAOS Shipping Company, Limassol CY 3300, Cyprus; drc@danaos.com

¹¹ Systems Certification Department, TUV HELLAS (TUV NORD) SA, 15562 Athens GR, Greece; glefthe@tuv-nord.com

¹² Research Department, ATOS SPAIN SA, 28037 Madrid, Spain; hristo.koshutanski@atos.net

* Correspondence: hatzivas@ics.forth.gr or hatzivas@hmu.gr; Tel.: +30-2810-391600

Received: 6 July 2020; Accepted: 13 August 2020; Published: 17 August 2020



Abstract: Nowadays, more-and-more cyber-security training is emerging as an essential process for the lifelong personnel education in organizations, especially for those which operate critical infrastructures. This is due to security breaches on popular services that become publicly known and raise people's security awareness. Except from large organizations, small-to-medium enterprises and individuals need to keep their knowledge on the related topics up-to-date as a means to protect their business operation or to obtain professional skills. Therefore, the potential target-group may range from simple users, who require basic knowledge on the current threat landscape and how to operate the related defense mechanisms, to security experts, who require hands-on experience in responding to security incidents. This high diversity makes training and certification quite a challenging task. This study combines pedagogical practices and cyber-security modelling in an attempt to support dynamically adaptive training procedures. The training programme is initially tailored to the trainee's needs, promoting the continuous adaptation to his/her performance afterwards. As the trainee accomplishes the basic evaluation tasks, the assessment starts involving more advanced features that demand a higher level of understanding. The overall method is integrated in a modern cyber-ranges platform, and a pilot training programme for smart shipping employees is presented.

Keywords: cyber-ranges; security training; security modelling; serious games; dynamic adaptation; training programmes; computers in education; bloom; STRIDE; smart shipping

1. Introduction

The 4th Industrial Revolution brings the Information Society to the foreground. Every day, highly interconnected systems, utilizing not just the ordinary computer technologies but also the Internet of Things (IoT) and the cloud, exchange high volumes of data and user-related information [1,2]. This complex ecosystem cannot be safeguarded easily, as the attack surface is continuously increasing, while the security of the deployed primitives is not always retained [3–5]. Therefore, successful attacks have been demonstrated by researchers or have been actually performed by hackers, exploiting the underlying vulnerabilities (e.g., [6,7]). The risk still remains high, not only for large organizations, but for small-to-medium enterprises (SMEs) and individuals as well.

As a human is generally considered the weakest link in a computer system, professional training is now becoming a necessity [8,9], not only for raising the users' awareness but also for training the technical staff to operate the various protection mechanisms that must be acquired (e.g., cryptographic protocols, intrusion detection/prevention systems, machine learning and artificially intelligent modules, digital forensics, etc.). Gartner estimates that the global cyber-security awareness and training market will worth around USD 1.5 billion by 2021 [10].

Except from the related academic education that is mainly designed for computer science students, professional programmes are gaining more and more ground, ranging from introductory short courses for non-security persons to highly specialized certifications for security experts. The means to offer such training include (e.g., [11–19]): traditional in-class teaching, on-line training platforms and virtual labs, as well as modern cyber-ranges frameworks that mirror an actual system and provide hands-on experience to the trainee under realistic operational conditions. However, in most cases, these modules target a specific subset of the potential beneficiaries and their educational flexibility is limited. Moreover, the training programmes are designed by technical personnel, who, in most cases, are not aware of the mainstream pedagogical principles. This is a general characteristic of lifelong education that focuses on adult professionals.

In this paper, we try to tackle this issue by combining pedagogical methods that promote skill development and security models that capture the security-related aspects of a process. More specifically, based on the Bloom's taxonomy [20], we categorized the level of difficulty and knowledge maturity that is required in order to learn the underlying training modules for a programme, and based on the Microsoft's STRIDE model [21], we map all these modules in terms of the security aspects that they involve. At first, the trainer organizes the educational content and the learning process for a professional cyber-security certification, by mapping the learning objectives and the training methods with the Constructive Alignment [22] framework. Then, the trainee consumes the teaching material and is continuously evaluated. The assessment starts from the knowledge base and the easiest layers of the Bloom's taxonomy, and if the user is successful, he/she can proceed to the upper layers and the advanced training procedures. The Kolb's learning lifecycle [23] is iteratively performed until the student masters the involved teaching material and accomplishes the learning objectives. The training is finished when the trainee has reached a specific level of understanding for the examined security properties that are included in the STRIDE analysis of this certification. The proposed method is deployed in the THREAT-ARREST cyber-ranges platform [24] as part of the overall trainee and training programme assessment.

The rest paper is organized as: Section 2 refers the related work and the background theory. Section 3 sketches the proposed methodology for the design and evaluation of the cyber-security training programme. Section 4 details the process for establishing a programme for the personnel of a smart shipping company and a preliminary implementation in the THREAT-ARREST cyber-ranges platform. Section 5 summarizes a discussion concerning modern aspects of cyber-security training. Finally, Section 6 concludes and refers future extensions.

2. Materials and Methods

2.1. Modern Cyber-Security Training Platforms

Nowadays, a high variety of research and commercial platforms is available for cyber-security training for both individuals and organizations. A comparison of them with our method is presented in Table 1 and is detailed in [24].

Table 1. Cyber-security training platforms: (A) THREAT-ARREST, (B) BeOne, (C) Kaspersky, (D) ISACA CSX, (E) CyberBit, (F) online training platforms. The following notations are utilized for (Y)es, (N)o, and (P)artial.

Feature	A	B	C	D	E	F
Automatic security vulnerability analysis of a pilot system	Y	N	N	N	N	N
Multi-layer modelling	Y	P	Y	Y	Y	P
Continuous security assurance	Y	N	N	Y	Y	N
Serious gaming	Y	N	Y	Y	N	P
Realistic simulation of cyber systems	Y	P	Y	Y	Y	N
Combination of emulated and real equipment	Y	N	P	Y	N	N
Programme runtime evaluation	Y	N	N	Y	Y	Y
Programme runtime adaptation	Y	N	Y	Y	N	P

Usually, most of the general-purpose e-learning platforms (e.g., Coursera (Mountain View, CA, USA, 2012–2020), Udacity (Mountain View, CA, USA, 2011–2020), edX (MA, USA, 2012–2020), etc.) offer introductory and main educational courses on cyber-security. On the other hand, specialized solutions, such as the SANS (Bethesda, MD, USA, 2000–2020) [11], CyberInternAcademy (MO, USA, 2017–2020) [12], StationX (London, UK, 1996–2020) [13], Cybrary (College Park, MD, USA, 2016–2020) [14], and AwareGO (Reykjavik, Iceland, 2011–2020) [15], support more advance and focused training. In most cases, all these approaches target individuals whose goal is to develop/sharpen new skills. However, they fail to provide hands-on experience on real systems or even cyber-ranges. Modern cyber-ranges platforms, such as BeOne (Hilversum, The Netherlands, 2013–2020) [16], ISACA’s CyberSecurity Nexus (CSX) (Rolling Meadows, IL, USA, 1967–2020) [17], Kaspersky (Moscow, Russia, 1997–2020) [18], and CyberBit (Raanana, Israel, 2019–2020) [19], offer more advance features.

THREAT-ARREST combines all modern training aspects of serious gaming [25,26], emulation and simulation in a concrete manner [27], and offers continuous security assurance and programme adaptation based on the trainee’s performance and skills (Table 1). The platform [24] offers training on known and/or new advanced cyber-attack scenarios, taking different types of action against them, including: preparedness, detection and analysis, incident response, and post incident response actions. The THREAT-ARREST platform supports the use of security testing, monitoring and assessment tools at different layers in the implementation stack, including:

- Network layer tools (e.g., intrusion detection systems, firewalls, honeypots/honeynet);
- Infrastructure layer tools (e.g., security monitors, passive and active penetration testing tools (e.g., configuration testing, SSL/TLS testing);
- Application layer tools (e.g., security monitors, code analysis, as well as passive and active penetration testing tools such as authentication testing, database testing, session management testing, data validation and injection testing).

The procedure begins by analyzing the organization’s system. The Assurance Tool [28] evaluates the current security level and reports the most significant security issues that must drive the following training process. Then, hybrid training programmes are produced, and tailored to the organizational needs and the trainee types. This includes the main training material along with serious games, as well as the simulation and emulation of the cyber range system. THREAT-ARREST also provides continuous evaluation of: (a) the performance of individual trainees in specific training programmes;

and (b) the effectiveness of training programmes across sub-groups of trainees or the entire organization. These evaluations are used to tailor programmes to the needs of individual trainees or alter them at a more macroscopic level.

The whole operation is defined under a methodology called “Cyber Threat and Training Preparation (CTTP) modelling” [24], which determines the learning goals of a training programme, the learning path of the trainee, as well as how to drive the on-demand instantiation of the virtual labs with the advance cyber-ranges features for these programmes and assess the trainee’s actions automatically.

This article documents this latest characteristic of the THREAT-ARREST platform and the CTTP modelling concept (see Sections 2.3 and 3). Moreover, the scope of a CTTP programme can be aligned with cyber-security professional specialization programmes, e.g., from ISACA or ISC². Therefore, the dynamic adaptation of the training process and the continuous improvement and building of skills constitutes a novel and competitive feature of the THREAT-ARREST solution.

2.2. Teaching Cyber-Security

Surveys concerning cyber-security exercises are reported in [29–31]. ISO-22398 [32] is the international standard that defines several exercise methodologies, such as seminars, simulations, workshops, tabletops and serious games, capture the flag (CTF), red/blue team, etc. These techniques provide hands-on experience to trainees and can assist the development of technical skills. The educational process may involve serious games, simulation with virtual labs, and/or collaboration learning. Although the importance of pedagogical aspects in exercises is recognized in the literature [33], it has not been adequately studied and covered by researchers and practitioners, respectively [33].

To support effectual training, one has to understand how expertise is built and which educational approaches can improve the trainee’s performance [29]. Ordinarily, skills’ development and behavioral learning start with lecture-oriented teaching. As the trainee’s knowledgeable capacity increases, his/her “cognitive learning” is enhanced. Then, deeper knowledge on the subject can be built, by moving to “constructivist learning” approaches that mostly utilize exploratory learning [34,35] (react to learning as a researcher) and problem-based learning [36] (begin by resolving an actual problem and examining the relevant background information). Studies on university students [37] reveal that reaching a high-order of thinking and understanding becomes critical and of great importance in the cyber-security field. Although students successfully complete a relevant course and know (cognitive learning) the main concepts, they usually incorrectly reason about the application of core notions (constructivist learning), such as the differences between confidentiality/integrity or authentication/authorization.

Ericsson defined a well-established Deliberate Practice (DP) theory [38] for the continuous skills’ improvement. Thereupon, students require well-specialized goals that improve a specific area of expertise in their field, while on the other hand, they are “not benefitting by tasks which can be completed in an automated fashion”. The full achievements of the DP approach can be accomplished when the trainee reaches the highest layers on the Miller’s pyramid [39]—an educational method for assessing the trainee’s competence based on four levels of: “Knows”, “Knows how”, “Shows how”, and “Does”. Cyber Security Exercises (CSEs) [40] is a novel educational methodology for cyber-security that combines the aforementioned pedagogical approaches. An exercise is defined in three phases of: (i) planning the scope and objectives, (ii) implementation, and (iii) evaluation/feedback. This also complies with the relevant phases defined by the MITRE corporation [41] (exercise planning, exercise execution, and post exercise). At the planning stage, the trainer identifies the scope of the exercise, the involved security aspects, and the pedagogical methods, as well as which elements will be simulated during the exercise and the scenario steps. During the implementation stage, the trainer monitors the students and tries to handle events and incidents, driving the students to pass through all learning goals. The process is based on the Boyd’s Observe-Orient-Decide-Act (OODA) loop [42]. In the feedback stage, the students and the trainer go through all the main exercise elements. This is the most

valuable phase for the individuals as they can ask questions on the underlying concepts, which will hopefully lead to the achievement of the defined learning objectives.

The study in [43] indicates that students can reach competence in cyber-security only via hands-on learning with virtual labs led by an instructor. Therefore, a proper training programme must incorporate a series of good content and tutor interaction, pedagogical framework, and essential virtualized exercises for hands-on interplay. In [44], researchers propose a technology-enhanced pedagogical framework for training with virtual labs. The process starts by applying the Constructive Alignment [22] (map intended learning outcomes with deployed teaching activities) for the design of the curriculum. The learning follows the Kolb's experiential learning cycle [23] (disassembled in four subsequent phases of learning for "Concrete Experience", "Reflective Observation", "Abstract Conceptualization", and "Active Experimentation") and the educational elements are categorized based on the Bloom's Taxonomy [45] (method for the classification of learning objectives into levels of complexity and specificity). Collaborative learning may also be supported for team work. The students are evaluated via on-line quizzes and discussion boards.

Several studies also examine the inclusion of modern gamification techniques in the learning process [46,47]. The implication of serious games is generally considered positive, as the trainee can become familiarized with the involved topics in a more relaxed manner, even in his/her free time.

Another aspect that is usually neglected in cyber-security training programmes is "psychology". This affects both the attacker and the threat model—motivation to devote effort and launch an attack; and the legitimate user-communication/team-working skills, tendency to ignore warnings or defined procedures, etc. These issues are examined in [48]. The "age, sex, or cultural background may make a person more subjectable to some malicious behavior". Thus, despite their familiarization with technology, young people may be at greater risk of being tricked by phishing emails than older ones. Moreover, "different type of trainees has diverse expectations" from a cyber-security course. For instance, computer science students are mostly interested on how an attack can be performed, while psychology students focus more on why someone would exploit a vulnerability and harm a system or a person, and general public may be concerned about the side-effects of a successful hit.

Other challenging issues [49,50] include: (i) the "dynamicity" of the Computer Science, (ii) the "workforce needs" and the requirement for industry standards, and (iii) a "common taxonomy" for threats and the underlying security properties. A modern curriculum design methodology must be able to easily align in the continuous evolving Computer Science and cyber-security fields [49]. Moreover, training programmes should cover the current threat landscape and potentially lead to a professional certification [50]. A common vocabulary across all these aspects must be followed by a well-established programme or body of programmes [50].

The THREAT-ARREST platform supports a model-driven operation based on a methodology called CTTP modelling, which administrates the whole training process. At first, experts examine a piloting system (i.e., for smart shipping, healthcare, and smart energy) and record its main components, user types, etc. The core CTTP sub-model defines how a digital twin of this system can be instantiated on the developed Emulation and Simulation tools. Thereupon, the experts also apply the STRIDE threat model [21] in order to capture the current security status of the piloting system, including the potential threats, vulnerabilities, and the proper deployment of the required defense mechanisms. This information is also part of the core sub-model (a well-structured XML or JSON format [28]) and offers a common and widely-used vocabulary across the whole training experience.

Based on the analysis outcomes, we identify the most critical security aspects for the examined organization and tailor a training programme to its needs. The training perspectives are recorded in the training sub-model. This includes the learning objectives for each trainee type and the organization as a whole, as well as the dynamic adaptation and skill development features that are presented in this article (Sections 3 and 4).

The trainer defines complete training programmes with ordinary training material (e.g., lectures, tutorials, etc.), serious games, and virtual labs (emulated and simulated scenarios). The learning

path for a programme is consisted by a series of CTTP models. Each model defines which of these modules will be activated and their correlation with the learning objectives (Constructive Alignment). The model-driven approach enables us to provide a high variety of CTTP models where different scenarios of escalated difficulty are activated based on the trainee’s type, expectations, and performance. The variations of a model are mapped in the Bloom’s taxonomy. The trainee begins the training by building the basis of the cognitive learning and then proceeding to constructivist learning and high-order thinking. Multi-user CTTP models are also supported (i.e., red/blue team and advance CTF scenarios), offering also collaborative learning opportunities. Thus, the successful learning of a security (or other) topic is performed in several iterations based on the Kolb’s learning cycle. Moreover, the programmes curriculum can correlated with professional specification bodies, such as those from ISACA and ISC², and learning outcomes of the models and the programme as a whole are mapped based on the Constructive Alignment methodology.

2.3. The Building-Blocks of the THREAT-ARREST Cyber-Security Training Framework

The operation of the THREAT-ARREST cyber-ranges platform is driven by the CTTP models. In this subsection, we briefly introduce the CTTP-modelling features and how we establish a training programme. More details can be found in [24].

2.3.1. CTTP Modelling

The THREAT-ARREST modelling approach is consisted of four main stages (see Figure 1): (i) analysis of a pilot system, (ii) establishment of the training programme, (iii) training and user feedback, and (iv) post-training monitoring and security evaluation.

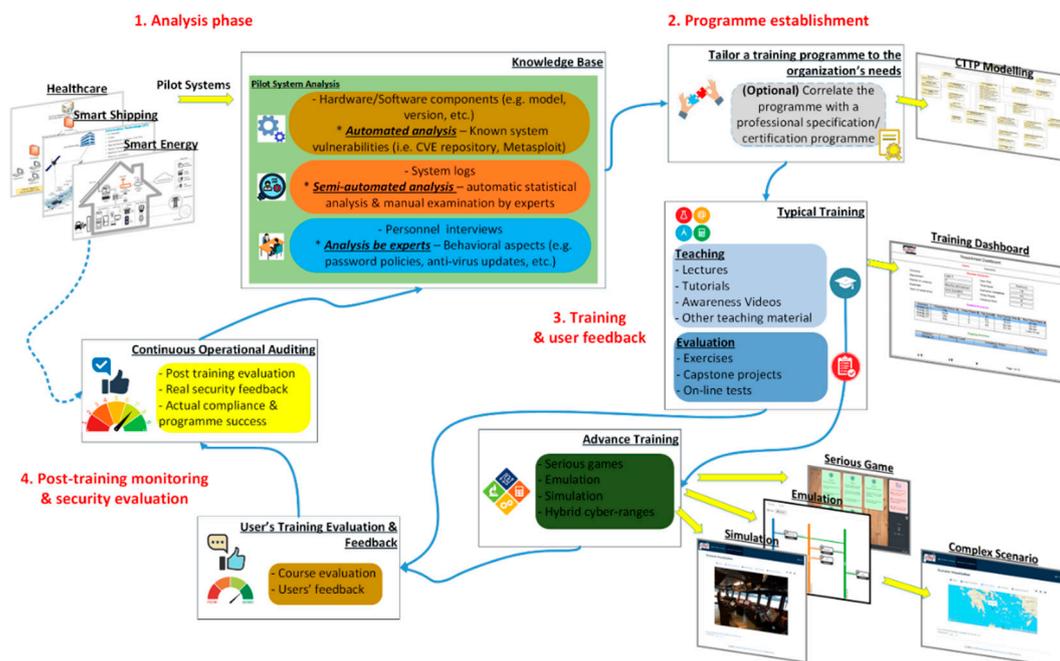


Figure 1. The THREAT-ARREST lifecycle.

Initial Analysis of a Pilot System

At first, we analyze the customer organization system based on the STRIDE method and build the knowledge base for the training programme. The goal is to estimate the current security status and identify the weak points (e.g., system or behavioral vulnerabilities). The platform’s Assurance Tool [28] deploys monitoring modules in the piloting system that disclose its technical features (such as the type and version of the running software or the installed hardware components) and check if it operates

securely. Then, it searches to widely-known security repositories (i.e., CVE) and automatically discovers the active vulnerabilities of the system (e.g., if a server uses MS SQL 5.5.35, then it is vulnerable to buffer overflow attacks based on the CVE-2014-0001). The vulnerabilities set is assessed in a semi-automated fashion by the experts, who identify the most significant of them for the evaluated organization. Based on this information, we define the core assurance sub-model.

Experts also interview the organizations personnel and record the followed operational procedures (e.g., password-update policy, anti-virus updates, etc.). The training programme is designed afterwards based on the overall outcomes of this initial analysis.

Moreover, during this phase, the experts gather real-operational log or other data files from the piloting system. This knowledge is further processed in order to enhance the advance training procedures of the THREAT-ARREST platform. At first, we perform statistical analysis on the original data to disclose the statistical patterns of each file. This is performed either through manual examination by experts or via an automatic statistical analysis module. The goal is to produce synthetic events (i.e., a series with legitimate and/or phishing emails) or other data (i.e., a database's content with dummy but realistic entries) via our Data Fabrication Tool that will be later used in order to provide advance training under realistic conditions.

CTTP Programme Establishment

Then, based on the initial analysis results, we tailor a CTTP programme to the organization's special needs, which could also be combined and cover the training for a professional certification programme (e.g., Certified Information Security Manager (CISM) by ISACA or Certified Information Systems Security Professional (CISSP) by ISC²), in order to increase the THREAT-ARREST's efficiency. Therefore, we define the main parameters of the "Training Programme", such as the programme's goals, actuators, trainee rules, etc.

Afterwards, we gather the relevant teaching material for the typical training (e.g., lectures, tutorials, awareness videos, etc.) and model the advance training scenarios based on "simulation sub-model", "emulation sub-model", and "gamification sub-model", as well as the "data fabrication sub-model" for the required synthetic data. The resulted training ingredients and exercises are classified based on the Bloom's taxonomy. Henceforth, we can map the desired security learning outcomes of the STRIDE modelling with the developed training elements, based on the Constructive Alignment [22] technique.

Training and User Feedback

Once the trainee has completed the basic training for a learning unit, the accompanied CTTP models are activated in the Dashboard and the trainee can now proceed with the advanced training. The CTTP models describe a virtual system and how to instantiate it via the Emulation, Simulation, and Gamification Tools, respectively.

These virtual labs and digital twins, which could resemble the organization's actual system and followed procedures, offer hands-on experience to the trainees/personnel. Thus, they can test and evaluate new technologies and policies, break-down the system, restore the default state and start over again, without affecting the actual system. The trainees begin the programme, consume the teaching material and are assessed against the desired learning goals. The CTTP models can be adjusted dynamically at runtime in order to be adapted to each individual trainee's needs. The goal is to continuously adapting the difficulty level throughout the various iterations of the games and virtual labs and the phases of the Kolb's lifecycle.

After the completion of the training, the platform displays the results for each trainee and the programme as a whole. This process indicates the scores of the trained personnel and their achievements regarding the educational processes. Discussion sessions can follow in collaboration with the trainers in order to revise the main learning topics and explain potential open issues or unresolved tasks to the trainees. Finally, the trainees can also complete questionnaires and provide feedback to

the THREAT-ARREST operator, e.g., for the platform modules, the programme, etc., in order to update and improve our system. All these could form ordinary characteristics of a training platform.

Post-Training Monitoring and Security Evaluation

However, the successful completion of a programme does not always reflect to the improvement of the pilot organization's security in a straightforward manner. The security level is increased only when the trainees apply what they have learnt in the actual system. The evaluation of this phase is one of the THREAT-ARREST's novelties in comparison with other alternative solutions.

Thus, our platform continues to audit the pilot system for a determined period after the training phases. The deployed controls from the initial phase (Section 2.3.1) continuously assure the organization's security-sensitive components. The goal is to capture if the trainees really applied what they were toughed.

For example, in the analysis phases we discover that the trainees do not update their email passwords in a regular basis, i.e., by examining the log-file of the mailing server (assurance sub-model). Thus, we tailor a programme to include the learning topic of password management (Training Programme and simulation, emulation, gamification, and data fabrication sub-models). When the programme is finished, we inspect the server's log and check if the password-update entries have been increased or not.

The confirmation that the personnel adheres with the learned features, and thus the system's security is really improved, constitutes the actual validation that the programme was successful. This process is facilitated by the Assurance Tool and the relevant model. Feedback is collected from this phase in order to improve the THREAT-ARREST's operation for future training iterations and new programmes.

3. Results

3.1. Modelling of the Learning Process

This section presents the main educational and pedagogical aspects of the proposed framework. This includes the incorporation of the STRIDE threat model for the analyses of the cyber-security aspects that are involved in the programme, the Bloom's taxonomy for the classification of the learning elements, the Kolb's learning lifecycle, and the Constructive Alignment, along with the integration of these methods in the cyber-ranges platform THREAT-ARREST [24]. In this article, we extend the CTPP models and embody the aforementioned methods in our training framework. The goal is to enrich the overall model-driven approach in an attempt to accomplish continuous and dynamic adaptation of the training process to the trainee's particularities and enhance the skills' development operations.

3.1.1. Security Modelling

During the initial analysis phase of the THREAT-ARREST lifecycle (Section 2.3.1), we analyze the piloting environment based on the STRIDE methodology [21]. STRIDE is a widely-known security model for defining threats, which was designed by Microsoft. The name is the abbreviation of the six threat categories that it analyzes: (i) Spoofing, (ii) Tampering, (iii) Repudiation, (iv) Information disclosure, (v) Denial of Service (DoS), and (vi) Elevation of privilege. Each of one of them reflects a potential violation of a desired security property in the system, i.e., authentication, integrity, non-repudiation, confidentiality, availability, and authorization, respectively. Figure 2 depicts this mapping between threats and security goals.

The threat model assesses the detailed system design. Data-flow diagrams (DFDs) identify the involved entities, events, and the boundaries of the system. The model has been successfully applied to cyber-only and cyber-physical environments. While Microsoft no longer maintains STRIDE, the model is part of the Microsoft Security Development Lifecycle (SDL) and implemented within the Threat Modeling Tool, which is still available.

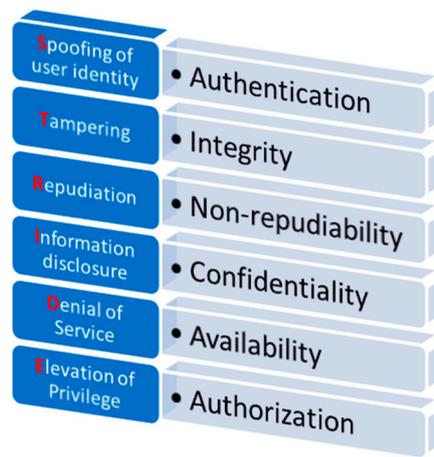


Figure 2. The STRIDE threat model.

Today, there are several threat modelling techniques [51], including Attack Tress, Security Cards, the MITRE ATT&CK framework, etc. STRIDE is a mnemonic method that focuses on assets. We choose this primitive as it can be easily understood and applied by a trainer during the design of the training programme and the underlying training procedures, correlating also threats with respective defensive countermeasures.

3.1.2. Training Programme Preparation

Training programmes are established during the second THREAT-ARREST modelling phase (Section 2.3.1). At first the trainer must design the lifecycle for a training programme. The preparation of the learning procedure is important and resolves the problem of teaching a learning topic in the determined time limits of the programme. The trainer can sketch the learning evolution and becomes more confident in the class (or virtual class). Problematic issues are foreseen and avoided while the timely preparation helps in saving time and reveals the potentials of the educational content.

Learning is a cyclic process and involves the four Kolb’s stages [23]. At first, the trainee based on his/her knowledge and experience faces new problems, takes decisions, acts, and applies what he/she has learnt in practice. Then, the trainee proceeds, copes with real conditions and acquires new experiences. The gained experiences are examined via several perspectives, the results are processed, their significance is understood, and conclusions are drawn. Finally, these experiences are grouped, linked to scientific data and/or theoretic approaches, general principles are drawn, and action guidelines are formed. These phases are repeated in a cyclic manner, as they are depicted in Figure 3.

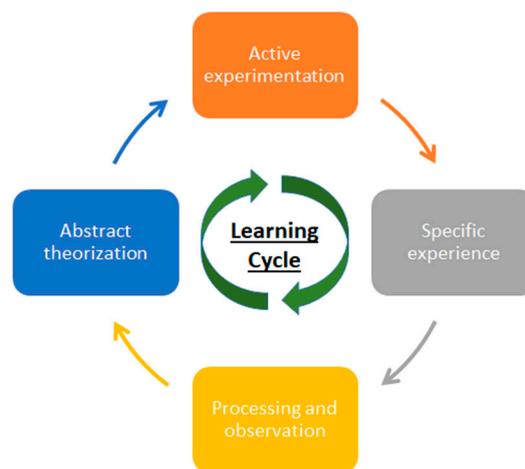


Figure 3. The 4 phases of the learning cycle.

The trainee's evaluation has to be continuous, systematic, methodic, pedagogical, and multi-factor in terms of what has been taught, learned, and is capable of doing. Thus, an effective training procedure must be able in adapting to each individual trainee's needs and capabilities, and continually contribute to their improvement.

Benjamin Bloom was one of the first scientists who systematically categorized the educational objectives and the related educational goals [20]. The so called "Bloom's taxonomy" is one of the main principles of the educational sciences, which has been revised and updated in the last years [45]. In general, the taxonomy forms a hierarchical model for the classification of educational learning objectives into levels of specificity and complexity. The overall method tries to enhance the communication between educators on the design of curricula, exercises, and examinations. It has been adopted by related teaching philosophies that lean more on skills rather than on content.

It consists of 6 layers, with the 3 bottom levels (remembering, understanding, and applying) denoting the basic understanding of the examined topic, while the coverage of the 3 top ones (analyzing, evaluating, and creating) reveals that the trainee has achieved a higher-order of thinking. Thus, the learning procedure is built from bottom-up, as the trainee goes through the cognitive, affective, and sensory learning domains [45]. Starting from the lowest maturity layer, where the trainee needs only to know the basic learning material, the process may reach at the highest point, where the trainee must have fully understood the overall learning concept. Figure 4 illustrates the main features for the latest revisited Bloom's taxonomy [52].

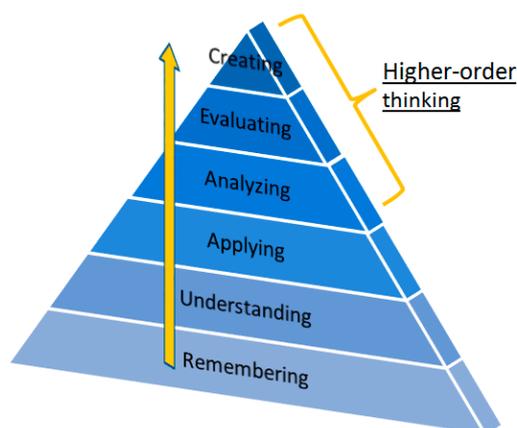


Figure 4. The revisited Bloom's taxonomy.

The first three layers assess the trainee's knowledge about the teaching content while skill development is promoted with "higher-order thinking". This also forms the final aim of the Bloom's taxonomy—building a culture of thinking.

The Blooms taxonomy was chosen for the scope of our study (instead of other candidate ones like the Miller's pyramid [39]) as: (i) it fully covers the educational objectives for cyber-security training, (ii) it is a well-established pedagogical methodology and widely-known among tutors, and (iii) it offers a good balance between simplicity and completeness for the categorization of the learning elements.

3.1.3. Continuous Trainee Assessment and Dynamic Adaptation of the Training Process

The trainee is taught the teaching material and then he/she is evaluated (in a single or several learning cycles). Afterwards, the results are surveyed and feedback is provided (both to the trainee and the trainer). During the evaluation phase, the overall process chooses the involved learning goals that will be evaluated (based on the teaching material which has been consumed by the specific trainee so far) and records the trainee's achievements. The process selects these goals based on the Bloom's revisited taxonomy, starting from the bottom (base of the knowledge pyramid) to the top (advanced

knowledge and hands-on capabilities/experiences). As the trainee accomplishes the lower-level goals, he/she proceeds to the upper/layers. Denoting also the increment of the training difficulty.

When the accomplishment ratio for the goals of a specific maturity layer goes beyond a threshold (i.e., 85%), we consider that the trainee has “cover” this layer. Thus, four “professional certification levels” are determined for each educational phase, based on the layers of the Bloom’s taxonomy:

- Foundation: the trainee has covered the first layer. He/she knows the main theoretic background of the educational topic.
- Practitioner: the trainee proceeds and accomplishes the layers 2–3. He/she has practical knowledge regarding the application and operation of the underlying concepts.
- Intermediate: the trainee reaches the layers 4–5. He/she has hands-on experience and technical knowledge regarding the deployment and management correlation of the various learning subjects.
- Expert: the trainee reaches the top layer 6. He/she has complete knowledge of the educational topic and is able in designing, developing, and administrating all aspects of the involved subject.

The absolute completion of a topic (100%) presents that the trainee has successfully learned all the underlying learning goals. Moreover, various trainee types with divert expectations and skill development needs could target a different level of certification.

4. The Smart Shipping Use Case

This section details the implementation of our educational method in the THREAT-ARREST platform, as well as the application of the adaptive learning for the real case of a smart shipping organization. The overall programme preparation and evaluation is composed of eight main phases: (i) description of the training programme, (ii) learning outcome of the training module, (iii) teaching and learning strategies, (iv) student participation, (v) overview of assessments and training levels, (vi) study plan (learning schedule), (vii) resources required to complete the training, and (viii) bench marking of the module. The phases are detailed in the following subsections.

4.1. Description of the Training Programme

The maritime sector is under an on-going process of digitalization in all aspects of operation. For a long period, seafarers have been trained with computer-based training programs on-board according to regulated training models. These days they are consuming training courses offered by sophisticated e-learning platforms. No doubt that maritime personnel are considered skilled enough to navigate properly in a web environment.

A typical topology of the on-board information technology (IT) and operation technology (OT) infrastructure [53] which is exposed to cyber threats and to risks in the format of environmental, crew safety or financing negative uncertainties is portrayed below in Figure 5.

Ships are becoming more and more integrated with shore-side operations because digital communication is being used to conduct business, manage operations, and stay in touch with head office. Furthermore, critical ship systems essential to the safety of navigation, power and cargo management have been increasingly digitalized and connected to the Internet to perform a wide variety of legitimate functions (e.g., updates, versioning upgrades, remote maintenance, voyage or ship performance monitoring from ashore, etc.). The ship–shore interface is conducted with several communication methodologies and protocols whistle cyber threats could be applicable to the full range of networking.

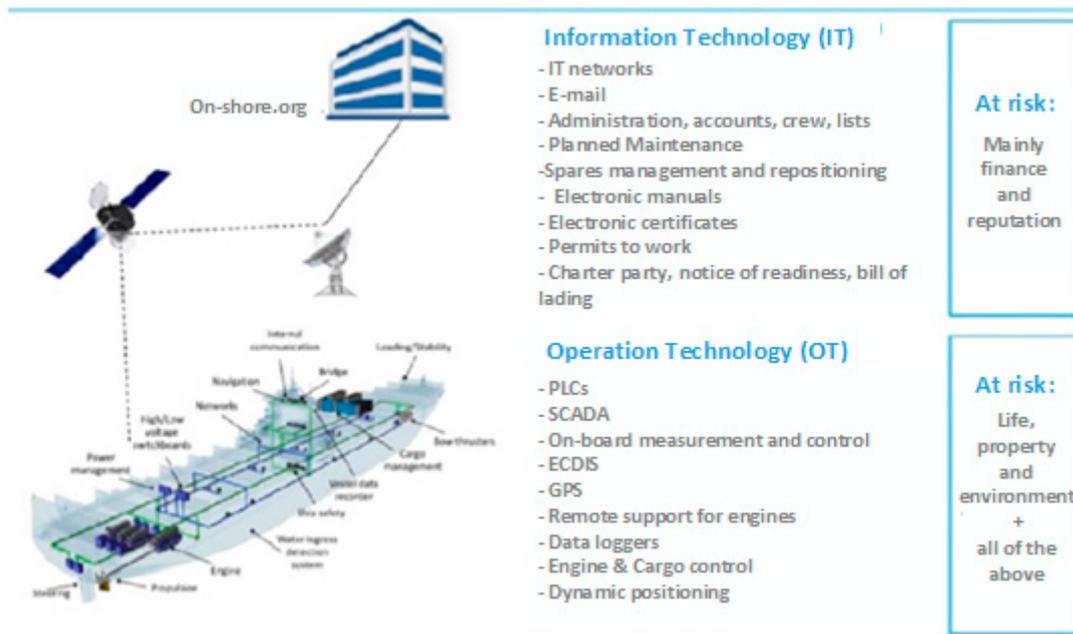


Figure 5. Smart shipping system architecture.

A schematic approach on the aforementioned networking for consumption of services between two distinct partners (shore and ship, supplier and vessel, third-party OS system provider and vessel, etc.) is following. The next figure is displaying and describing the configuration of DANAOS' communication protocols (web services, emails, telco, calls etc.) and security protections. Firewalls applied at each side of junctions between network components and data protection is secured with not storing data in centralized repositories but with controlling from a tailor-made and internally developed service platform (DANAOSone platform [54]). The overall platform modules are depicted in Figure 6.

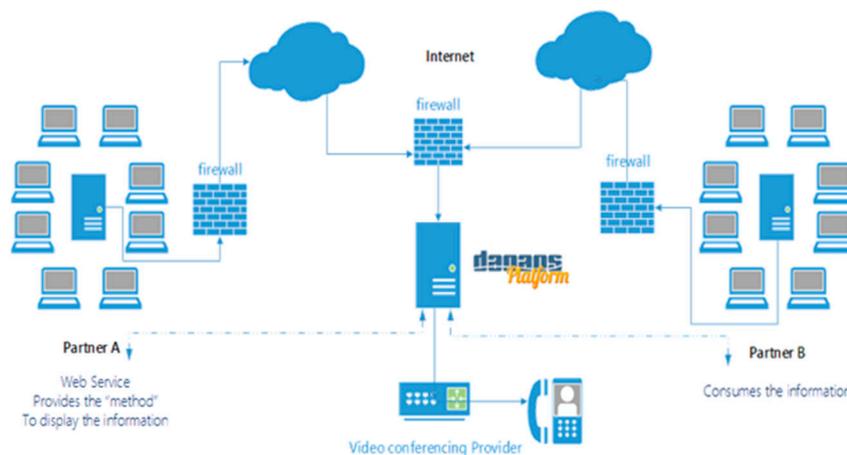


Figure 6. DANAOS configuration of communication protocols.

Cyber threats are raised where vulnerabilities in the system exist. A cyber-attack involves the attacker who in turn is motivated to trigger the attack in order to achieve a certain objective and the victim, who in turn faces the consequences of the attack. Protective barriers either in the form of technical protection or human awareness are set forward to prevent attack from impacting the system network components and cause negative consequences [55]. A schematic flow of cyber threat mechanism is given in Figure 7.

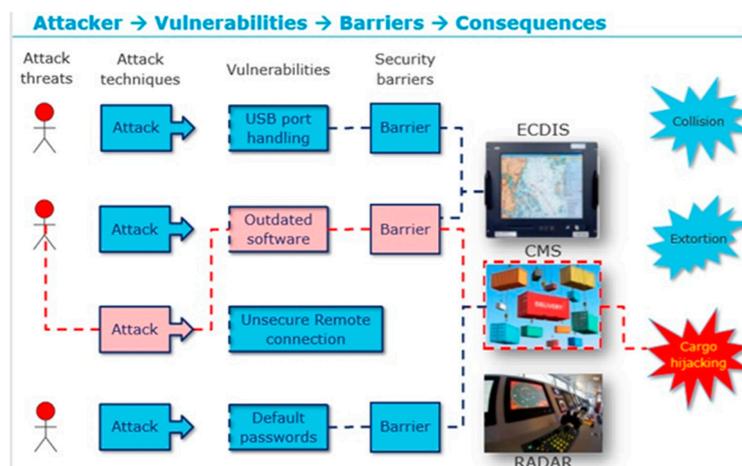


Figure 7. Flow of cyber threat mechanism.

Along that cyber threat mechanism, training and awareness is the key supporting element and an important barrier along with technical and physical protection to an effective approach to cyber safety and security.

4.2. Learning Outcome of the Training Module

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

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

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

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

Applicable personnel should be able to identify the signals when a system has been compromised. For example, training scenarios should trigger and evaluate user awareness aiming at the effective and efficient identification of hidden threats between applicable signs such as:

- An unresponsive or slow to respond system;
- Unexpected password changes or authorized users being locked out of a system;
- Unexpected errors in programs, including failure to run correctly or programs running; unexpected or sudden changes in available disk space or memory;
- Emails being returned unexpectedly;
- Unexpected network connectivity difficulties;
- Frequent system crashes;
- Abnormal hard drive or processor activity;
- Unexpected changes to browser, software or user settings, including permissions.

4.3. Teaching and Learning Strategies

At first, we begin by establishing a training programme that is tailored to the organization’s particularities. Then, we model the overall “learning path” (from basic to advance training) and the trainee starts the process. He/she is continuously evaluated, and the learning procedures are adapted to his/hers needs. Figure 8 sketches the overall process, which is further detailed in the following subsections.

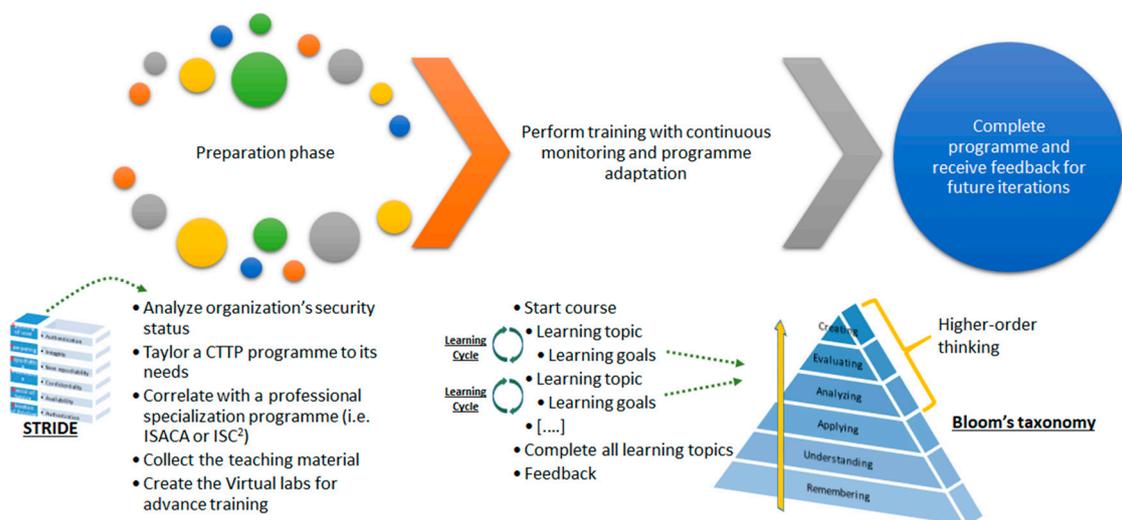


Figure 8. Training Programme lifecycle and the Learning path.

Initially, security experts interview the personnel of the evaluated organization (i.e., DANAOS shipping company). Then, we execute the Assurance Tool of the THREAT-ARREST platform [24,28] with the specifications of the pilot system (e.g., software modules, hardware equipment, network topology, business processes, etc.). With this Tool, we can: (i) export the system’s security vulnerabilities and threats, (ii) conduct a risk analysis to identify the most significant of them, and (iii) perform statistical analysis on the various system log-files in order to produce realistic synthetic logs (i.e., with the platform’s Data Fabrication Tool). Afterwards, these logs are utilized by the CTPP models and can be processed by the Gamification, Emulation, and/or Simulation Tools [25–27].

After the initial analysis, we define which are the main user/trainee types (e.g., simple users, operators, administrators, security experts, business managers and general personnel, CISOs, etc.), the security-related features (based on the STRIDE model), and the learning goals that we want to achieve (based on the Bloom’s taxonomy). Furthermore, we determine the involved learning topics that have to be taught to the organization’s personnel for the basic training procedure (e.g., information systems security, network security, cryptography, social-engineering, password management, etc.). For the advance training procedures, several valuable scenarios are also designed (e.g., serious games, emulated and/or simulated settings, potential synthetic logs, etc.).

The outcome is a tailored training programme for the specific needs of the evaluated user types. The programme specifies the learning topics and the advance evaluation scenarios for each trainee type, along with the correlated learning goals.

4.4. Student Participation

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

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

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

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

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

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

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

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

The guidelines for preventing deliberate attacks on ships and port facilities is defined in the International Ship and Facility Security Code ISPS adopted by the International Maritime Organization (IMO) in 2002 [56]. DANAOS is also following the guidelines of the Center of Internet security (CIS) [57] to apply critical security controls to equipment and data onboard vessels.

4.5. Overview of Assessments and Training Levels

In the aforementioned context of risk awareness framework and signal identification, THREAT-ARREST develops an advanced training programme incorporating emulation, simulation, serious gaming and visualization capabilities to adequately train and evaluate crew users with different types of responsibility and levels of expertise in recognizing signals of possible cyber-attacks, raising awareness on impact and consequences of attacks while following the necessary corrective actions to defend high-risk cyber systems. This also includes the design of several cyber-ranges scenarios, as are illustrated in Figure 9.

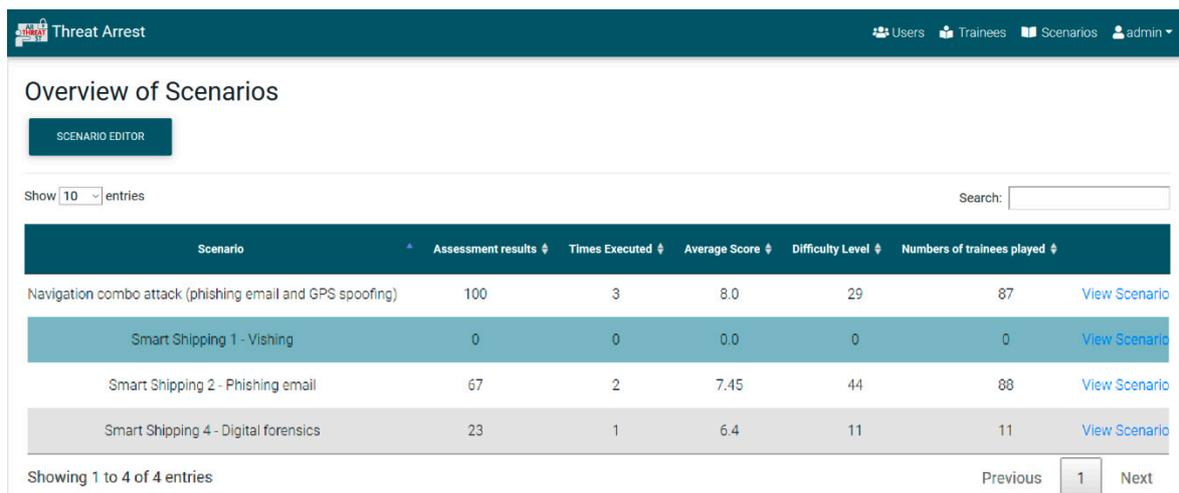


Figure 9. Scenarios overview.

From the previous figure, Table 2 summarizes the four main cyber-ranges exercises that have been implemented so far. Notice that due to the model-driven approach of the THREAT-ARREST platform, we can easily produce a high volume of variations of these four scenarios and the related CTP models (as depicted in Figure 9), supporting the dynamic adaptation features based on the pedagogical methods that were described in the previous sections. Moreover, the same models can be applied in other application domains (e.g., smart energy, healthcare, etc.) with slight changes.

Table 2. Main Smart Shipping Scenarios.

#	Description	Trainee Type	Security Expertise	Platform Tools
1	Navigation combo attack (phishing email and GPS spoofing)	Captain	Highly-privilege actuator with low/moderate security knowledge	<ul style="list-style-type: none"> Emulation Simulation Gamification
2	Vishing (social engineering)	Crew/Offshore officers	Non-security actuators with low access privileges	<ul style="list-style-type: none"> Training Gamification
3	Attacks on the Offshore system	IT Administrators of the shipping company	Highly-privilege actuators with moderate/high security knowledge	<ul style="list-style-type: none"> Emulation Assurance Tool
4	Digital Forensics	The organization’s security engineers	Security experts	<ul style="list-style-type: none"> Emulation Simulation Data Fabrication

The smart shipping pilot is based on the system of the DANAOS shipping company. This mainly includes the backend system at the organization’s premises, along with the DANAOS communication platform (DANAOSone), as well as the systems on the smart vessels and their communication with the main system. Figure 10 depicts the pilot’s architecture and main components.

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

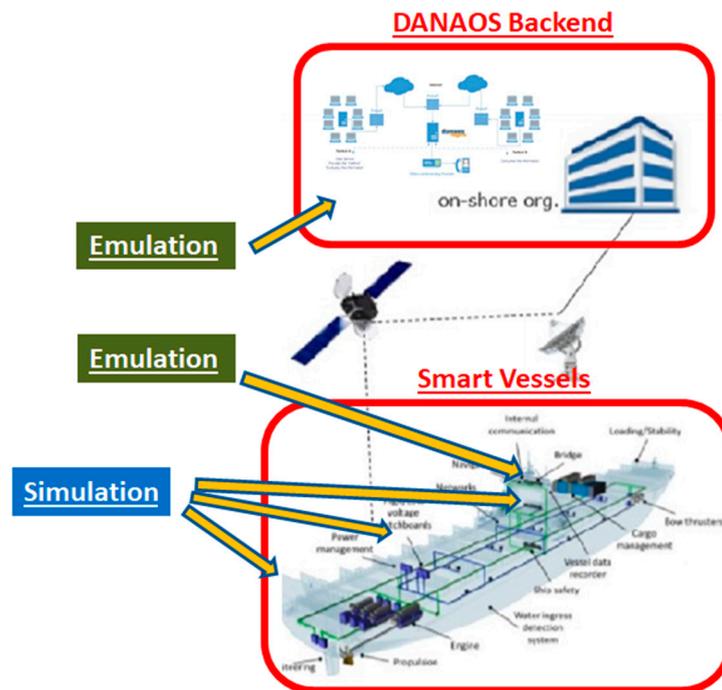


Figure 10. The Smart Shipping pilot architecture and Virtual Lab deployment.

Application Example of the STRIDE Model and the Bloom Taxonomy

In this subsection, we will describe the application of the STRIDE methodology for the modelling of the security aspects of the social engineering scenario. The trainee type is the captain of the vessel (valuable actuator with moderate security knowledge). He/she must start a (simulated) journey from the Heraklion port to Piraeus, which will be designated by the backend office via an email to the captain. All legitimate emails are digitally signed with PGP.

The programme involves the security aspects of “Tampering” and “Spoofing”. During the basic training, the trainee gets familiar with the main cryptographic primitives (Remembering), practices cryptography via related tools, i.e., CryptTool-2, (Understanding), and signs/verifies emails with PGP (Applying). Moreover, the trainee is touch the general concepts of social engineering and phishing attacks (Remembering), reviews specific examples of attacks and plays a PROTECT game with a social engineering card-deck (Understanding), and tries to classify email examples as legitimate or malicious (Applying).

For the advance training (Analyzing/Evaluating) as the emulated scenario starts, a faulty (but legitimate) email, commanding the captain to go to the Thessaloniki port, is sent. The email contains the details of another journey and was sent to the trainee by mistake: (i) the trainee identifies that this is a legitimate email, (ii) since the destination port was Piraeus, the trainee understands that this email was sent to him/her by mistake, and (iii) the trainee ignores the email and reports it back to the backend office. Then, the trainee receives a malicious (phishing) email, alerting him/her that a bad weather condition will take place, thus, he/she needs to go to another port to make a stop: (i) the trainee identifies that this is a phishing email and ii) ignores the email and reports it to the backend office. Lastly, the captain receives a legitimate email with the weather forecast, denoting that the weather is good, and the destination is the Piraeus port: (i) the trainee understands that this is a legitimate email and (ii) starts the journey in the Simulation Tool (where CTP simulation sub-models can be activated with on-ship attacks for more complex scenarios, i.e., GPS spoofing).

If the trainee succeeded in all steps and has learnt the underlying concepts, he/she can act as the trainer and create the emails (legitimate, faulty, or malicious) that will be sent to other trainees during the emulation scenario (Create). Table 3 summarizes the modelling steps for the social engineering scenario of Table 2 and Figure 9. The overall accomplishments of the trainee disclose his/her level of

understanding concerning the tampering and spoofing perspectives of social engineering attacks and the usage of the relevant countermeasures that would assure integrity and authentication, respectively.

Table 3. Modelling of a Social Engineering Scenario.

STRIDE Property	Bloom Taxonomy Layer	Description
Tampering/Integrity	Remembering	Introductory lesson to cryptography
	Understanding	Exercises with the educational Crypt Tool 2
	Applying	Practice with PGP (sign/verify emails)
	Analyzing/Evaluating	Emulated scenario where the trainee has to verify emails' integrity with PGP and send signed responses to the back office
Spoofing/Authentication	Creating	Act as the back office employee or the attacker and send the emails of the emulated scenario to other trainees
	Remembering	Lesson for social engineering and phishing attacks
	Understanding	Review of actual phishing email examples and play a tailored PROTECT game
	Applying	Classify email examples as legitimate or malicious
	Analyzing/Evaluating	Emulated scenario where the trainee must audit emails (e.g., the sender's email address, the email's content, PGP verification, etc.) and justify if they are legitimate, faulty, or malicious.
	Creating	Act as the back office employee or the attacker and send the emails of the emulated scenario to other trainees

4.6. Study Plan (Learning Schedule)

4.6.1. Basic Training

The basic training involves the Training and the Gamification Tools [25]. The trainees are registered and we compound their training sessions.

For the preparation of the Training Tool, we gather the content for the basic training (e.g., lectures, awareness videos, tutorials, and other educational material) and map it to the programmes for these specific trainees.

Then, the users start the training process by consuming the related teaching material. After completing a training section, the trainee's knowledge can be evaluated by exercises, capstone projects, and/or online tests (e.g., questionnaires).

Meanwhile, the trainee can practice his/her knowledge by playing serious games that are related with the learning material which has been consumed by the specific trainee. Each game has a pool of gaming ingredients, such as cards, set of questions, scenarios, etc. In each round, the trainee is given one of these ingredients and tries to find the correct action. For the THREAT-ARREST, an ingredient has also a tag-list that contains the learning topics which are related to the ingredient. For example, a card in the PROTECT game [25] for phishing attacks is correlated with training for information systems security and social-engineering (see Figure 11).

When a trainee starts a game, the Training Tool collects the learning topics that have been consumed by the specific trainee and sends them to the Gamification Tool. Then, the game selects randomly a set of the underlying ingredients from the pool that contain the learning topics in their tag-list. The trainee plays the game and the score is maintained within the game. Once it is over, the overall evaluation is sent back to the Training Tool and the trainee's profile is updated.

The basic training is considered successful when the trainee:

- Has consumed the main teaching material;
- Has passed the training evaluation (e.g., exercises, exams, etc.) with an adequate score;
- Has passed a game, which contains all the involved learning topics of the learning unit, with an adequate score.

Once a good level of understanding has been accomplished by the trainee, he/she can proceed with the related advance training scenarios, which are modelled in the form of CTTTP models.

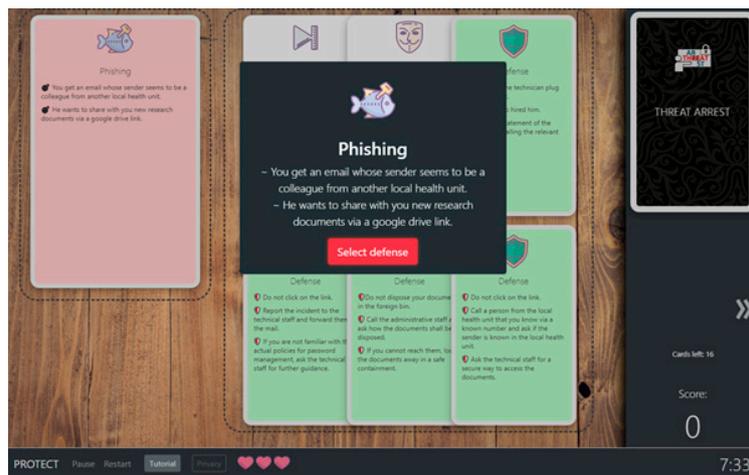


Figure 11. Game view of the serious game PROTECT.

4.6.2. Advance Training

The advance training involves emulated and/or simulated scenarios (see Figure 9 and Table 2). Once the trainee has completed the basic training for a learning unit, the accompanied CTPP models are activated in the Training Tool's Dashboard and the trainee can now proceed with the advanced training. The CTPP models describe a virtual system and how to instantiate it via the Emulation and Simulation Tools. In most cases, this virtual system will resemble the pilot system of the evaluated organization.

The trainee chooses one of the available/active CTPP models from the Dashboard. Then, the Training Tool parses the CTPP model and identifies the underlying emulated/simulated components, exports the instantiation scripts for each of these emulated/simulated components, and deploys the components sequentially, based on a designated instantiation order which is defined in the CTPP model. Specifically, the Training Tool sends the script for each component to the relevant Tool, receives an acknowledgement that the component is up and running, and proceeds to the next component. When all components are set correctly and are operative, the trainee is notified in the dashboard and can begin interacting with them (see Figure 12).

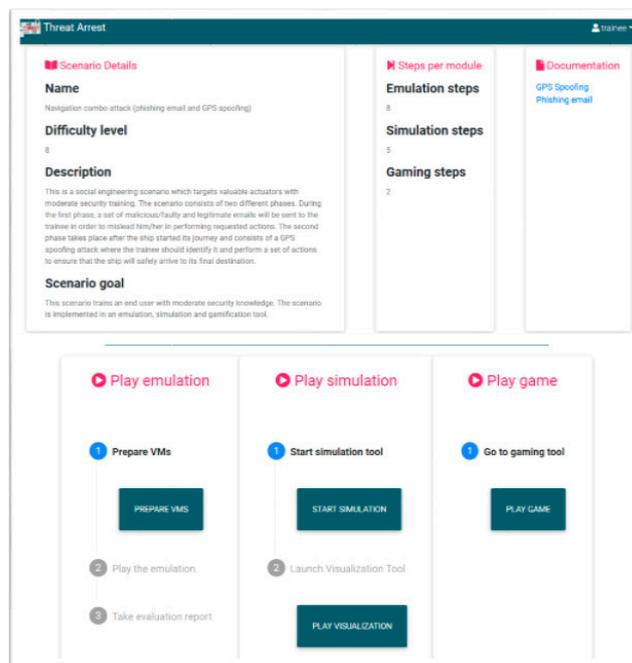


Figure 12. Training scenario details.

4.7. Resources Required to Complete the Training

THREAT-ARREST platform includes mechanisms that have been deployed with respect to the aggregated scoring of trainees in the various training scenarios, in order to provide real-time assessment information through the interface of the Training Tool. The evaluation process is briefly depicted in Figure 13.

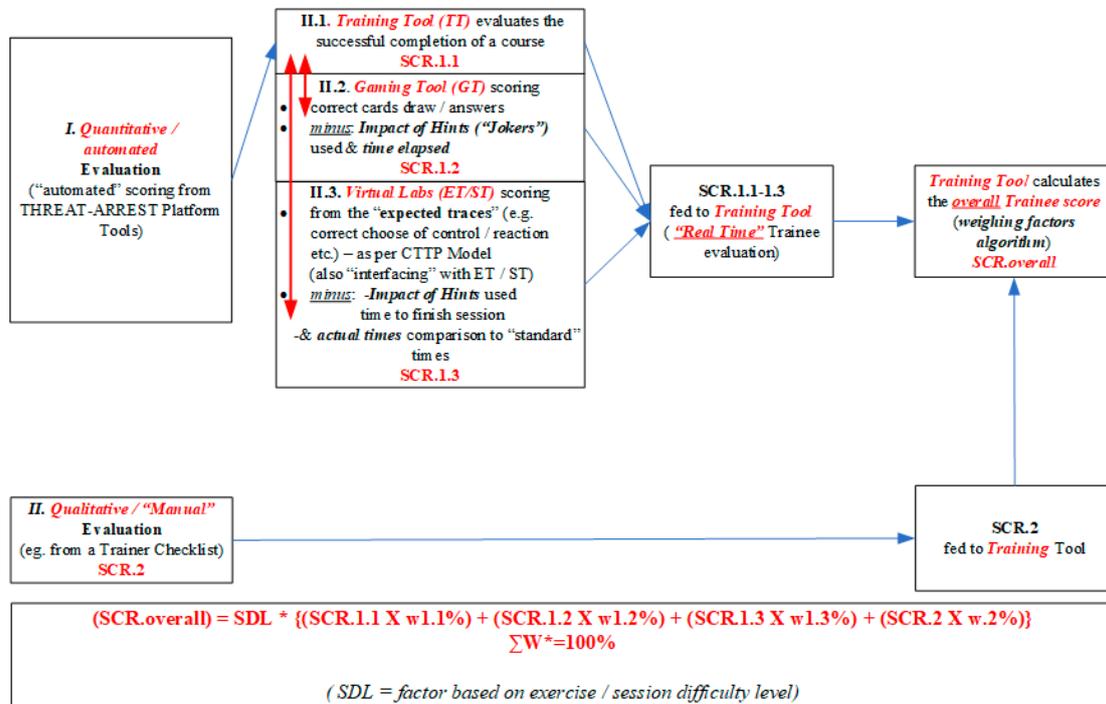


Figure 13. Scoring method for trainees' performance assessment.

Based on that, two complementary basic scoring "sources" are being used:

- 1 A quantitative (automated) scoring based on the TREAT-ARREST platform's tools and the relevant information derived from the CTTP Models. The first one can be divided to three sub-scores stemmed from:
 - a The Training Tool;
 - b The Gamification Tool;
 - c And the virtual labs with the Emulation and Simulation Tools.
- 2 And a qualitative (manual) scoring, e.g., when the trainee answers a questionnaire.

The overall score is calculated through the formula presented at the bottom of Figure 13, with the weights of each score to be defined by the administrator or the trainer. The exact algorithm and weights are pre-defined, based on a specific scenario/exercise and the CTTP Programmes standardization/certification associations.

Additionally, to the evaluation of the individual progress of each trainee, we also need a way to evaluate a CTTP Programme for an organization. Thus, aggregated metrics are also utilized to capture the success of an organization's trainees. In the main form, the min and max scores will be used from all the pilot trainees to disclose the deviation of the training among trainees of the same category (e.g., administrators) as well as the mean value and regression analysis to reflect the overall achievement and the generic security posture of the examined organization.

4.8. Benchmarking of the Module

After each iteration, the trainee’s scores are updated (see Figure 14).

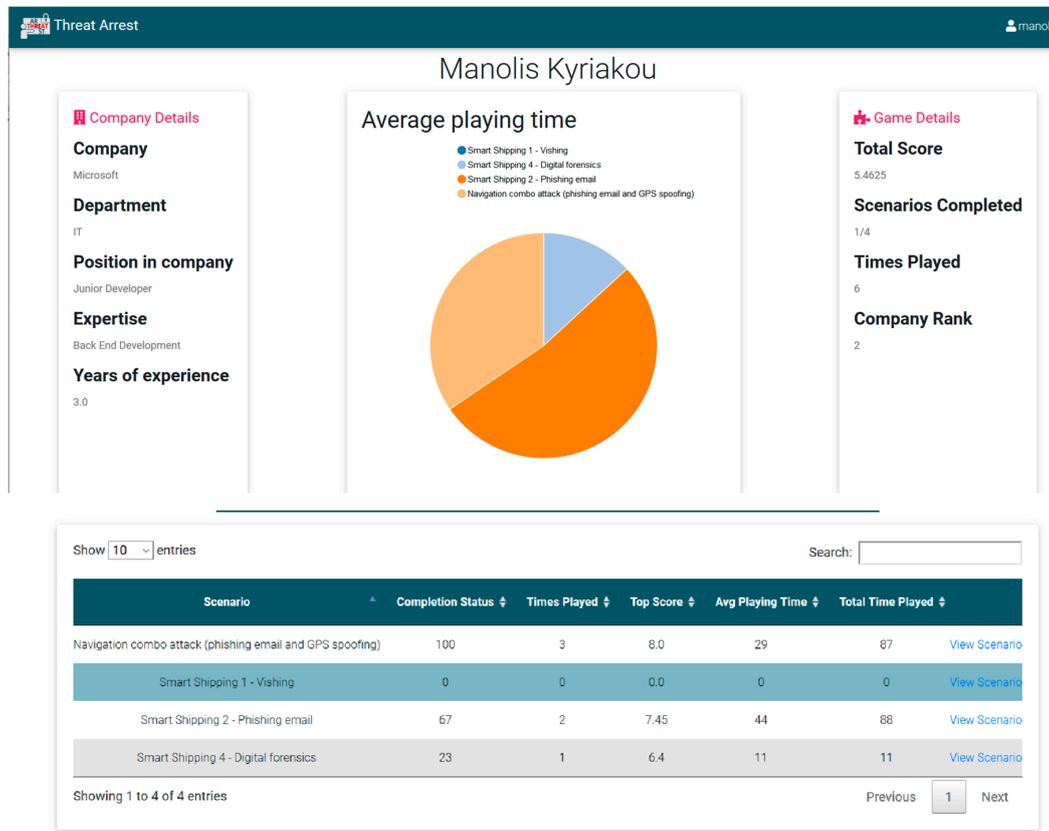


Figure 14. Trainee’s scores.

The organization can also review the progress of all its trainees along with the evaluation metrics for the programme as a whole (see Figure 15).

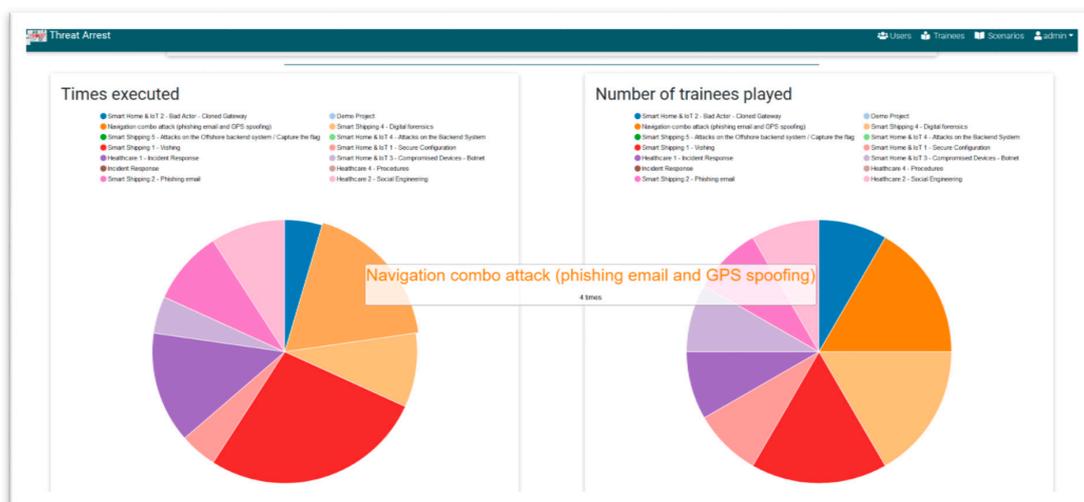


Figure 15. Smart shipping trainees’ scores and overall programme evaluation graphs.

DANAOS capitalizes on the THREAT-ARREST platform which delivers security training, based on a model-driven approach where CTPP 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 while driving the training process, and align it (where possible) with operational cyber system security assurance mechanisms to ensure the relevance of training.

The THREAT-ARREST's maritime pilot objective is to increase the security awareness in shipping Information and Communications Technology (ICT) systems' operators, and security attacks and help towards identifying new threats which jeopardize the operations of ICT systems in the Shipping Management industry.

5. Discussion

Cyber-security training is always important for the general public and can be even imperative for some economic sectors. The evolving digitalization of our daily activities is expected to bring more and more cyber-security in the foreground. Although there is a plethora of training platforms with advance technical features, the focus to the pedagogical aspects is expected to gain more focus for the next generation of these platforms.

The European Cyber Security Organization (ECSO) along with the European Cybersecurity Competence Network Pilot projects published a concrete report for 2019–2020 [58,59], concerning the modern features and aspects that novel cyber-security training platforms have to support. The overall THREAT-ARREST approach supports several of the modern educational features that an innovative training environment has to support, such as virtual labs, serious games, collaborating exercises, discussion sessions, the human in the training loop, etc. Moreover, the maritime sector is identified among the important economic sectors that require advance cyber-security training programmes.

This paper tackles the incorporation of educational methods to the overall lifecycle of a complete training programme with the dynamic adaptation of the training process to the trainee's particularities. In the current version, these procedures are more-or-less predefined to some degree by the trainer or the programme designer. Therefore, we can support different difficulty levels for different trainee types (ranging from main security for the general public to advance training for security experts), as well as, the gradual building of the Bloom's knowledge pyramid for each one of them. The model-driven operation enables us to easily generate a high variety of training models and cope with the dynamicity of the training requirements.

One important aspect which should be offered by a modern platform based on the surveys from ECSO [58,59], is the adaptation of the training based on machine learning and artificial intelligence. Therefore, the dynamicity will be mostly supported by an intelligent system and will be further adapted to a person's behavior. The goal is to make the training even more human-centric. The THREAT-ARREST platform does not support this functionality. Nevertheless, the benchmarking of the training modules (Section 4.8) could act as a training dataset for the potential machine learning proposals. Improvements can be suggested regarding the time that is required for specific trainee groups to complete an exercise, the use of assistive hints throughout the exercise, as well as the assessment of the mapping between the training modules and the learning objectives. Furthermore, a model-driven design, such as the one developed by THREAT-ARREST, could make the implementation of this vision feasible.

As aforementioned, expansion to other economic sectors and industries should also be considered [58]. Now, we are in progress of providing targeted training scenarios for healthcare and smart energy piloting systems. Videos with demos for the main platform tools as well as a set of training scenarios can be found on our YouTube channel at www.youtube.com/channel/UCBUCInDkE6cjYtw7cEgP0vQ. The platform is currently under evaluation and actual training sessions with real employees from the shipping company are to be conducted this summer.

6. Conclusions

This paper proposes an educational methodology for the dynamic adaptation of cyber-security training programmes. A training session is disassembled into learning topics, which are then

categorized based on the revisited Bloom's taxonomy and are mapped to the STRIDE security model. The trainee starts the learning process by consuming the main teaching material (e.g., lectures, tutorials, videos, etc.) and proceeds to more advanced learning procedures, involving hands-on experience on emulated/simulated components. The trainee is continuously evaluated. The assessment begins from learning topics that cover the knowledge basis of the examined teaching unit (modelled in the Bloom's taxonomy), and if the trainee is successful, he/she can proceed to the correlated modules for advanced training. The beneficiary aims to develop his/her skills and earn a professional certification on specific cyber-security fields, based on the four specialization levels that are offered (foundation, practitioner, intermediate, and expert). The overall method is integrated in the cyber-ranges platform THREAT-ARREST and a preliminary application is presented, where a training programme for smart shipping personnel is established.

As a future extension, we consider the further evaluation of the method based on feedback that we receive by trainers and/or other users of the platform. Artificial Intelligence empowered by machine learning for the adaptation of the training to the trainee's skills is also an interesting approach that can be implemented when a sufficient volume of trainee profiles has been collected from future iterations. Moreover, we are now planning new training programmes for the cases of healthcare and smart energy organizations.

Author Contributions: Conceptualization, all co-authors; methodology, G.H., F.O., and G.L.; software, M.S., G.T., F.F., L.G. and T.H.; validation, F.O., G.H., H.K. and G.L.; resources, F.O.; data curation, M.S. and G.T.; writing—original draft preparation, G.H.; writing—review and editing, G.H. and M.S.; visualization, T.H., G.T. and L.G.; Supervision and Project administration, S.I. and G.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work has received funding from the European Union Horizon's 2020 research and innovation programme H2020-DS-SC7-2017, under grant agreement No. 786890 (THREAT-ARREST).

Acknowledgments: This work has received funding from the European Union Horizon's 2020 research and innovation programme H2020-DS-SC7-2017, under grant agreement No. 786890 (THREAT-ARREST).

Conflicts of Interest: "The authors declare no conflict of interest".

References

1. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A survey of Internet of Things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet Things J.* **2017**, *4*, 1125–1142. [CrossRef]
2. Hatzivasilis, G.; Fysarakis, K.; Soultatos, O.; Askoxylakis, I.; Papaefstathiou, I.; Demetriou, G. The Industrial Internet of Things as an enabler for a Circular Economy Hy-LP: A novel IIoT Protocol, evaluated on a Wind Park's SDN/NFV-enabled 5G Industrial Network. In *Computer Communications—Special Issue on Energy-Aware Design for Sustainable 5G Networks*; Elsevier: Amsterdam, The Netherlands, 2018; Volume 119, pp. 127–137.
3. Habibi, J.; Midi, D.; Mudgerikar, A.; Bertino, E. Heimdall: Mitigating the Internet of Insecure Things. *IEEE Internet Things J.* **2017**, *4*, 968–978. [CrossRef]
4. Hatzivasilis, G.; Soultatos, O.; Ioannidis, S.; Verikoukis, C.; Demetriou, G.; Tsatsoulis, C. Review of Security and Privacy for the Internet of Medical Things (IoMT). In Proceedings of the 1st International Workshop on Smart Circular Economy (SmaCE), Santorini Island, Greece, 30 May 2019; pp. 1–8.
5. Hatzivasilis, G.; Soultatos, O.; Ioannidis, S.; Spanoudakis, G.; Katos, V.; Demetriou, G. MobileTrust: Secure Knowledge Integration in VANETs. *ACM Trans. Cyber-Phys. Syst.* **2020**, *4*, 1–25. [CrossRef]
6. Khandelwal, S. United airlines hacked by sophisticated hacking group. *The Hacker News*, 30 July 2015.
7. Hirschfeld, J.D. Hacking of government computers exposed 21.5 million people. *The New York Times*, 9 July 2015.
8. Santa, I. *A Users' Guide: How to Raise Information Security Awareness*; ENISA: Heraklion, Greece, 2010; pp. 1–140.
9. Manifavas, C.; Fysarakis, K.; Rantos, K.; Hatzivasilis, G. DSAPE—Dynamic Security Awareness Program Evaluation. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*; Springer: Cham, Switzerland, 2014; pp. 258–269.
10. Kish, D.; Carpenter, P. Forecast Snapshot: Security Awareness Computer-Based Training, Worldwide. 2017. Gartner Research, ID G00324277, March 2017. Available online: <https://www.gartner.com/en/documents/3629840/forecast-snapshot-security-awareness-computer-based-trai> (accessed on 24 July 2020).

11. SANS: Online Cyber Security Training. 2000–2020. Available online: <https://www.sans.org/online-security-training/> (accessed on 24 July 2020).
12. CYBERINTERNACADEMY: Complete Cybersecurity Course Review on Cyberinternacademy. 2017–2020. Available online: <https://www.cyberinternacademy.com/complete-cybersecurity-course-guide-review/> (accessed on 24 July 2020).
13. StationX: Online Cyber Security & Hacking Courses. 1996–2020. Available online: <https://www.stationx.net/> (accessed on 24 July 2020).
14. Cybrary: Develop Security Skills. 2016–2020. Available online: <https://www.cybrary.it/> (accessed on 24 July 2020).
15. AwareGO: Security Awareness Training. 2011–2020. Available online: <https://www.awarego.com/> (accessed on 24 July 2020).
16. BeOne Development: Security Awareness Training. 2013–2020. Available online: <https://www.beonedev.com/en/security-awareness/> (accessed on 24 July 2020).
17. ISACA: CyberSecurity Nexus (CSX) Training Platform. 1967–2020. Available online: <https://cybersecurity.isaca.org/csx-certifications/csx-training-platform> (accessed on 24 July 2020).
18. Kaspersky: Kaspersky Security Awareness. 1997–2020. Available online: <https://www.kaspersky.com/enterprise-security/security-awareness> (accessed on 24 July 2020).
19. CyberBit: Cyber Security Training Platform. 2019–2020. Available online: <https://www.cyberbit.com/blog/security-training/cyber-security-training-platform/> (accessed on 24 July 2020).
20. Bloom, B. Taxonomy of educational objectives: The classification of educational goals. In *Handbook I: Cognitive Domain*; David McKay Company: New York, NY, USA, 1956.
21. Johnstone, M.N. Threat modelling with STRIDE and UML. In Proceedings of the 8th Australian Information Security Management Conference (AISM), Perth Western, Australia, 30 November 2010; pp. 18–27.
22. Biggs, J. *Teaching for Quality Learning at University: What the Student Does*, 4th ed.; Open University Press: Maidenhead, UK, 2011; pp. 1–416.
23. Sims, R. R. Kolb’s Experiential Learning Theory: A Framework for Assessing Person-Job Interaction. *Acad. Manag. Rev.* **1983**, *8*, 501–508. [[CrossRef](#)]
24. Othonas, S.; Fysarakis, K.; Spanoudakis, G.; Koshutanski, H.; Damiani, E.; Beckers, K.; Wortmann, D.; Bravos, G.; Ioannidis, M. The TREAT-ARREST Cyber-Security Training Platform. In Proceedings of the 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), Luxembourg, 27 September 2019.
25. Goeke, L.; Quintanar, A.; Beckers, K.; Pape, S. PROTECT—An Easy Configurable Serious Game to Train Employees Against Social Engineering Attacks. In Proceedings of the 1st Model-Driven Simulation and Training Environments for Cybersecurity (MSTEC), Luxembourg, 27 September 2019.
26. Beckers, K.; Pape, S.; Fries, V. HATCH: Hack and trick capricious humans—A serious game on social engineering. In Proceedings of the 30th International BCS Human Computer Interaction (HCI) Conference Fusion, Bournemouth, UK, 11–15 July 2016; pp. 1–3.
27. Braghin, C.; Cimato, S.; Damiani, E.; Frati, F.; Mauri, L.; Riccobene, E. A model driven approach for cyber security scenarios deployment. In Proceedings of the 1st Model-Driven Simulation and Training Environments for Cybersecurity (MSTEC), Luxembourg, 27 September 2019.
28. Somarakis, I.; Smyrlis, M.; Fysarakis, K.; Spanoudakis, G. Model-driven Cyber Range Training—The Cyber Security Assurance Perspective. In Proceedings of the 1st Model-Driven Simulation and Training Environments for Cybersecurity (MSTEC), Luxembourg, 27 September 2019.
29. Hautamäki, J.; Karjalainen, M.; Hämäläinen, T.; Häkkinen, P. Cyber security exercise: Literature review to pedagogical methodology. 13th annual International Technology. In Proceedings of the Education and Development Conference, Valencia, Spain, 11–13 March 2019; pp. 3893–3898.
30. McDaniel, L.; Talvi, E.; Hay, B. Capture the Flag as Cyber Security Introduction. In Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 5–8 January 2016; pp. 5479–5486.
31. James, J.E.; Morsey, C.; Phillips, J. Cybersecurity education: A holistic approach to teaching security. In *Issues in Information Systems*; Maria, E.C., Ed.; IACIS: Leesburg, VA, USA, 2016; Volume 17, pp. 150–161.
32. ISO 22398: Societal Security—Guidelines for Exercises. Available online: <https://www.iso.org/standard/50294.html> (accessed on 24 July 2020).
33. Arabo, A.; Serpell, M. Pedagogical Approach to Effective Cybersecurity Teaching. In *Transactions on Edutainment XV*; Springer: Berlin/Heidelberg, Germany, 2019; Volume 11345, pp. 129–140.

34. Freitas, S.; Oliver, M. How can exploratory learning with games and simulations within the curriculum be most effectively evaluated? *Comput. Educ.* **2006**, *46*, 249–264. [[CrossRef](#)]
35. Israel, M.; Lash, T. From classroom lessons to exploratory learning progressions: Mathematics + computational thinking. *Interact. Learn. Environ.* **2019**, *28*, 362–382. [[CrossRef](#)]
36. Mann, L.; Chang, R.L.; Chandrasekaran, S.; Coddington, A.; Daniel, S.; Cook, E.; Crossin, E.; Cosson, B.; Turner, J.; Mazzurco, A.; et al. From problem-based learning to practice-based education: A framework for shaping future engineers. *Eur. J. Eng. Educ.* **2020**, 1–21. [[CrossRef](#)]
37. Scheponik, T.; Sherman, A.T.; Delatte, D.; Phatak, D.; Oliva, L.; Thompson, J.; Herman, G.L. How Students Reason about Cybersecurity Concepts. In Proceedings of the Frontiers in Education Conference (FIE), Erie, PA, USA, 12–15 October 2016; pp. 1–5.
38. Ericsson, K.A. Deliberate practice and acquisition of expert performance: A general overview. *Acad. Emerg. Med.* **2008**, *15*, 988–994. [[CrossRef](#)] [[PubMed](#)]
39. Miller, G.E. The assessment of clinical skills/competence/performance. *Acad. Med.* **1990**, *65*, 63–67. [[CrossRef](#)] [[PubMed](#)]
40. Karjalainen, M.; Kokkonen, T.; Puuska, S. Pedagogical Aspects of Cyber Security Exercises. In Proceedings of the IEEE European Symposium on Security and Privacy Workshops, Stockholm, Sweden, 17–19 June 2019; pp. 103–108.
41. Kick, J. Cyber Exercise Playbook. The MITRE Corporation. Available online: https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf (accessed on 24 July 2020).
42. Lif, P.; Somestad, T.; Granasen, D. Development and evaluation of information elements for simplified cyber-incident reports. In Proceedings of the International Conference On Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA), Glasgow, UK, 11–12 June 2018; pp. 1–10.
43. Said, S.E. Pedagogical Best Practices in Higher Education National Centers of Academic Excellence/Cyber Defense Centers of Academic Excellence in Cyber Defense. Ph.D. Thesis, Union University, Tennessee, TN, USA, May 2018.
44. Athauda, R.; AlKhaldi, T.; Pranata, I.; Conway, D.; Frank, C.; Thorne, W.; Dean, R. Design of a Technology-Enhanced Pedagogical Framework for a Systems and Networking Administration course incorporating a Virtual Laboratory. In Proceedings of the Frontiers in Education Conference (FIE), San Jose, CA, USA, 3–6 October 2018; pp. 1–5.
45. Pohl, M. *Learning to Think—Thinking to Learn: Models and Strategies to Develop a Classroom Culture of Thinking*, 1st ed.; Hawker Brownlow Education: Cheltenham, Australasia, 2000; pp. 1–98.
46. Švábenský, V.; Vykopal, J.; Čermák, M.; Laštovička, M. Enhancing cybersecurity skills by creating serious games. In Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITIICSE), Larnaca, Cyprus, 2–4 July 2018; pp. 194–199.
47. Jin, G.; Tu, M. Evaluation of Game-Based Learning in Cybersecurity Education for High School Students. *J. Educ. Learn.* **2018**, *12*, 150–158. [[CrossRef](#)]
48. Taylor-Jackson, J.; McAlaney, J.; Foster, J.; Bello, A.; Maurushat, A.; Dale, J. Incorporating Psychology into Cyber Security Education: A Pedagogical Approach. In Proceedings of the AsiaUSEC'20, Financial Cryptography and Data Security (FC), Sabah, Malaysia, 14 February 2020; pp. 1–15.
49. Shah, V.; Kumar, A.; Smart, K. Moving Forward by Looking Backward: Embracing Pedagogical Principles to Develop an Innovative MSIS Program. *J. Inf. Syst. Educ.* **2018**, *29*, 139–156.
50. Knapp, K.J.; Maurer, C.; Plachkinove, M. Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. *J. Inf. Syst. Educ.* **2017**, *28*, 101–114.
51. Shafiq, H.; Kamal, A.; Ahmad, S.; Rasool, G.; Iqbal, S. Threat modelling methodologies: A survey. *Sci. Int.* **2014**, *26*, 1607–1609.
52. Anderson, L.W.; Krathwohl, D.R.; Airasian, P.W.; Cruikshank, K.A.; Mayer, R.E.; Pintrich, P.R.; Raths, J.; Wittrock, M.C. *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives*; Reference and Research Book News: Dublin, OH, USA, 2001; Volume 16, pp. 1–336.
53. Bird, J.; Kim, F. Survey on application security programs and practices. In *A SANS Analyst Survey*; SANS Institute: Bethesda, MD, USA, 2014; pp. 1–24.
54. DANAOS Shipping Company: DANAOSone Platform. DANAOS Management Consultants S.A. Available online: <https://web2.danaos.gr/maritime-software-solutions/danaosone-platform/> (accessed on 24 July 2020).
55. Trustwave. *Security Testing Practices and Priorities: An Osterman Research Survey Report*; Osterman Research: Seattle, WA, USA, 2016; pp. 1–15.

56. IMO. SOLAS Chapter XI-2—*International Ship and Port Facility Security Code (ISPS Code)*; International Maritime Organization (IMO): London, UK, 2004.
57. CIS: Center of Internet Security. Available online: <https://www.cisecurity.org/> (accessed on 24 July 2020).
58. ESCO: Results of Simulation-Based Competence Development Survey. European Cyber Security Organisation, 2019–2020 Report. Available online: <https://echonetwork.eu/report-results-of-simulation-based-competence-development-survey/> (accessed on 24 July 2020).
59. Aaltola, K.; Taitto, P. Utilising Experiential and Organizational Learning Theories to Improve Human Performance in Cyber Training. *Inf. Secur. Int. J.* **2019**, *43*, 123–133. [[CrossRef](#)]



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).