The THREAT-ARREST Cyber-Security Training Platform

Othonas Soultatos[1,9], Konstantinos Fysarakis[2], George Spanoudakis[2], Hristo Koshutanski[3], Ernesto Damiani[4], Kristian Beckers[5], Dirk Wortmann[6], George Bravos[7], and Menelaos Ioannidis[8]

[1] Foundation for Research and Technology, Vassilika Vouton 70013, Greece
[2] Sphynx Technology Solutions AG, Zug 6300, Switzerland
[3] ATOS Spain SA, Madrid 28037, Spain
[4] University of Milan, Milano 20122, Italy
[5] Social Engineering Academy (SEA), Frankfurt 60322, Germany
[6] SimPlan AG, Hanau 63452, Germany
[7] Information Technology for Market Leadership (ITML), Athens GR 11525, Greece
[8] Lightsource Labs Limited (LSE), Dublin IR D06C8X4, Ireland
[9]Department of Computer Science, City, University of London, London, UK
sultatos@ics.forth.gr,othonas.soultatos@city.ac.uk
fysarakis@sphynx.ch, spanoudakis@sphynx.ch,
hristo.koshutanski@atos.net, ernesto.damiani@unimi.it,
kristian.beckers@social-engineering.academy,
dirkwortmann@simplan.de, gebravos@itml.gr,
menelaos@lightsourcelabs.com

Abstract. Cyber security is always a main concern for critical infrastructures and nation-wide safety and sustainability. Thus, advanced cyber ranges and security training is becoming imperative for the involved organizations. This paper presets a cyber security training platform, called THREAT-ARREST. The various platform modules can analyze an organization's system, identify the most critical threats, and tailor a training program to its personnel needs. Then, different training programmes are created based on the trainee types (i.e. administrator, simple operator, etc.), providing several teaching procedures and accomplishing diverse learning goals. One of the main novelties of THREAT-ARREST is the modelling of these programmes along with the runtime monitoring, management, and evaluation operations. The platform is generic. Nevertheless, its applicability in a smart energy case study is detailed.

Keywords: Security Training, Cyber Range, Training Programmes, Training Exercises, Dynamic Adaptation, CTTP, Smart Grid, Smart Energy.

1 Introduction

Massive advancements in computer technologies have given rise to a cyber-infrastructure enabling the acquisition, storage, sharing, integration, and processing of data, through distributed software services cutting across organizational and national

boundaries. It is estimated that up to 200 billion devices will be connected to the Internet by 2020 (i.e. 26 connected objects per person [1]), while 5.5 million new "things" were being connected every day in 2016 alone. This cyber infrastructure has facilitated the development of complex interconnected cyber systems, supporting an ever-increasing spectrum of everyday personal, societal and business activities, making modern society and enterprise increasingly dependent on them.

The unprecedented levels of data sharing and cyber systems interoperability, and the complex compositional structures of cyber systems have also led to increasingly sophisticated, stealthy, targeted, and multi-faceted cyberattacks. The "cyber-war" against essential infrastructures around the globe has already been underway. Examples include attacks in airports and airlines [2], [3] government services (U.S. Office of Personnel Management [4]), health insurance companies and health providers [5].

Preserving the security of cyber systems is a particularly challenging problem [6], [7], [8]. 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 infrastructures that they deploy.

However, despite the importance of security training, the initiatives to "educate" enterprise personnel (particularly of SMEs) and make it realize the importance cyber-security are limited [9], [10]. The provision of effective and comprehensive security training in organizations and enterprises is becoming even more important due to the sheer complexity of cyber systems that need to be secured and the ever-increasing number and level of sophistication of cyber-attacks [11], [12].

Even though at a first glance, the existence of a wide spectrum of security tools appears to provide a comprehensive machinery for detecting and responding effectively to cyber-attacks (e.g. [13], [14]), in reality the very existence of several alternative tools, targeting different aspects and layers of modern cyber systems and having different capabilities, makes it difficult to establish effective tool usage strategies and processes for addressing the ever-expanding landscape of cyber-attacks. Moreover, the advent of more "intelligent" cyber-security solutions [8], [13], which make use of technologies, like machine learning, statistical analysis and user behavior analysis, requires sophisticated and hands-on training of the key personnel of organizations, who have responsibility for security, for the latter to be able to master them.

Overcoming the above difficulties requires the development of advanced security training frameworks to adequately prepare stakeholders with responsibility in defending high-risk computer systems and organizations to counter advanced cyber-attacks. A framework of this type must be able to accommodate and cover emerging security controls and tool innovations from different providers in a scalable manner (i.e. [7], [15]). It should also be supported by experience sharing [16], [17] and put emphasis on the human aspects of security. In this direction, technologies, such as serious gaming (e.g. [18], [19], [20]), whose aim is to address security attacks launched through social engineering, get an important role, as one of the most effective ways to defend systems against attacks and train humans to resist social-engineering.

In response to these needs, the overall aim of THREAT-ARREST is to develop an advanced training platform incorporating emulation, simulation, serious gaming, and visualization capabilities to adequately prepare stakeholders with different types of responsibility and levels of expertise in defending high-risk cyber systems, and organizations to counter advanced, known, and new cyber-attacks. The THREAT-ARREST platform will deliver security training, based on a model-driven approach where **cyber threat and training preparation (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. The platform will also support trainee performance evaluation and training programme evaluation, and adapt training programmes based on them. The effectiveness of the framework will be validated on a real pilot system in the area of smart energy.

The rest paper is structured as follows: Section 2 presents the related work in cyber security training landscape along with a qualitative comparison. Section 3 defines the CTTP modeling and its application on a smart energy scenario. Sections 4 details the platform architecture and the underlying modules for hybrid training, gamification, emulation, simulation, and visualization. Finally, Section 5 concludes this work.

2 Related Work & Comparison

Today, there are several research and commercial solutions for cyber security training for organizations or individuals. The most representative of them are reviewed below.

Apart from the general-purpose online training platforms (e.g. Coursera Udacity, edX, etc.) that can provide main educational courses on cyber security, there are also specialized platforms, like the SANS [21], CyberInternAcademy [22], StationX [23], Cybrary [24], and AwareGO [25]. In most cases, they target individual students/trainees whose goal is to develop/sharpen new skills. Nevertheless, these approaches fail when it comes to hands-on experience on real systems or cyber ranges.

The German company BeOne Development has implement its own solution of security awareness training [26]. It includes e-learning modules, awareness videos, and simulation tools. For the former, the BePhished simulator is utilized, which is focused on phishing attacks. To facilitate the process for establishing new training exercises, they have also developed the Security Awareness Library which contains 28 learning topics. Multinational working environments and cultural differences are taken into account, as the training becomes more effective when used examples are recognized by employees from their own daily jobs. The product can offer pre-packaged and generic programs, organization-specific look and feel, or tailor-made programs that have been developed in close consultation with the customer. The overall approach supports general teaching processes for the main training, while the more advanced simulation-centric training targets phishing attempts.

ISACA developed the CyberSecurity Nexus (CSX) training platform [27]. It provides instructional lectures and hands-on lab works on real equipment. The trainee

gets experience in applying basic concepts and industry-leading methods. Capture-the-flag scenarios are also supported, advancing the trainee's technical skills. The users are assessed and the goal is to earn a relevant professional certification. This would assist an organization's chief information security officer (CISO) to hire employees with the right skills.

Kaspersky offers advanced computer-based training programs for all organizational levels [28]. Except from online training, the platform supports benchmarking against world/industry averages, robust simulation, and true gamification. It builds an educational schedule and internal learning with constant reinforcement, offered automatically through a blend of training formats, including learning modules, email reinforcement, tests, and simulated phishing attacks. It follows the trainees' progress via a user-friendly dashboard, supporting live data tracking, trends, and forecasts.

CyberBit was founded in 2015 and its cyber security training platform provides a realistic simulation of cyber-attacks in an environment that mirrors a real-life network and a security operations center (SOC) [29]. This cyber range solution is consisted of a virtual network (mirror of an actual system), an attack engine (malicious traffic), a traffic generator (legitimate data), and a virtual SOC (trainee's viewpoint). The goal is to simulate hyper-realistic cyber ranges. The platform provides a high variety of training scenarios, such as incident response and pentesting. The trainers set up the training session which includes debriefing, session recording, trainee ranking, and scenario management. Scenario customization is also supported via a graphical interface.

On the other hand, the THREAT-ARREST platform offers training on known and/or new advanced cyber-attack scenarios, taking different types of actions 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 & injection testing)

The procedure begins by analyzing the organization's system. An assurance tool 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, tailored to the organization 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 will be used to tailor programmes to the needs of individual trainees or alter them at a more macroscopic level.

The qualitative comparison results are summarized in **Table 1**. THREAT-ARREST combines all modern training aspects of serious gaming, emulation, and simulation in a concrete manner, and offers continuous security assurance and programme adaptation based on the trainee's performance and skills.

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)arial.

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

3 CTTP Modelling

3.1 Pilot System Modelling & Continuous Security Assurance

One of the main novelties of the THREAT-ARREST approach is the modelling of the training process, the real-time assessment of the security features for an examined system, and the continuous evaluation of the trainer.

The development of the THREAT-ARREST framework will be based on a model-driven approach in which the delivery of cyber-threat training and preparation (CTTP) programmes will be driven by CTTP models. A CTTP model will define the structure and automate the development of a CTTP programme by determining:

1. the components of a cyber-system, their relations and the cyber threats covered by the CTTP programme
2. the ways in which these components should be simulated and emulated
3. the ways in which cyber-attacks against the cyber system may manifest themselves
4. the actions that trainees are expected to take against these attacks and the tools that may be used for this purpose, and
5. 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 a cyber-system, i.e., the software architecture layer (SAL) and the physical architecture layer (PAL). It

also covers dependencies between components in SAL & PAL. The SAL part of the CTTP model is an application-level model of the cyber system, specifying the different software components of it (e.g. data repositories and servers, client facing dashboards, clients and drivers running on external devices, etc.). SAL is specified by a SAL sub-model having the form of a typed directed graph. The nodes of this graph represent the software components of the cyber system and specify: (i) the type of the software component, (ii) any implementation dependencies that the component may have (e.g., on libraries and operating systems), and (iii) the key responses that the component produces upon input stimuli. Part (ii) is important for emulating the component and part (iii) is important for simulating the component. The edges of the SAL model represent call, data and resource dependencies between components (e.g., data flows, access to shared memories).

The PAL part of the CTTP model covers the network and the computational infrastructure used by the cyber system. PAL is specified by a PAL sub-model, which is also a typed directed graph. The nodes of this graph represent the physical components of the cyber system including, for example, computer servers, terminals, network routers and controllers and other telecommunication components, surveillance equipment, sensors and devices that may be used by the system (e.g., external mobile devices, special hardware of industrial automation platforms, healthcare equipment or geolocation devices). PAL model nodes hold information about the properties of the physical component they represent. They describe, for example, the type of the physical component (e.g. desktop, server, routing device, etc.), the key responses that it produces upon input stimuli, and other general capabilities (e.g. number of CPU-cores, storage and memory capabilities). The edges connecting the nodes of the PAL model represent the network-level topology of the cyber system and describe the connection's type and properties such as IP address space, link rate, type of linkage (e.g. wireless, Ethernet, etc.).

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

(a) A deployment model specifying the allocation of the software (SAL) components of the cyber system onto its physical (PAL) components.

(b) 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 behavior 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 assurance sub-model also specifies assessment measures, determining how to detect attacks arising from the threats and assess the effectiveness of the security controls. It also specifies the assessment tools that should be used to realize these measures prior to the deployment of the system (e.g., static analysis and testing tools) or during the operation of the system (monitoring and dynamic testing tools). It will also specify parameters determining how the attacks may manifest themselves, how the security controls may respond to them (e.g., the attack manifestation events captured and detection time, the undertaken response actions) and the outputs that the deployed assessment tools will generate for the situation.

3.2 Motivating Example – Smart Energy Home

We demonstrate the application of CTTP modeling on a smart energy scenario, where energy is collected by solar panels installed in houses. The solution is provided by the Lightsource company in Ireland. **Fig. 1** depicts the main application modules.

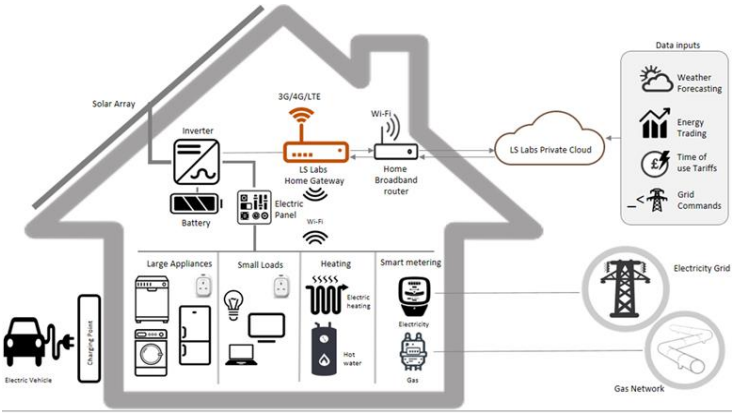

Fig. 1. Smart energy system architecture

Fig. 2 and **Fig. 3** show the PAL and SAL parts of the CTTP model of a smart energy metering cyber system for smart homes. As shown in **Fig. 2**, at the PAL layer, this cyber system consists of a number of smart-meters (i.e., SM-1, ... , SM-n), and a number of photovoltaic sensor devices (i.e., Sensor-1, ... , Sensor-n). The smart-meters are connected to the Smart Meter Server while the sensors are connected to the Sensor Server for monitoring and management purposes. The two servers are connected to the Main Server (Gateway), which is equipped with a hardware Security Device (i.e., trusted platform module (TPM) enabled host). The entire system is connected to the internet via firewall equipment.

As shown in **Fig. 3**, the SAL layer of the smart metering system consists of an external communication service, used by third party operators, and an internal communication service. The two services are connected and share a set of software security tools offering authentication and security monitoring. The external communication service interfaces with an Intrusion Detection System (IDS), connecting the entire system to the Internet. The internal communication application is used for interconnecting the smart-meter monitoring and command service with the sensor monitoring and command service. The two monitoring and command services are used in order to collect information from the smart-meters and photovoltaic sensors, issue control commands and act as dashboards for data visualization. They also interface with the appropriate software and firmware solutions, driving the various sensors and smart-meters, towards data and command exchange. **Fig. 3** depicts the SAL layer as graph.

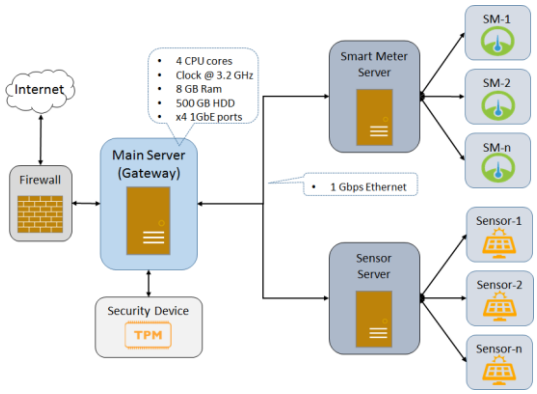

Fig. 2. PAL sub-model of the CTTP model of a smart metering system.

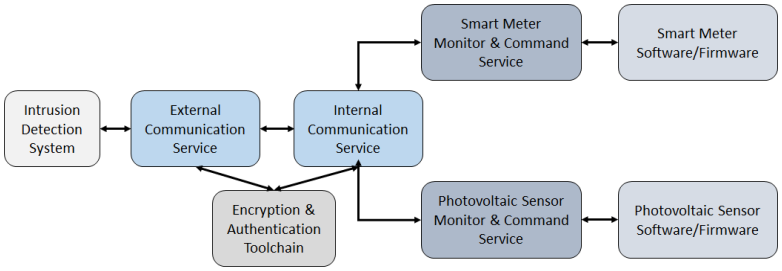

Fig. 3. SAL sub-model of the CTTP model of a smart metering system.

The deployment of SAL components onto PAL components is shown in **Fig. 4**. In particular, we can see that some PAL components are used in order to host a single SAL component, such as the firewall solution. Multiple software services are hosted on a single device, such as the two communication services, while on the other hand software components depend on multiple PAL components, such as the smart-meter and sensor software/firmware components. As we can see, the deployment sub model is conceptualized as a three-dimensional graph, indicating the relation between the PAL and SAL sub-models, where a node of each level may have dependencies to one or multiple nodes of the same or different level.

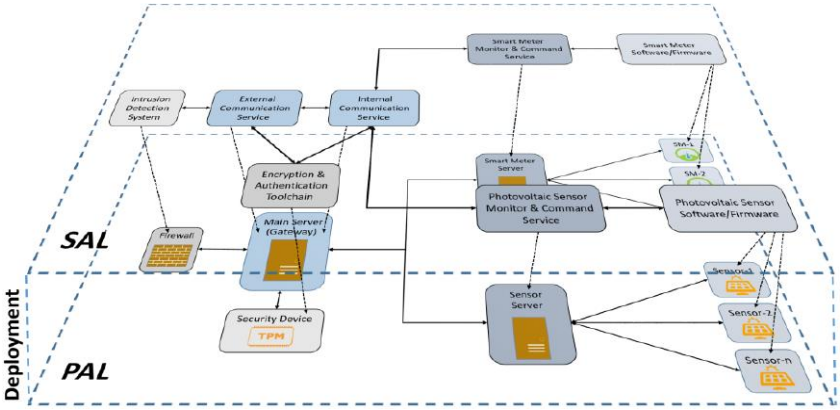

Fig. 4. PAL, SAL and deployment sub-models of the CTTP model of a smart metering system.

A part of the assurance model of the smart metering system in our example is shown in **Fig. 5**. This model specifies threats for system components, assumptions affecting the manifestation of them, and the security controls that are used to mitigate the threats. The model shown in **Fig. 5** is based on the protection profile for smart gateways specified in [30]. According to the part of the model shown in the figure, the smart metering system gateway is threatened by Time Modification, Local Data Disclosure, Resident Data and Privacy threats. For each of these threats, the model specifies:(a)assumptions regarding the behavior of system components and actors that affect the manifestation of the threat (e.g. the assumption that system administrators are trusted - A.TrustedAdmins) - and (b) the security controls which are used to mitigate the threats (e.g. the use of user authentication before any action - i.e. FIA. UAU.2). CTTP models of the form described above will provide the basis for generating training scenarios involving the simulation and/or emulation of cyber system components, attacks launched upon them, and the use of assessment and response tools.

Based on the threats and parameters of the assurance model, for example, it will be possible to generate synthetic system events corresponding to the manifestation of attacks, feed them onto the emulated or simulated physical or software security controls and observe their response to the simulated attacks. It will also be possible to check the ability of system actors to initiate and use the assessment tools in order to detect the attacks and/or assess the effectiveness of the responses of the security controls, and generate training scenarios to explore the validity of assumptions and the impact of their potential violation (e.g., the possibility of having untrusted admin personnel, as opposed to the assumption A.TrustedAdmins in the assurance model of the smart metering system). The likelihood of a violation of this assumption could also be estimated through the statistical profiling of violation indicators (events) that are collected and analyzed by the assurance tool of the THREAT-ARREST platform.

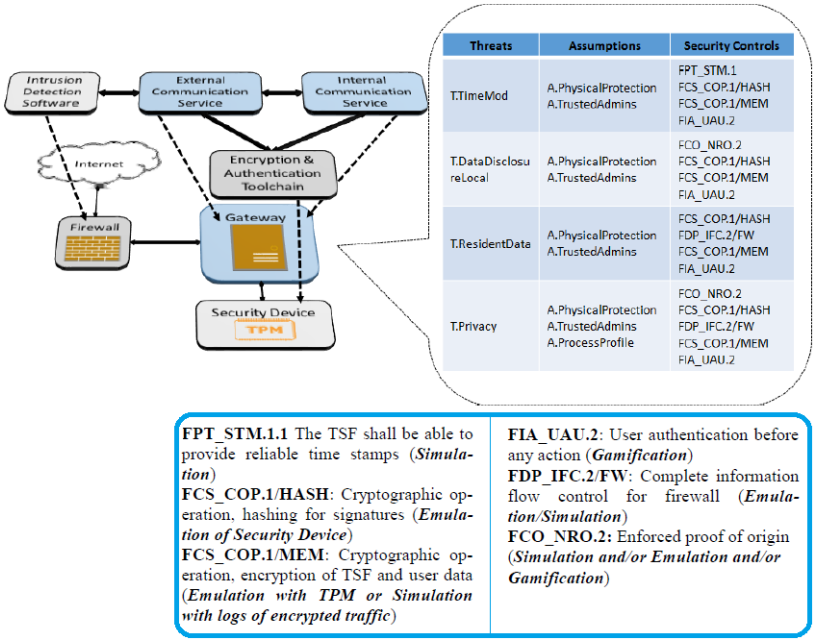

Fig. 5. Assurance model of a smart metering system.

4 Platform Architecture

An initial conceptualization of the platform is shown in **Fig. 6**. As shown in the figure, the envisaged platform will comprise the following key components.

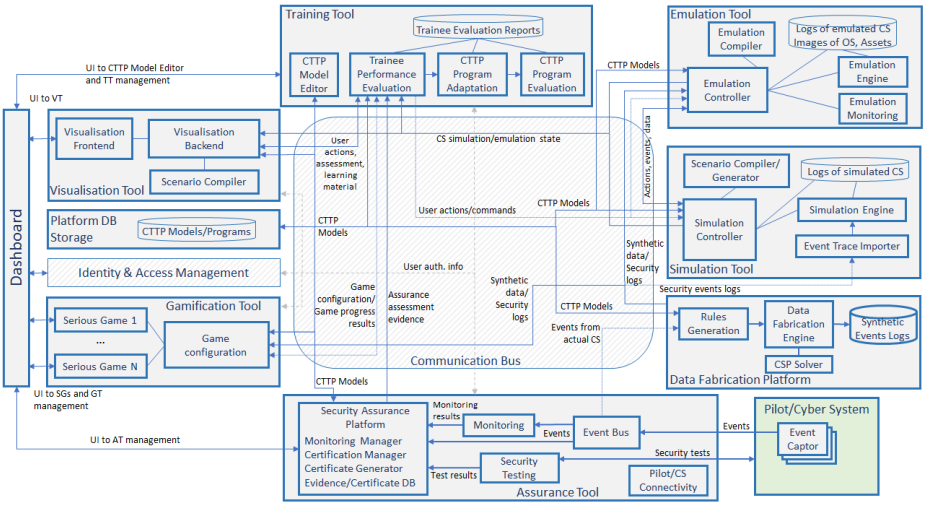

Fig. 6. The THREAT-ARREST platform.

4.1 Assurance Tool

The assurance tool supports the continuous assessment of the cyber system's security through the combination of runtime monitoring and dynamic testing in order to provide information about the actual status. It also collects runtime system events and generates alerts that provide the basis for setting up realistic simulations.

The assurance tool carries out a continuous runtime assessment of the aspects of the target cyber system that are important for CTTP training programme. These aspects are defined by the CTTP model (security assurance sub model). For example, the CTTP model defines the components of the cyber system that should be monitored, the events of these components that are of importance (e.g. operating system calls, external service calls, user actions, etc.), and the conditions that should be satisfied by them. It also defines dynamic system tests that should be executed at runtime and should be combined with monitoring to form hybrid assessments of security [31], [32]. The collected monitoring events and testing outcomes form the operational system evidence that is passed over to simulation component to enable statistical profiling and thereby the generation of realistic simulations.

4.2 Hybrid Training

The CTTP models 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. This hybrid training mode is useful when emulating the entire system is not needed or is not feasible but hands-on experience is required for certain system components. In hybrid training scenarios, trainees will in general be expected to monitor, test and take actions on emulated components, and observe the effects of these actions to the rest of the cyber system following the propagation of these effects through simulation. Hybrid training scenarios will also be useful in cases where the training process is divided in consecutive related parts. Each part may require that specific components should be emulated and the rest could be simulated in order to preserve system resources. Using a hybrid approach, the training platform will be able to terminate the emulation of specific components and proceed with their simulation, as they will not be required for a certain part of the training, or choose to emulate components that used to me simulated in a previous part of the training phase. Overall, the training scenarios that will be supported by THREAT-ARREST will vary with respect to:

- The extent of *system coverage*: With regards to this criterion, scenarios may be distinguished into those involving attacks targeted to: (a) single components of a cyber-system, (b) clusters (i.e., subsets of interconnected) of components of a cyber-system, or (c) the whole set of components of a cyber-system.
- The *type of attacks*: With regards to this criterion, scenarios may be distinguished into those involving: (a) historic attacks, or (b) live attacks unfolding as the scenario is simulated by the platform.
- The *type of response* required: With regards to this criterion, scenarios may be distinguished with regards to the type of response to a security incident that they

are aimed to train people for. Different types of response are typically defined in reference to the phase in the life cycle of an incident that they focus on. These, according to [33], are: (a) preparation/preventive responses (i.e., actions whose aim is to prepare organizations for incident handling and/or prevention), (b) detection and analysis responses, (c) containment, eradication and recovery responses, or (d) post-incident responses.

- The *trainee's profile*: With regards this criterion, scenarios may be distinguished with regards to the initial cognitive profile of the trainee, as obtained from the security games and the performance of the trainee in the training scenarios that he/she has been exposed so far.

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

Beyond supporting the definition of CTTP models and programmes, the training tool will also ensure a high level of interactivity with the trainees and deliver the training scenarios, enabling them to respond, sending the appropriate commands to the emulated and simulated components. Also, it will continuously receive information about the status of the emulation and simulation, evaluating in real time the state of progress based on user's responses and their effects on the components and will determine the overall performance of the trainees. The tool will also be responsible for validating the assumptions of the assurance model based on the trainees' responses to the training scenarios and generate warnings in case these assumptions are violated. It will also be able to assess the performance of trainees and evaluate and adapt CTTP programmes. Finally, the tool will collaborate with the visualization tool for the effective delivery of training.

4.3 Gamification

Beyond simulation, emulation and hybrid-based training, the CTTP model will also drive training based on games. This form of training will focus on developing skills to prevent attacks based on exploiting human factors (i.e., the users) of a cyber-system. The delivery of games based training will be driven by the assumptions of the assurance sub-model, particular those that have to do with human users. Games will be used to test whether the assumptions made in an assurance model are plausible and to gradually improve the ability of human users to behave according to them. For instance, if the target cyber system is equipped with a two-factor user authentication system, using passwords and security tokens, we can assume that the users will change the passwords frequently and abstain from sharing the security tokens. A possible game scenario will pose questions to the users based on these assumptions and their decisions will drive the training procedure. For example, users will be asked if they would share the security token in order to favor a person that gained their trust, simulating a phishing attack. Games will also be used to perform an initial profiling of

trainees in order to establish the form and level of additional types of training (and their difficulty) that would be beneficial for them. For example, a game may be used to test the familiarity of trainees with access controls and depending on it steer any follow up training towards, for example, emulation in order to give trainees a more hands-on exposure to access control.

The gamification tool will host various serious games, scenarios and training evaluation mechanisms, which will enable trainees to develop skills in being resilient to and preventing social engineering attacks (e.g., phishing, impersonation attacks etc.). The games to be provided will be driven by the threats and assumptions specified in CTTP models (security assurance).

Beyond providing serious games, the gamification will also support an initial cognitive profiling of trainees and measure their familiarity with various security issues. This profile will be used in order to adjust the type and level of difficulty of the training process. Moreover, it will prompt the trainees to take part in serious games which test whether they behave according to the security assumptions and policies provided by the security assurance model of CTTP models. Their performance at these games will determine the unfolding of the scenarios and will have impact on the status of the emulated and simulated components. Furthermore, the tool will support post training assessments of trainee awareness (in terms of knowledge, attitudes and behavior) of these types of attacks that will be useful in tailoring other forms of CTTP training.

4.4 Emulation

Based on the CTTP model, it will be possible to emulate SAL and PAL components. Emulation will involve creating live instances of SAL and PAL components such as virtual machines, executing the services/operations available for them, and enabling data and stimuli flows using the network and deployment links connecting them in the SAL, PAL and deployment sub-models. In the smart metering system, for example, components that could be emulated in a CTTP programme include the Smart Meter command service and the security controls shown in **Fig. 5**. Emulation enables training scenarios where the behavior of certain SAL/PAL components cannot be described in sufficient detail to enable the simulation of their behavior, or when hands-on experience of trainees in observing and controlling components is necessary.

In emulations, there will also be emulated clients of the cyber system requesting services from it and trainees will be required to interact with the emulated components (e.g. log in the VMs) and perform certain operations in order to protect the relevant components and through them wider parts of or the entire emulated cyber system. For example, after logging onto a VM they will be able to use testing or monitoring tools to detect an attack, analyze it and respond to it (e.g. deactivating some functionality, strengthening access restrictions, etc.) in real time. Trainees may also be allocated to groups with responsibility of defending specific system components or even be given the role attackers to insight on how attacks can be launched.

4.5 Simulation

The CTTP model will also enable the simulation of the propagation of the effects that attacks on some cyber system components would have on other parts of the system. For instance, the information provided by the CTTP model can be used for the simulation of the propagation of a DDoS attack, targeting the smart gateway on our previous example, and its effects on the simulated hardware and software components. The propagation of such effects will be controlled by simulating the response mechanisms specified for SAL and PAL components and their capabilities and enabling data and other stimuli (e.g. calls) flow across components through the links of the SAL and the PAL sub-models. The effects of attacks may also be propagated from the PAL to the SAL layer (and vice versa) based on component links specified in the deployment model of the CTTP model. Simulations will vary with regards to the level of difficulty that they present to trainees. This level can be controlled by reducing the degree of information that is available for an attack, the time at which this information becomes available following an attack, and the consistency of information generated by the different cyber system security controls and the external assessment tools used.

To ensure the provision of realistic simulations, the THREAT-ARREST framework will continually monitor the real cyber system and log any events of importance related to it. The events to monitor and the types of analysis that will be applied to them will be defined by the assessment measures of the assurance sub-model. The captured assurance related events will be statistically profiled. Statistical profiling will cover event meta data (e.g. the timing of their occurrence and other characteristics such as their sender and receiver) and – where allowable by the applicable security policies – the actual event payload (e.g. data passed between components, parameter values of component operation calls, size of files read or written, etc.).

4.6 Visualization Tool

The visualization tool will enable the graphical representation of simulations and emulations, the effect of training actions on simulated and emulated systems as well as the status of the underlying components.

Using the visualization platform, the framework's operators will be able to select the desired training scenarios and tune their parameters. Moreover, this platform will be able to parse and visualize the CTTP model and the sub-models described in the previous sections and present the appropriate graphs to the users. The operators will utilize these graphs to select which parts of the cyber system should be simulated or emulated. The visualization platform is also responsible for the representation of the status of the simulated/emulated components and the effects of the training actions.

5 Conclusions

This paper presented the THREAT-ARREST solution – a platform for advanced cyber security training for medium to large organizations. At first, the organization's real system is analyzed, revealing the most severe threats and vulnerabilities. Then, a

training programme is established which adheres to the organization's specific needs. The various concepts are formed as CTTP models and the overall learning procedures are monitored and adapted at runtime. Except from the ordinary on-line educational material (e.g. lectures, tutorials, videos, etc.), the advanced hybrid training involves serious games as well as emulated/simulated scenarios. The overall approach can cover the training against known and new attack cases and prepares the trainer to be able to detect, respond, and mitigate them under realistic circumstances.

6 Acknowledgements

This work has received funding from the European Unions Horizon 2020 research and innovation programme under grant agreements No. 769066 (RESIST) and No. 786890 (THREAT-ARREST).

References

1. Intel: A guide to the Internet of Things. Intel, 2015. https://www-ssl.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html.
2. Storm, D.: Hackers allegedly attack Polish LOT airline, 10 flights and over 1,400 people grounded. ComputerWorld, article 2938485, June 22, 2015.
3. Khandelwal, S.: United airlines hacked by sophisticated hacking group. The Hacker News, July 30, 2015.
4. Hirschfeld J. D.: Hacking of government computers exposed 21.5 million people. The New York Times. July 9, 2015.
5. Newcomb, A.: Anthem hack may have impacted millions of non-customers as well. ABC News, February 25, 2015.
6. Al-Ghamdi, A. S. A.-M.: A survey on software security testing techniques. International Journal of Computer Science and Telecommunications, vol. 4, issue 4, 2013, pp. 14-18.
7. Salas, M.I.P., Martins, E.: Security testing methodologies for vulnerabilities detection of XSS in Web services and WS-Security. Electronic Notes in Theoretical Computer Science, Elsevier, vol. 302, 2014, pp. 133-154.
8. Hatzivasilis, G., et al.: AmbISPDM. Applied Intelligence, Springer, vol. 48, issue 6, pp. 1623-1643, 2017.
9. Santa, I.: A users' guide: how to raise information security awareness. ENISA Reports, November 29, 2010, pp. 1-140.
10. Manifavas, C., et al.: DSAPE – Dynamic Security Awareness Program Evaluation. HCI International, June, 2014, Heraklion, Greece, Springer, LNCS, vol. 8533, pp. 258-269.
11. Bird, J., Kim, F.: Survey on application security programs and practices. A SANS Analyst Survey, 2014, pp. 1-24.
12. Trustwave: Security testing practices and priorities. An Osterman Research Survey Report, 2016, pp. 1-15.
13. Hatzivasilis, G., et al.: WARDOG: Awareness detection watchdog for Botnet infection on the host device. IEEE Transactions on Sustainable Computing – Special Issue on Sustainable Information and Forensic Computing, May 2019, pp. 1-18.
14. Hatzivasilis, G., et al.: CloudNet Anti-Malware Engine: GPU-Accelerated Network Monitoring for Cloud Services. IOSec, Springer, LNCS, 11398, 2018, pp. 122-133.

15. Hatzivasilis, G.: Password-Hashing Status. Cryptography, MDPI Open Access Journal, vol. 1, issue 2, number 10, 2017, pp. 1-31.
16. Shillair, R., et al.: Online safety begins with you and me: Convincing Internet users to protect themselves. Computers in Human Behavior vol. 48, 2015, pp. 199-207.
17. Safa, N. S. and Rossouw V. S.: An information security knowledge sharing model in organizations. Computers in Human Behavior, vol. 57, 2016, pp. 442-451.
18. Beckers, K., Pape, S., Fries, V.: HATCH: hack and trick capricious humans – a serious game on social engineering. HCI Conference Fusion, Bournemouth, UK, 2016, pp. 1-3.
19. Boopathi, K., Sreejith, S., Bithin, A.: Learning cyber security through gamification. Indian Journal of Science and Technology, vol. 8, issue 7, 2015, pp. 642-649.
20. Schreuders, Z. C., Butterfield, E.: Gamification for teaching and learning computer security in higher education. ASE, USENIX, Austin TX, USA, 2016, pp. 1-8.
21. SANS: Online cyber security training. https://www.sans.org/online-security-training/ .
22. CYBERINTERNACADEMY: Complete cybersecurity course review on CYBERINERNACADEMY. https://www.cyberinternacademy.com/complete-cybersecurity-course-guide-review/ .
23. StationX: Online cyber security & hacking courses. https://www.stationx.net/ .
24. Cybrary: Develop security skills. https://www.cybrary.it/ .
25. AwareGO: Security awareness training. https://www.awarego.com/ .
26. BeOne Development: Security Awareness Training. https://www.beonedevelopment.com/en/security-awareness/ .
27. ISACA: CyberSecurity Nexus (CSX) training platform. https://cybersecurity.isaca.org/csx-certifications/csx-training-platform .
28. Kaspersky: Kaspersky security awareness. https://www.kaspersky.com/enterprise-security/security-awareness .
29. CyberBit: Cyber Security Training Platform. https://www.cyberbit.com/blog/security-training/cyber-security-training-platform/ .
30. Bundesamt für Sicherheit in der Informationstechnik (BSI) / Federal Office for Information Security, Germany. 2013. Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP).
31. Katopodis, S., Spanoudakis, G. and Mahbub, K.: Towards hybrid cloud service certification models. International Conference on Services Computing, June, 2014, pp. 394-399.
32. Hatzivasilis, G., Papaefstathiou, I., Manifavas, C.: Software Security, Privacy and Dependability: Metrics and Measurement. IEEE Software, vol. 33, issue 4, 2016, pp. 46-54.
33. Cichonski, P., et al.: Computer security incident handling guide. NIST, Special Publication 800-61 v2, 2012, pp. 1-79.