The THREAT-ARREST Cyber Ranges Platform

*Model-driven cyber ranges design and continuous assurance of the security posture

George Hatzivasilis, Sotiris Ioannidis
Institute of Computer Science
Foundation for Research and Technology – Hellas (FORTH)
Heraklion, Crete, Greece
{hatzivas, soiris}@ics.forth.gr

Michail Smyrlis, George Spanoudakis
Innovation Department
Sphynx Technology Solutions AG
Zug, Switzerland
{smyrlis, spanoudakis}@sphynx.ch

Fulvio Frati, Chiara Braghin, Ernesto Damiani
Department of Computer Science
University of Milan
Milano, Italy
{fulvio.frati, chiara.braghin, ernesto.damiani}@unimi.it,

Hristo Koshutanski
Atos Research & Innovation
Atos Spain SA
Madrid, Spain
hristo.koshutanski@atos.net

George Tsakirakis
Research and Development Department
ITML
Athens, Greece
gtsa@itml.gr

Torsten Hildebrandt
Research Department
SimPlan
Hanau, Germany
torsten.hildebrandt@simplan.de

Ludger Goeke
Innovation Department
Social Engineering Academy
Frankfurt, Germany
ludger.goeke@social-engineering.academy

Oleg Blinder, Michael Vinov
Research Department
IBM Israel
Haifa, Israel
{olegb, vinov}@il.ibm.com

George Leftheriotis
Systems Certification Department
TUV Hellas
Athens, Greece
tglefthe@tuv-nord.com

Martin Kunc
Research Department
CZ.NIC ZSPO
Praha, Czech Republic
martin.kunc@nic.cz

Fotis Oikonomou
Applied Research Department
DANAOS Shipping Company
Limassol, Cyprus
drc@danaos.com

Robert Bordianu
Lightsource BP
Dublin, Ireland
robert.bordianu@lightsourcelabs.com

Giovanni Magilo
Research Department
ARESS
Puglia, Italy
giovannimaglio@gmail.com

***Abstract*—Emerging technologies are facilitating our daily activities and drive the digital transformation. The Internet of Things (IoT) and 5G communications will provide a wide range of new applications and business opportunities, but with a wide and quite complex attack surface. Several users are not aware of the underlying threats and most of them do not possess the knowledge to set and operate the various digital assets securely. Therefore, cyber security training is becoming mandatory both for simple users and security experts. Cyber ranges constitute an advance training technique where trainees gain hands-on experiences on a safe virtual environment, which can be a realistic digital twin of an actual system. This paper presents the cyber ranges platform THREAT-ARREST. Its design is fully model-driven and offers all modern training features (i.e. emulation, simulation, serious games, and fabricated data). The platform has been evaluated under the smart energy, intelligent transportation, and healthcare domains.**

Keywords—security training, cyber range, security assurance, learning path, security assessment, smart energy, smart shipping, healthcare

I. INTRODUCTION

The evolution of the Information and Communications Technology (ICT) has created a new technological landscape [1]-[2], exploiting among others high-performance computing, 5G communications, advance machine learning (ML) and artificial intelligence (AI), augmented and virtual realities (AR and VR), Big Data analytics, social networking, mobility, and the Internet of Things (IoT).

The increased systems' interactions and complexity leave fruitful space for the currently known security vulnerabilities to survive and expand, as well as for new threats to emerge [3]. The market demand for skillful professionals is expected to grow drastically, and security awareness and training programmes are going to become a necessity, both for individuals and organizations.

Cyber ranges (CRs) form a special method of cyber security training and is considered as a promising solution for the educational needs of this digital era [4]-[5]. Apart from the traditional in-class or on-line educational means (e.g. lectures, tutorials, reading material, etc.), with CRs the learner has the opportunity to gain hands-on experience on setting, defending, or even attacking a system by practicing on a legal, safe, and virtual environment. The trainer creates a virtual lab which may resemble an actually operational system or subsystem. There, the trainee can learn how to administrate mainstream and/or advance security mechanisms, try different configurations and settings, and assess the overall results under realistic attack scenarios. The virtual environment is instantiated or destroyed on demand for each trainee, and the process can be repeated again-and-again. Nevertheless, the design and development of

even a mainstream programme requires significant expertise, time, and effort by the trainer.

Thereafter, the trainee can follow the defined learning path to obtain knowledge and acquire new skills, complete a full programme, and earn a relevant certification []. However, the fact that someone fulfils the training and learning requirements does not mean that he/she will also adopt automatically his/her behavior in the digital world accordingly. On the contrary, several researches have revealed that only a small percentage of the learnt concepts (around 10%-40%) is automatically embraced by individuals. This is an important problem for organizations, especially those ones that operate critical infrastructures, as non-compliance of their personnel to the defined security policies is deriving the deployed protection mechanisms inadequate and the underlying systems vulnerable to attacks. Thus, the real efficacy of training itself, even with advance CRs, is still a perspective that needs to be significantly improved.

This paper presents the EU-funded CR, called THREAT-ARREST (www.threat-arrest.eu). The platform marshals modern training methods (i.e. emulation, simulation, gamification, and fabrication of realistic synthetic data) to enhance the learning experience for trainees. The overall process is fortified with pedagogical methodologies (i.e. Bloom's revisited taxonomy and Kolb's experience gaining life-cycle) to define the learning path and ensure the learning outcomes. Moreover, the educational scope can be designed in such a way that it will cover the requirements and demands for professional certification schemes from organizations like ISACA and ISC^2. This option will further increase the acceptability of a specific CR platform in the market.

The paper is structured as follows. Section II positions the THREAT-ARREST CR with respect to the related work. Section III presents the main CR capabilities and the tools implementing those capabilities, while Section IV draws conclusions and future work. Appendix A shows the main tools' interactions underpinning training scenarios executions.

II. Related Works

A. Cyber Ranges Platforms

Overviews of cyber security training in critical infrastructures (e.g. nuclear, energy, healthcare, transportation, and aviation sectors), are documented in [6]-[9]. Today, the demand for security experts is continuously increasing [6]. CRs constitute a promising solution of advance training, which could fill the gap by enhancing educational material with hands-on experiences.

The majority of the CR platforms are developing automated mechanisms to easy the implementation of training scenarios, virtual labs, and the trainees' evaluation [8]-[9].

Online platforms, like, edX, Coursera, and Udacity, provide general-purpose training and offer main cyber security courses. Specialized platforms, such as SANS [10], Cybrary [11], StationX [12], CyberInternAcademy [13], and AwareGO [14] focus on individual learners whose target is to sharpen existing or develop new skills. Nonetheless, such solutions fail when it comes to hands-on experiences on actual systems or CRs.

Identify applicable funding agency here. If none, delete this text box.

BeOne Development has developed its own platform for security awareness training [15]. This solution involves awareness videos, e-learning modules, and simulation modules. Thereupon, the BePhished simulator is used especially for training on phishing attacks. To easy the creation of training exercises, BeOne implements the Security Awareness Library that includes 28 learning contents. Cultural differences and multinational working environments are considered, as education is more effective if the learnt examples are correlated with the trainees' daily activities. This platform provides generic and pre-packaged programmes, organization-specific look and feel, or customized programmes which are designed in close collaboration with a client's experts. The BeOne solution offers generic teaching procedures for the core training and the advance simulation-centric training focuses on phishing assaults.

ISACA implemented the CyberSecurity Nexus (CSX) platform [16]. It offers lectures and hands-on lab exercises on real systems. The learner gains experience by practicing main concepts and industry-leading methodologies. Capture-the-flag (CTF) exercises are also provided, improving the learners' technical capabilities. Trainees are evaluated and the target is to gain related professional certifications. Thereafter, the chief information security officer (CISO) for an organization can hire personnel with the required skills.

Kaspersky provides enhanced computer-based training programmes for all organizational layers [17]. Apart from online training, the tool offers benchmarking against industry/world averages, as well as realistic gamification and simulation. It implements an internal learning and educational schedule with constant reinforcement, provided automatically via a mixture of training formats, involving learning modules, tests, email reinforcement, and/or simulated phishing campaigns. The platform monitors the learners' progress through a user-friendly dashboard, providing also forecasts, trends, and live data tracking.

CyberBit's platform offers realistic simulation of cyber-attacks in a mirror system of a real network with a security operations center (SOC) [18]. This CR is composed of a virtual network (digital twin of a real setting), the traffic generator (benign data), the attack engine (malicious traffic), and the virtual SOC (learners' point of view). The target is to simulate hyper-realistic CRs. This solution offers various training scenarios, like pentesting and incident response. The educators set up the training sessions that include session monitoring, trainee assessment, debriefing, and scenario administration. Scenario customizations are also supported through a graphical interface.

The THREAT-ARREST solution supports training on known as well as new advanced cyber-attack scenarios, taking different type of actions, such as preparedness, detection and analysis, incident response, and post incident response. THREAT-ARREST offers monitoring, assessment, and security testing for various layers in the implementation stack, like:

- Network layer modules (such as honey-pots/honeynet, firewalls, intrusion detection systems, etc.)

– Infrastructure layer (e.g. passive and active penetration testing, security monitors, etc.)

– Application layer (like code analysis, security monitors, and penetration testing)

The overall process starts by assessing the organization's security posture. The Assurance Tool estimates the current level of security and reports the most critical security issues, based on which the training process is designed. Thereafter, hybrid training programmes are developed, customized to the organization's demands and the underlying trainee groups. This involves the educational material along with serious games and the emulation/simulation of the CR system. THREAT-ARREST also supports continuous evaluation of: (a) the individual trainees' performance in specific courses; and (b) the efficacy of complete programmes across trainees' groups and the organization as a whole. Those assessments are utilized for the customization of programmes to the skills of individual trainees or adjustment at a more macroscopic perspective.

Table 1 documents a qualitative comparison for these CR platforms. THREAT-ARREST incorporates all modern training features of serious gaming, simulation, and emulation in a unified manner, and provides continuous security assessment and training adaptation based on the trainee's capabilities.

TABLE I. 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

B. *Adopting Training in the Workplace*

Even though there is an increasing need for modern security training and advance CR platforms (e.g. with games, simulation, emulation, etc.), the transfer of the learned capabilities from the trainees to their workplace and the adaptation of the organizational operations have been totally neglected in almost all cases (e.g. ([6], [7], [8]). Noncompliance of users with the security policies that the organization has defined is of main concern ([20], [7], [19]). If the personnel do not totally follow such policies, the effectiveness of the deployed defenses is lost. From the different compliance methods, effectual training is the most widely used one.

Nonetheless, only a few studies are assessing the effects of professional training to organizations and promote compliance policies in the workplace ([20], [7]). Also, only in rare cases theory is used to evaluate the aspects that affect trainees' compliance with security policies or even present empirical evidence from actual training. Ordinarily, it is believed that training programmes have to utilize procedures and material which can actively engage learners and motivate them to systematic cognitive processing of the underlying contents ([6], [9]). Apart from novel technical features (such as gamification and simulation), the continual communication between the instructor with the trainees is vital for the enhancement of the individuals security compliance ([6], [20], [9]).

Researchers usually integrate pedagogical principles as the main approach to advance learners' compliance ([7], [19], [9]). In 1998, Baldwin and Ford [21] defined the transfer of learning to the workplace as "the degree to which trainees effectively apply the knowledge, skills, and attitudes gained in the training context to the job".

However, it is recorded that approximately only 10%-40% of all training experiences would be transferred to the working environment ([22], [6], [7]). Furthermore, as time passes from the programme's completion, trainees tend to become less motivated in retaining the obtained operational behaviors (i.e. after twelve months). Therefore, for the currently supported technical solutions and methodologies, only a small percent of the learnt outcomes would be permanently transferred to the workplace. Thus, improving learning transfer constitutes the main concern of novel cyber security training platforms. This is also one of the main THREAT-ARREST goals with the developed continuous adaptation and assurance mechanisms, which are presented in the following section.

III. THE THREAT-ARREST PLATFORM

A high-level view of the THREAT-ARREST platform is depicted in Fig. 1. The main components are presented in the subsections below, while components' interactions (sequence of steps) for scenario initialization, training and disposal are given in the Appendix.

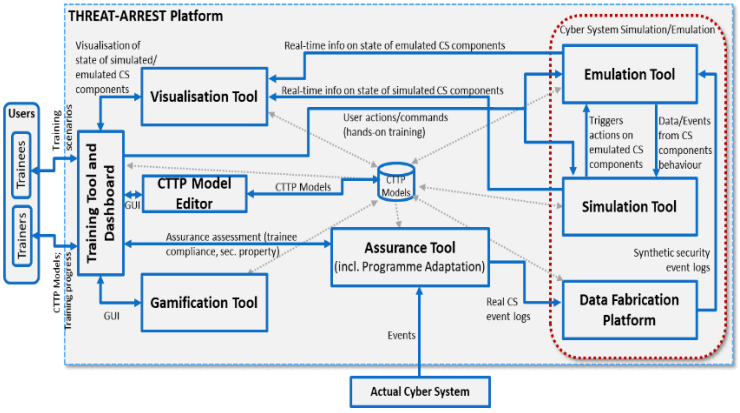


Fig. 1. The THREAT-ARREST platform

A. *The Assurance Tool*

The Assurance Tool provides continuous evaluation of the operational system's security posture via the integration of dynamic testing and runtime monitoring [4]. The tool also gathers system events at runtime and produces notifications

which consist the basis for designing realistic virtual labs (with emulated/simulated components and serious games).

The Assurance Tool performs a continuous runtime evaluation of system aspects that are significant for the definition of a Cyber Threat and Training Preparation (CTTP) programme. These features are determined in the CTTP model (security assurance sub model). For example, the CTTP model determines the system components which should be monitored, the relevant events that are of importance (like user actions, external service calls, operating system calls, etc.), and the conditions which they have to satisfy. Moreover, it deploys dynamic system tests which are performed at runtime and are incorporated with monitoring to implement hybrid security evaluations [23], [24]. The gathered monitoring information and testing results are the operational system evidence. This data is parsed to simulation components and enables statistical profiling, as well as the production of realistic simulations.

B. Hybrid Training

The CTTP models can define virtual labs with hybrid training scenarios by combining emulated and simulated components. In this case, some of the system components are emulated (implement the full component functionality, i.e. a VM) while the rest ones are simulated (deploy only the main part of the component's functionality/interactions, e.g. a simple program that outputs a temperature value, representing a sensor of a smart home etc.). Hybrid training becomes quite useful when the emulation of the entire system is not feasible or required, and obtaining hands-on experiences is requested for specific system components. With hybrid scenarios, learners are expected to monitor, test, and act on emulated components, while observing the effects to the rest cyber system and their propagation through simulation. In some occasions, simulation may be also preferred to retain the CR resources, as in practice it will be less demanding than emulation. The CR platform could also terminate specific emulated components at some time-point and continue with their simulated versions (e.g. in case that they would not be needed for a certain training phase), or decide to emulate components that were simulated in a previous training stage. Totally, the training scenarios that can be deployed by THREAT-ARREST vary based on:

- The *system coverage* level: With respect to this factor, scenarios can be distinguished into those engaging attacks that focus on: (i) single system components, (ii) clusters (e.g. subsets of interconnected) of system components, or (iii) all system components.
- The *attacks type*: With respect to this factor, scenarios are distinguished into those performing: (i) historic attacks, or (ii) live attacks that are executed as the simulated/emulated scenario is propagated by the CR platform.
- The required *response type*: With respect to this factor, scenarios are differentiated based on the required response to a security incident. Different responses are determined according to the different training stages. Such responses include [25]: (i) preparation/preventive actions, (ii) analysis and detection, (iii) containment, eradication, and recovery activities, and/or (iv) post-incident actions.
- The *trainee's profile*: With respect to this factor, scenarios are differentiated based on the cognitive trainee's profile, as disclosed by introductory security games and the trainee's performance on the training scenarios where he/she has been exposed so far.

The permitted variability forms based on the criteria above, are determined as part of scenarios constructing the CTTP programme. Via an Editor, the Training Tool supports the definition of CTTP models and programmes, the assignment of learning exercises/materials for CTTP programmes, allow trainees' responses to deployed threats, communication with the emulated/simulated components, assessment of the trainees' performance, as well as evaluation and adaptation of a CTTP programme as a whole.

Except from the CTTP models and programmes definitions, the Training Tool supports a high interactivity level of the trainee with a training scenario, allowing him/her to respond and/or send appropriate commands to emulated/simulated components. Moreover, it continuously collects information concerning the emulation and simulation status, assesses in real time the scenario progress based on trainee's responses and their effects on components, and calculates the overall trainee's performance. The tool also validates the assumptions defined in the assurance model based on the trainee's responses to the instantiated scenario and produces notifications when such assumptions get violated. The Training Tool evaluates the trainee's performance, as well as assesses and adapts the whole CTTP programmes. Finally, this tool interacts with the Visualization Tool for the effective training delivery.

C. Gamification

Except from emulation, simulation, and hybrid-based training, a CTTP model can also provide training via serious games. Such training targets on advancing skills to block attacks based on exploiting human aspects (e.g. the users) of a cyber system. The support of game-based training is correlated with the assumptions from the assurance sub-model, specifically those ones which involve human users. Games can test whether these assumptions are plausible and to gradually advance the users' ability to behave according to them. For example, if the targeted system applies a two-factor user authentication mechanism, requiring security tokens and passwords, it is considered that users would alter their passwords in a frequent basis and refrain from sharing the tokens. A relevant gamification scenario would make to the user questions concerning those assumptions and the answers would drive the training propagation. For instance, trainees can be asked wherever they would share their security tokens to favor another person who gained their trust, simulating a phishing attempt.

Games are also utilized for the initial profiling of trainees in order to disclose the trainee's cyber security skills and determine the appropriate form of training (and its difficulty) which could be sufficient for them. Therefore, an introductory game is utilized for the evaluation of the trainee's familiarity with access controls, and based on it, drive any follow up training towards,

for instance, emulation for a more hands-on exposure to access control aspects.

The Gamification Tool host various serious games (i.e. PROTECT [26] and AWARENESS QUIZ [27]), scenarios, and training evaluation mechanisms, which allow a trainee to develop skills in preventing and being resilient to social engineering assaults (e.g. phishing campaigns, impersonation attempts, etc.). These games are driven by the assumptions and threats from the related security assurance CTTP models.

Finally, this tool can facilitate post training evaluations of trainees' awareness (in terms of knowledge and attitudes) for the trained attack types.

D. Emulation

Based on the CTTP model, The Emulation Tool can emulate software and hardware components, defined as Software Architecture Layer (SAL) and Physical Architecture Layer (PAL) elements [5]. The tool creates live instances of SAL and PAL components like VMs, performing the available operations/services for them, and enabling data and stimuli flows utilizing the deployment and network links connecting them in the SAL, PAL, and deployment sub-models. Emulation is utilized when the behavior of specific SAL/PAL components cannot be sufficiently described in detail to permit the simulation of its behavior, or when trainee's hands-on experience in controlling and observing these components is necessary.

With emulations, there are also emulated clients of the cyber system requesting services from it, and trainees have to interact with the emulated components (e.g. login a VM) and execute specified actions to defend the related components, and via them, wider parts of or even the entire emulated setting. For instance, after accessing a VM, trainees can make use of monitoring and testing tools to identify attacks, examine them, and respond to them in real time (e.g. strengthening access restrictions, deactivating some functionality, etc.). Learners can also be assigned to groups with accountability of defending certain system components or even act as attackers to insight on how an attack can be performed.

E. Simulation

The CTTP model can deploy the simulation of attacks on some system components or the propagation of the side-effects on other parts of this system [5]. For example, the provided CTTP model information can drive the simulation of distributed denial of service (DDoS) attack propagation, targeting a smart home gateway, as well as the effects on the simulated SAL and PAL components. The propagation of those side-effects is controlled by simulating the response operations determined for SAL and PAL elements and enabling data and other stimuli (e.g. calls) flow across components via the links of the SAL and PAL sub-models. The attacks' side-effects might be also propagated from the PAL to the SAL level (and vice versa) based on component links determined in the deployment model of the CTTP model. Simulations can vary based on the difficulty level which they present to the trainee. This level is controlled by limiting the degree of information which is available for an attack, the time when such information becomes available following the attack, and the consistency of data generated by the different system's security mechanisms and the external utilized assessment tools.

To enable realistic simulations, the THREAT-ARREST framework is continuously monitoring the real operational system and logs any significant events related to it. The events to audit and their analysis type is determined by the assessment measures of the assurance sub-model. Then, the captured assurance relevant events are statistically profiled. Statistical profiling covers event meta data (such as the timing of their happening or other features like their sender and receiver) and – where allowable by the applicable security policies – the actual event payload (like data passed among the components, parameter values for component operation calls, size of files written or read, etc.).

F. Visualization

The Visualization Tool enables the graphical representation of emulations and simulations, the effect of training actions on emulated/simulated components, and the state of the relevant components.

Utilizing the visualization framework, the THREAT-ARREST platform's operator can choose the desired training scenarios and configure their parameters. Furthermore, the platform can parse and visualize the CTTP model and the sub-models described in the sections above, and present the relevant graphs to the users. The operator can use those graphs to pick the system parts that will be emulated or simulated. The Visualization Tool is also responsible for the representation of the status of the emulated/simulated components and the effects of the training actions.

G. Data Fabrication

The Data Fabrication Platform (DFP) [28] is a web-based platform for generating high-quality structured data for testing, development, and training. The methodology used is termed "model-based rule-guided fabrication". DFP consumes data declaration directives (data model or metadata) along with user-defined rules as input, creates a Constraint Satisfaction Problem (CSP), and solves the problem using a proprietary CSP Solver, which has been used for verifying IBM hardware systems for over a decade.

Two types of synthetic data have been used for the THREAT-ARREST objectives:

(i) Static general-purpose synthetic data, such as health records, for the needs of setting/performing a given training scenario;

(ii) Static or dynamic (interactive) security (event) logs for cybersecurity training in the context of a training scenario, such as security logs regarding malicious (anomalous) accesses to a server hosting a database of health records.

In the first case (i), data is modelled in advance via the DFP web-based user interface and fabricated off-line, before a training session starts. Fabricated data is populated in predefined databases and/or predefined file locations to be deployed and consumed in a virtual lab environment.

In the second case (ii), a dedicated data fabrication functionality has been exposed through REST API so that other platform components can dynamically request data fabrication. For instance, during scenario initialisation the Training Tool initialises a data fabrication process while upon successful confirmation of log fabrication finalisation, the Emulation Tool fetches the fabricated logs and deploys those in the corresponding VMs of the Virtual Lab environment.

H. Trainee Competency Evaluation && Certification

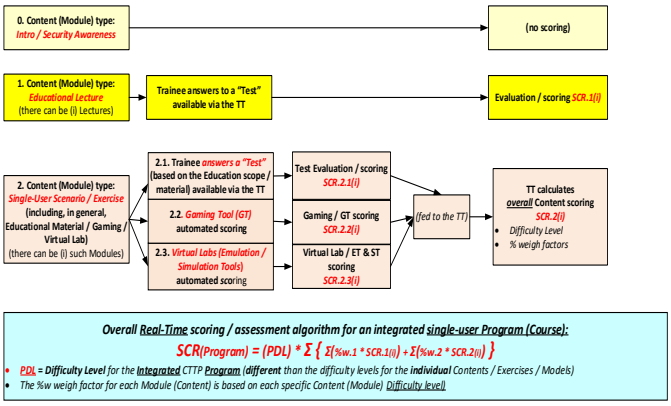
Consolidating, the overall Trainee Scoring & Competency Evaluation consists of:

1. ***Real-time*** Assessment & Scoring, comprising:

- *Quantitative* (automated) scoring, based on platform tools monitoring (including time-metrics) and the relevant information derived from the CTTP models;
- *Qualitative* (manual) scoring, where the Trainee answers on-line tests / questionnaires.

2. ***"After-Action-Review" (AAR)*** evaluation, where, following the completion of an integrated CTTP Programme, the *Trainer* gives an overall Trainee evaluation report – an opportunity for a qualitative, overall Trainee Evaluation feedback.
3. ***"Long-term"*** Trainee performance / skills improvement assessment (Assurance Tool implementation / monitoring of Trainees' performance and actions in the actual cyber-system / cyber-system security posture assessment, performed *pre*- and *post*-Training, in order to assess the Trainees actions in the actual cyber-systems and in the long-term).

Regarding the Trainee Real-time (automated) scoring, a typical case / scoring process is depicted below in Figure 2



Finally, a Trainee can be Certified after successfully finishing an Integrated CTTP Programme (course) and following the standardized training & competency evaluation procedures explained in the previous sections.

IV. Conclusions

This paper described the THREAT-ARREST approach – a cyber ranges platform for advanced cyber security training for medium to large organizations. Initially, the organization's real system is analyzed, disclosing the most severe vulnerabilities and threats. Thereupon, a training programme is developed which adheres to the organization's specific requirements. The various elements are defined as CTTP models and the overall learning processes are assessed and adapted at runtime. Apart from the typical on-line educational content (e.g. lectures, videos, tutorials, etc.), the advanced hybrid training incorporates serious games and emulated/simulated virtual labs. The overall solution can cover the training against known and new attacks, and prepares trainees to detect, respond, and mitigate them under realistic conditions.

Future work includes extending end user validation of platform capabilities with organizations of different domains (energy, healthcare, smart shipping), extending platform integration and federation with other Cyber Ranges[1] both on a technical level scenario interoperation and on a conceptual (capability, taxonomy) level to further expand and align with end user needs of training.

Acknowledgment

This work has received funding from the European Union Horizon's 2020 research and innovation programme under the grant agreements No. 786890 (THREAT-ARREST) and No. 830927 (CONCORDIA).

References

[1] Hatzivasilis, G., et al.: SPD-Safe: Secure administration of railway intelligent transportation systems. Electronics – Special Issue on Advances in Public Transport Platform for the Development of Sustainability Cities, MDPI Open Access Journal, January 2021, vol. 10, issue 1, article 92, pp. 1-26.

[2] Hatzivasilis, G., et al.: AI-driven composition and security validation of an IoT ecosystem. Applied Sciences – Special Issue on Smart City and Multi-Agent Systems, MDPI Open Access Journal, August 2020, vol. 10, issue 14, article 4862, pp. 1-31.

[3] Maghool, S., et al.: The coevolution of contagion and behavior with increasing and decreasing awareness. PLOS ONE, December 2019, vol. 14, issue 12, article: e0225447, pp. 1-22.

[4] Somarakis, I., et al.: Model-driven Cyber Range Training – The Cyber Security Assurance Perspective. 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Luxembourg, September 2019, Springer, LNCS, vol. 11981, pp 172-184.

[5] Braghin, C., et al.: Towards the Monitoring and Evaluation of Trainees' Activities in Cyber Ranges. 2nd Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Guildford, UK, September 2020, Springer, LNCS, vol. 12512, pp. 79-91.

[6] Chouliaras, N., et al.: Cyber ranges and testbeds for education, training, and research. Applied Sciences 2021, 11, 1-23.

[7] Chowdhury, N., Gkioulos, V.: Cyber security training for critical infrastructure protection: A literature review. Computer Science Review 2021, 40, 1–20.

[8] Gustafsson, T., Almroth, J.: Cyber range automation overview with a case study of CRATE. 25th Nordic Conference on Secure IT Systems (NordSec), Springer, LNCS 2021, 12556, 192–209.

[1] Such as the ECHO approach at https://echonetwork.eu/wp-content/uploads/2021/04/HEADLINE_E-FCR-FIRST-RELEASE.pdf

[9] Hatzivasilis, G., et al.: Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. Applied Sciences 2020, 10, 1–26.

[10] SANS: Online cyber security training. https://www.sans.org/online-security-training/ .

[11] Cybrary: Develop security skills. https://www.cybrary.it/ .

[12] StationX: Online cyber security & hacking courses. https://www.stationx.net/ .

[13] CYBERINTERNACADEMY: Complete cybersecurity course review on CYBERINERNACADEMY. https://www.cyberinternacademy.com/complete-cybersecurity-course-guide-review/ .

[14] AwareGO: Security awareness training. https://www.awarego.com/ .

[15] BeOne Development: Security Awareness Training. https://www.beonedevelopment.com/en/security-awareness/ .

[16] ISACA: CyberSecurity Nexus (CSX) training platform. https://cybersecurity.isaca.org/csx-certifications/csx-training-platform .

[17] Kaspersky: Kaspersky security awareness. https://www.kaspersky.com/enterprise-security/security-awareness .

[18] CyberBit: Cyber Security Training Platform. https://www.cyberbit.com/blog/security-training/cyber-security-training-platform/ .

[19] Puhakainen, P., Siponen, M.: Improving employees' compliance through information systems security training: an action research study. MIS Quarterly 2010, 34, 757–778.

[20] Abraham, S., Chengalur-Smith, I.: Evaluating the effectiveness of learner controlled information security training. Computers & Security 2019, 87, 1–12.

[21] Baldwin, T.T., Ford, J.K.: Transfer of training: a review and directions for future research. Personnel Psychology 1988, 41, 63–105.

[22] Velada, R., et al.: The effects of training design, individual characteristics and work environment on transfer of training. International Journal of Training and Development 2007, 11, 282–294.

[23] Katopodis, S., Spanoudakis, G. and Mahbub, K.: Towards hybrid cloud service certification models. International Conference on Services Computing, June, 2014, pp. 394-399.

[24] Hatzivasilis, G., Papaefstathiou, I., Manifavas, C.: Software Security, Privacy and Dependability: Metrics and Measurement. IEEE Software, vol. 33, issue 4, 2016, pp. 46-54.

[25] Cichonski, P., et al.: Computer security incident handling guide. NIST, Special Publication 800-61 v2, 2012, pp. 1-79.

[26] Goeke, L., et al.: PROTECT – An Easy Configurable Serious Game to Train Employees Against Social Engineering Attacks. 1st Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Luxembourg, September 2019, Springer, LNCS, vol. 11981, pp 156-171.

[27] Pape, S., et al.: Conceptualization of a CyberSecurity Awareness Quiz. 2nd Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), ESORICS, Guildford, UK, September 2020, Springer, LNCS, vol. 12512, pp. 61-76,.

[28] IBM, "Create high-quality test data while minimizing the risks of using sensitive production data." *IBM InfoSphere Optim Test Data Fabrication*, IBM, 2017, https://www.ibm.com/il-en/marketplace/infosphere-optim-test-data-fabrication

APPENDIX: SCENARIO INITIALISATION, TRAINING AND DISPOSAL

To better illustrate the operational aspects of the THREAT-ARREST platform we will briefly overview the interactions among the main tools for the three life cycle phases of scenario initialization, training and disposal. Fig. 2 shows the sequence of steps for the three phases.

Once the trainee selects a training scenario, the Training Tool (TT) is responsible for the initialisation of all relevant components for each training session and, consequently, responsible for the aggregation of all information regarding the profiles, the performed trainee's actions and the assessment of the trainees. The first step in the initialisation process is related to the acquisition of the necessary information from the CTTP model of a given training program. This includes fetching the CTTP model and program from the Assurance Tool (AT).

Following that, the TT first initializes any data fabrication at the Data Fabrication Platform (DFP), if defined by the model. Based on notification of successful data fabrication process completion, the TT then initialises the Virtual Lab (VL) infrastructure environment through the Emulation Tool (ET) initialisation functionality using the specific emulation sub model of the given scenario. This is to ensure the fabricated data (i.e., security event logs) are already available when the VMs of the emulated cyber system (the green VMs in the figure) are initialised so they can fetch the data and deploy it inside the VMs through configurable scripts.

Once the VL is initialised, and based on the results of VL initialisation as returned by the ET (Emulation Controller), the TT initialises the monitoring of the VL environment for a set of VM identifiers, using a dedicated REST API at the Emulation Monitor (EMon) component. When the VL monitoring is successfully initialised, the TT initialises the simulation environment, if needed, using the specific simulation sub model of the given training scenario. Lastly, TT's Trainee Assessment module is initialized to provide real-time assessment to trainees.

With respect to the above sequence of communications, the initialization of each tool is performed either through a message broker communication or by a dedicated API as indicated in the figure. To carry out the initialisation, a CTTP model (relevant sub-model) is used as an input along with information about a training session such as the session ID, user ID, and role ID.

The Gamification Tool's PROTECT, and AWARENESS QUIZ games are accessed through the TT front-end (dashboard) by JWT-enabled interface access where the JWT indicates among other information, the scenario ID, session ID, and the gamification sub model. Similarly, the Visualisation Tool front-end is accessed by the trainees through a JWT-based URL.

Once a training scenario is successfully initialised, the TT shows the trainee the main screen of scenario-specific training activities including the different modalities of training and expected steps to follow for each modality. It is the point when the training activities start, as shown in Fig. 2.

There is no predefined sequence of training modality executions a trainee should follow as these are dictated by the CTTP model and specific training needs.

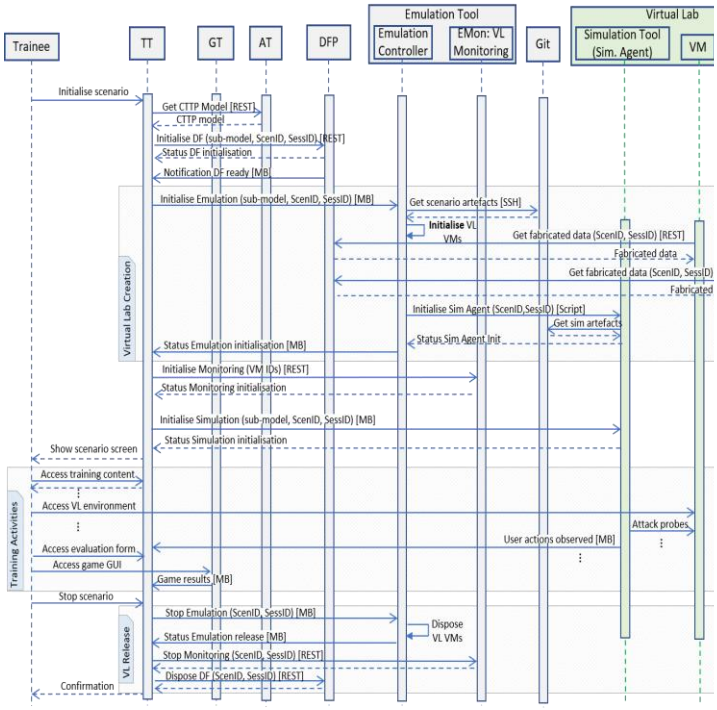


Fig. 2. THREAT-ARREST Tools Interactions for Scenario Initialisation, Training and Disposal

The figure however shows main sequences of activities which are respected in a common case: i) Access to training content; ii) Access to VL environment for hands on training, this also includes access to interactive simulation if that is involved in the scenario; iii) Attack probes simulated against the VL environment, for instance to determine if user actions are properly taking place and informing the Training Tool on such observed actions; iv) Access to evaluation form on Training Tool's main screen asking questions specific to the performed hands-on training to assess user performance and results of this activity; and finally, v) Access to serious games for knowledge, awareness assessment on concepts learned.

Once training is completed, the trainee is informed (through the main screen) on the steps completed, the score achieved and if any steps failed or still missing on any of the modalities. The trainee shall press the option (button) to finalise the scenario once he or she is ready. It will release the environment and inform the trainer (if any) on the results of a given scenario.

We note that if a session exceeds the maximum allowed time (T_{max}), the default platform behaviour is to allow the trainee to play with the VL environment using platform capability to track expected traces and show results out of these steps in the current session screen but no scoring is taken into account after T_{max}.

VL environment release includes: i) Disposal of the VMs including the Simulation Tool's VM by the Emulation Controller; ii) Stop monitoring of the VL environment on the EMon module; and finally iii) Dispose the data fabrication session deleting the fabricated data and all session-related resources. It's important to properly dispose a training session at the end of the training program to ensure resources are timely available in the platform for other training activities.