applied sciences

MDPI

Article

CYRA: A Model-Driven CYber Range Assurance Platform

Michail Smyrlis [1,2,*], Iason Somarakis [1,2], George Spanoudakis [2], George Hatzivasilis [3] and Sotiris Ioannidis [3]

[1] Sphynx Technology Solutions AG, 6300 Zug, Switzerland; somarakis@sphynx.ch
[2] Department of Computer Science, City University of London, London EC1V 0HB, UK; g.e.spanoudakis@city.ac.uk
[3] Institute of Computer Science, Foundation for Research and Technology, 700 13 Heraklion, Greece; hatzivas@ics.forth.gr (G.H.); sotiris@ics.forth.gr (S.I.)
* Correspondence: smyrlis@sphynx.ch or Michail.Smyrlis.2@city.ac.uk

Featured Application: Internet of Things, Industrial Internet of Things and 5G Cyber Range.

Abstract: Digital technologies are facilitating our daily activities, and thus leading to the social transformation with the upcoming 5G communications and the Internet of Things. However, mainstream and sophisticated attacks are remaining a threat, both for individuals and organisations. Cyber Range emerges as a promising solution to effectively train people in cybersecurity aspects. A Training Programme is considered adequate only if it can adapt to the scope of the attacks they cover and if the trainees apply the learning material to the operational system. Therefore, this study introduces the model-driven CYber Range Assurance platform (CYRA). The solution allows a trainee to be trained for known and new cyber-attacks by adapting to the continuously evolving threat landscape and examines if the trainees transfer the acquired knowledge to the working environment. Furthermore, this paper presents a use case on an operational backend ICT system, showing how the CYRA platform was utilised to increase the security posture of the organisation.

Keywords: cyber-ranges; cybersecurity; security assurance; training programmes; CTTP models; CTTP programmes; adaptation; training; education; security awareness

check for updates

Citation: Smyrlis, M.; Somarakis, I.; Spanoudakis, G.; Hatzivasilis, G.; Ioannidis I. CYRA: A Model-Driven CYber Range Assurance Platform. *Appl. Sci.* **2021**, *11*, 5165. https://doi.org/10.3390/app11115165

Academic Editor: José Machado

Received: 30 April 2021
Accepted: 29 May 2021
Published: 2 June 2021

1. Introduction

Cyber Ranges aims to provide advanced cybersecurity training exercises for both cybersecurity professionals and individuals regardless of their security expertise. Unfortunately, cybercriminals constantly improve their techniques and launch impactful attacks that affect both organisations and individuals, leading to an ever-changing threat landscape [1,2]. This is exacerbated nowadays by the complexity of the modern 5G, Internet of Things (IoT), and Industrial IoT (IIoT) systems and the lack of security awareness, as users are not able to promptly identify and minimise the impact of a cyberattack and instead act as enablers for the various threat actors to successfully deploy attacks [1,3,4]. According to the UK's 2021's Cyber Security Breaches Survey [5], four in ten businesses (39%) and a quarter of charities (26%) report having cybersecurity breaches or attacks in the last 12 months. Even though fewer businesses are identifying breaches or attacks than in 2020 (46%), the risk level is potentially higher than ever under COVID-19, making it harder for businesses to administer cybersecurity measures during the pandemic. One of the survey's key findings was unprepared staff risk being caught unaware. More specifically, only a total of 14% of organisations train their staff on cybersecurity, and 20% have tested their staff response through Cyber Range exercises. Further to this, Cybint [6] states that 95% of cybersecurity breaches are due to human error.

That being said, cyber-criminals and hackers will try to infiltrate an organisation through its weakest link. The need for not only more skilled cybersecurity professionals but also well-trained individuals regardless of their security expertise is ever-increasing.

Organisations devote significant efforts concerning money and time for training to enhance the personnel's job-related competencies [7–9]. Relevant investments all over the world are continuously increasing, as well as the demand for advanced and effective Training Programmes. Therefore, it is now becoming mandatory for the training provider, to provide evidence that training activities are being fully realised and ensure the training leads to to designated work competencies, such as increases in the security level or the operational performance of the organisation [8,10,11].

Information security training can raise the organisation's awareness among employees concerning the best practices for cybersecurity and privacy [11–13]. Although training and awareness are still critical for all organisations, they also constitute two of the most neglected areas of cybersecurity. Based on relevant researches, only 50% of companies perform some security training programme periodically [14]. Moreover, such programmes are usually encountered by the personnel and the high-level management just as another element on the checklist that has to be fulfilled [15]. Thus, there is no sufficient effort to assess whether employees benefited from a programme or not or if they are applying the learned practices and the acquired skills in their day-to-day activities.

The SANS Institute is highlighting in several of its reports the challenges that must be tackled by businesses providing security training, including programmes of support, time, and resources by people and departments in their customers' organisations [16]. Academic researchers have also proven that the training efforts can benefit individuals and organisations only when the newly acquired competencies and skills are transferred to the working environment [7,10]. Henceforth, the necessity to analyse and understand the consequences and antecedents of this training process transfer is emerging.

Regarding cyber-security training, although there is an increasing demand for modern Cyber-Range platforms with advance technical features (e.g., emulation, simulation, serious gaming), the transfer of the learned skills and the adjustment of the organisation's operation has been completely overlooked in almost all cases [17–19].

This study presents CYRA, a model-driven CYber Range Assurance Platform that allows (i) the continuous security assurance of the actual operating system, and (ii) the dynamic adaptation of the training procedures in the virtual cyber ranges environment. Initially, the organisation's technical assets and operational aspects are evaluated via automated and semi-automated mechanisms. Then, the actual security posture is disclosed and security Key Performance Indicators (KPIs) are defined, representing the desired level of protection that we want to accomplish through training. A relevant Cyber Threat and Training Preparation (CTTP) Programme is developed and the main training is begun. Throughout this process, the installed analysis mechanisms, from the initial phase, are continuously assessing wherever the trainees are applying the learned concepts in the actual system. If not, indications are provided to the trainer and the training procedures are adapted based on fully- or semi-automated techniques. Meanwhile, the deployed mechanisms may discover new threats that were not recognised before and drive the creation of additional training content.

The proposed solution has been successfully deployed in three Information and Communications Technology (ICT) domains of smart transportation, smart energy, and healthcare. For each of these pilots, three complete Training Programmes have been created, namely: "security awareness" for staff with no or low-security knowledge, "edge system security administrator" for personnel that require main security knowledge concerning the setting and usage of edge systems, and "backend security manager" for security and privacy experts. The platform has been evaluated under real operational conditions where cyber-range training was provided to actual employees. The security KPIs were set in advance, and the trainers guided the trainees to accomplish them and adapt this knowledge back in their workplace. The main training life-cycle has been presented in our previous works [20], while this paper concentrates on the aforementioned modules for CTTP Models and Training Programmes adaptation and continuous security assurance in the operational system.

The rest of the paper is organised as follows. Section 2 overviews the related studies in this field. Section 3 describes the Cyber-Range Assurance Platform. Section 4 details the creation of training programmes and their underlying elements. Section 5 presents the proposed adaptation tool of the platform and Section 6 a demonstration example. Section 7 outlines an evaluation analysis, where external trainers utilise the CTTP models and programmes editor and assess its usability and user-friendliness. Finally, Section 8 provides the concluding remarks and pointers to future work.

2. Related Works

2.1. Adopting Training in the Workplace

One of the main concerns of noncompliance of the personnel with the defined security policies for an organisation constitutes the main concern [12,18,21]. If employees do not fully comply with these policies, the efficacy of the relevant protection mechanisms is lost. From the various compliance approaches, effective training is considered the most commonly proposed solution. Nevertheless, only a few of the existing studies evaluate the results of professional training in organisations and promote policies for compliance in the working environment [12,18]. The theory is rarely utilised to explain what factors are affecting users' compliance with security policies or even provide empirical evidence from their actual application. In general, it is suggested that training programmes should make use of methods and contents that are actively engaging trainees and motivate them to undergo systematic cognitive processing of the taught information [17,20]. Apart from modern technological tools (e.g., simulation, serious games), the continuous communication of the trainer with the learners is vital to improving users' security compliance [12,17,20].

Researches for security training ordinarily incorporate pedagogical principles as the primary methodology to enhance the user's compliance [18,20,21]. In 1998, Baldwin and Ford [22] defined the transfer of learning to the working environment as "the degree to which trainees effectively apply the knowledge, skills, and attitudes gained in the training context to the job". A simplified illustration of the training transfer model is depicted in Figure 1.

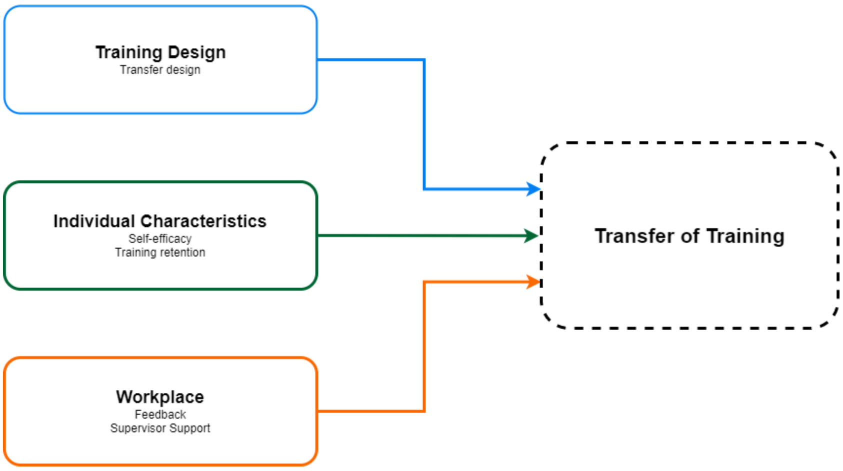


Figure 1. Transfer of training.

However, it is estimated that around 10–40% of all training experiences will be transferred to the workplace [7,17,18]. Moreover, as time passes from the completion of the training programme, employees usually becoming less motivated to retain the new operational behaviours (e.g., after one year). Based on the currently provided methods and training solutions, only a small percent of the desired training outcomes will be permanently transferred to the working environment. Thereupon, enhancing the learning transfer becomes the main concern for modern cybersecurity training platforms, which is also one of the main targets of this study and the proposed continuous assurance and adaptation mechanisms that are detailed in the next sections.

2.2. Cyber Ranges Platforms

Surveys for cybersecurity training in critical infrastructures, such as aviation, transportation, healthcare, energy, and nuclear sectors, are presented in [17–20]. In the last few years, there has been an increasing demand for cybersecurity professionals, which is expected to continue to grow [17]. Cyber Ranges are a promising solution for advanced training that can fill the gap by incorporating educational courses with hands-on experience.

Most of these platforms are implementing automated tools to facilitate the development of virtual labs and scenarios, as well as the adequate means to assess the trainees [19,20]. Karlzen had identified and surveyed the automation trends of 74 cyber ranges platforms [19].

Fourteen of these platforms are deploying such automated modules. The Austrian AIT Cyber Range utilises automation for the instantiation of virtual machines (VMs) during capture-the-flag (CTF) competitions [23]. During such events, it also uses a module called GameMaker, as the scenario engine for the execution of injections [24]. NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) cyber ranges platform utilises the tool suite EVE and ADAM for situational awareness during exercises [25]. The CCDCOE platform can also combine an automated availability scoring module [26]. Cyber Conflict Exercise [27] marshals a series of automated tools that are needed for cyber ranges. These include components for system configuration and deployment, attack execution, updating of flags, visualisation of changes in the emulated setting, and scoring. The CyTRONE platform incorporates a module, called CyRIS (Cyber Range Instantiation System) [28], for the automated configuration and deployment of services and systems in the training environment. Then, additional modules are used for the execution of attacks [29].

The DETERLab platform deploys virtual training environments based on abstract test definitions [30] and develops the Montage AGent Infrastructure (MAGI) for the automatic run of tests [30]. The Emulab platform allocates the hardware resources, sets the networking parameters, and executes other automated events [31], while the Linktest module can validate the generated emulated elements [32]. Similarly, KYPO uses the PM Portal module to set up and control the deployed exercises [33], while additional tools perform automated attacks in the virtual system and evaluation of the trainees. The LARIAT platform includes the Automatic Live Instantiation of a Virtual Environment (ALIVE) module for the configuration and instantiation of VMs for the emulated setting [34]. This includes the emulation of standardised network services, websites, and email services, etc.

The above-mentioned findings show that the existing educational solutions for cybersecurity are mostly concerned with the training environment configuration while the transfer of the learned concepts in the workplace is neglected. In the work presented in [20], the authors introduced a platform, developed under the EU-funded THREAT-ARREST project, where the trainee has the chance to be trained to counter advanced, known, and new cyber-attacks. CYRA acts as a continuation of this work that not only trains a user against several attacks through organisation-specific or generic training programmes but it also (a) investigates if the gained knowledge was applied to increase the security posture of an actual cyber system (if the trainee was part of an organisation) and (b) adopts the existing training programmes or creates new ones by following the adaptation procedures described in Section 5.

3. The CYber Range Assurance Platform (CYRA)

CYRA (see Figure 2) is a combination of three main components namely, Sphynx's Security Assurance Platform, the CTTP models and programmes editor and the CTTP Models and Programmes adaptation tool and was developed by Sphynx Technology Solutions AG (https://www.sphynx.ch/ (accessed on 23 April 2021)).

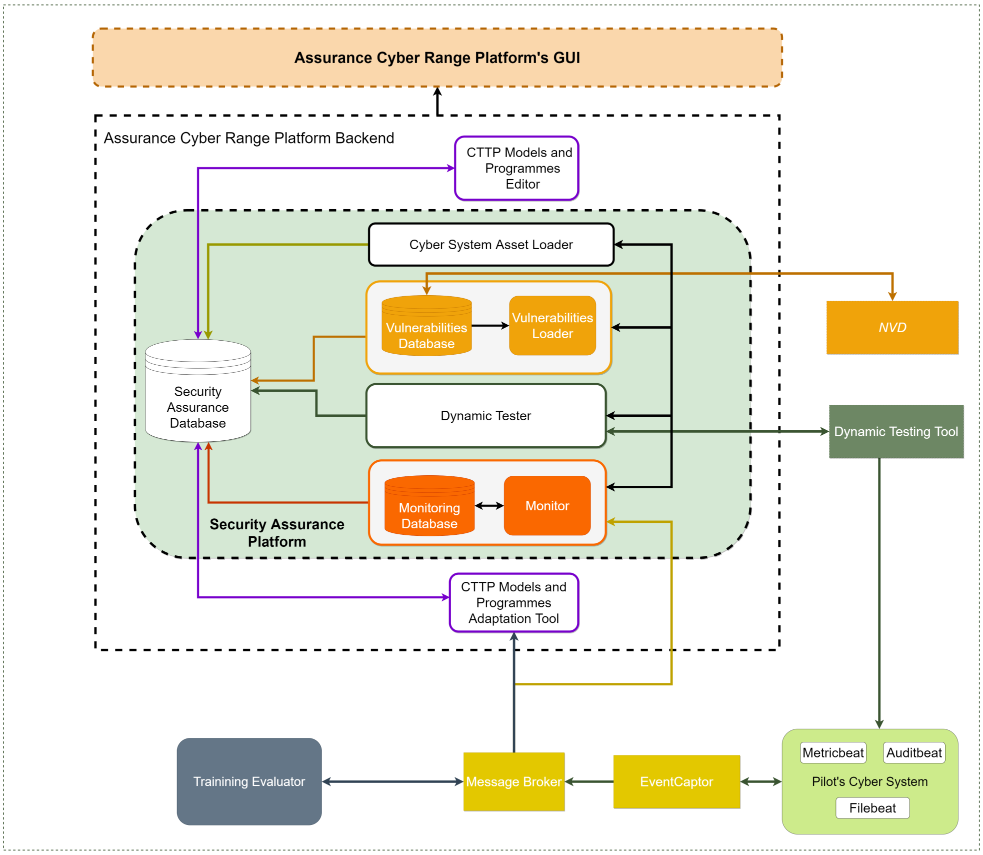

Assurance Cyber Range Platform's GUI
Assurance Cyber Range Platform Backend
CTTP Models and Programmes Editor
Cyber System Asset Loader
Vulnerabilities Database
Vulnerabilities Loader
NVD
Security Assurance Database
Dynamic Tester
Dynamic Testing Tool
Monitoring Database
Monitor
Security Assurance Platform
CTTP Models and Programmes Adaptation Tool
Trainining Evaluator
Message Broker
EventCaptor
Metricbeat
Auditbeat
Pilot's Cyber System
Filebeat

Figure 2. CYRA's architecture.

These components work together to provide Cyber Range training programmes that (a) can train users to understand the ever-increasing threat landscape, (b) are tailored to an organisations needs (based on the use of the Security Assurance Platform) and (c) can be adopted to upcoming cyber threats and/or changes of the assessed cyber systems. More details for the three mentioned components can be found below.

- Sphynx's Security Assurance Platform is a suite of various tools and technologies that enables clients to realise security assessments based on industrial and international standards (e.g., cloud, network, smart metering standards) through continuous monitoring and testing. The platform's main components are:
  - Asset Loader: The component responsible for receiving the cyber system's asset model for the target organisation. This model includes the assets of the organisation, security properties for these assets, threats that may violate these properties and the security controls that protect the assets.
  - Monitoring Module: A runtime monitoring engine built in Java that offers an API for establishing monitoring rules to be checked. This module is made of three sub-modules: a monitor manager, a monitor, and an event collector. The role of the module is to forward the runtime events from the application's monitored properties and finally obtain the monitoring results.
  - Dynamic Testing Module: The Dynamic Testing Module utilises a combination of various open-source penetration testing tools to execute different types of penetration testing assessments. The module actively interacts with a target system to discover vulnerabilities and determine if the vulnerabilities are exploitable. In addition, the module supports the uploading of a report generated from different types of tools and populates the assurance platform based on their results. Finally, as additional functionality, the module can discover and report assets that were not defined in the current asset model of the system.

  - Vulnerability Loader Module: The component responsible for loading the known vulnerabilities (of the identified assets) and updating the assurance platform depending on the organisation's assets included in the assurance model.
  - Event Captor: Event Captor is a tool that, based on collected data and triggering events, formulates a rule or a set of rules and pushes the latter towards monitoring the module for evaluation. Data and events are mostly collected through Elastisearch (https://www.elastic.co/ (accessed on 20 April 2021)) based on lightweight shippers (namely Beats), such as Filebeat, MetricBeat, and PacketBeat, that forwards and centralise log data. Data can also be collected through Logstash, an open server-side data processing pipeline that ingests data from a multitude of sources, transforms it, and then sends it to ElasticSearch. Event captor's are initiated through REST calls from the monitoring module respectively.
- The CTTP Model and Programmes Editor is responsible for creating the CTTP Models and Training Programmes. The editor is offered as a web service through the Cyber Range Platform.
- Lastly, the CTTP Models and Programmes adaptation tool is the tool responsible for adapting the existing training programmes and models or creating new ones in response to upcoming cyber threats and/or changes of the assessed cyber systems.

4. Cyber Threat and Training (CTTP) Models and Programmes

The Cyber Range approach presented herein incorporates emulation, simulation, data fabrication, and serious gaming tools that prepare end-users in defending high-risk cyber systems and organisations to counter advanced, known, and new cyber-attacks. At the core of our model-driven Cyber Range approach (see Figure 3) is the creation of the CTTP Models. A CTTP Model specifies 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. It also drives the training process and aligns it (where possible) with operational cyber system security assurance mechanisms to ensure the relevance of training. The first version of the CTTP models was described in [1]. Subsequently, the authors expanded the CTTP models by adding several attributes that would allow for a better description of the execution tools and the incorporation of security controls and re-structured the CTTP Programmes to better provide its educational scope. Having said that, the CTTP Programme structure is as follows:

```
CTTP Training Programme
  Training Programme Content (1..*)
    Educational Material (1..*)
      Evaluation Report (0..1)
    Training Scenario (0..1)
      Core cyber system asset model (0..1)
      CTTP Model (1..*)
```

To this end, a training programme (course) is made up of one or more training programme contents (thematic lecture and/or virtual lab). The content can include one or more educational materials (e.g., guidelines, handouts), which in turn can contain an evaluation report that the trainee will need to answer to be evaluated on the provided material. The content can also contain a training scenario. The latter includes the organisation's core cyber system asset model (if the scenario was created for an organisation) and one or more CTTP models defining the tools that will be used for the realisation of the scenario. A training scenario has (at a minimum) two compulsory parts namely: (a) the *training delivery parameter model* and (b) the *core cyber system asset model* and the *emulation*, *simulation*, *serious game*, *data fabrication* models or a combination of them. If a training programme is created for an organisation, the organisation's core cyber system asset model is also compulsory. The next subsections contain a brief description of the above-mentioned terms.

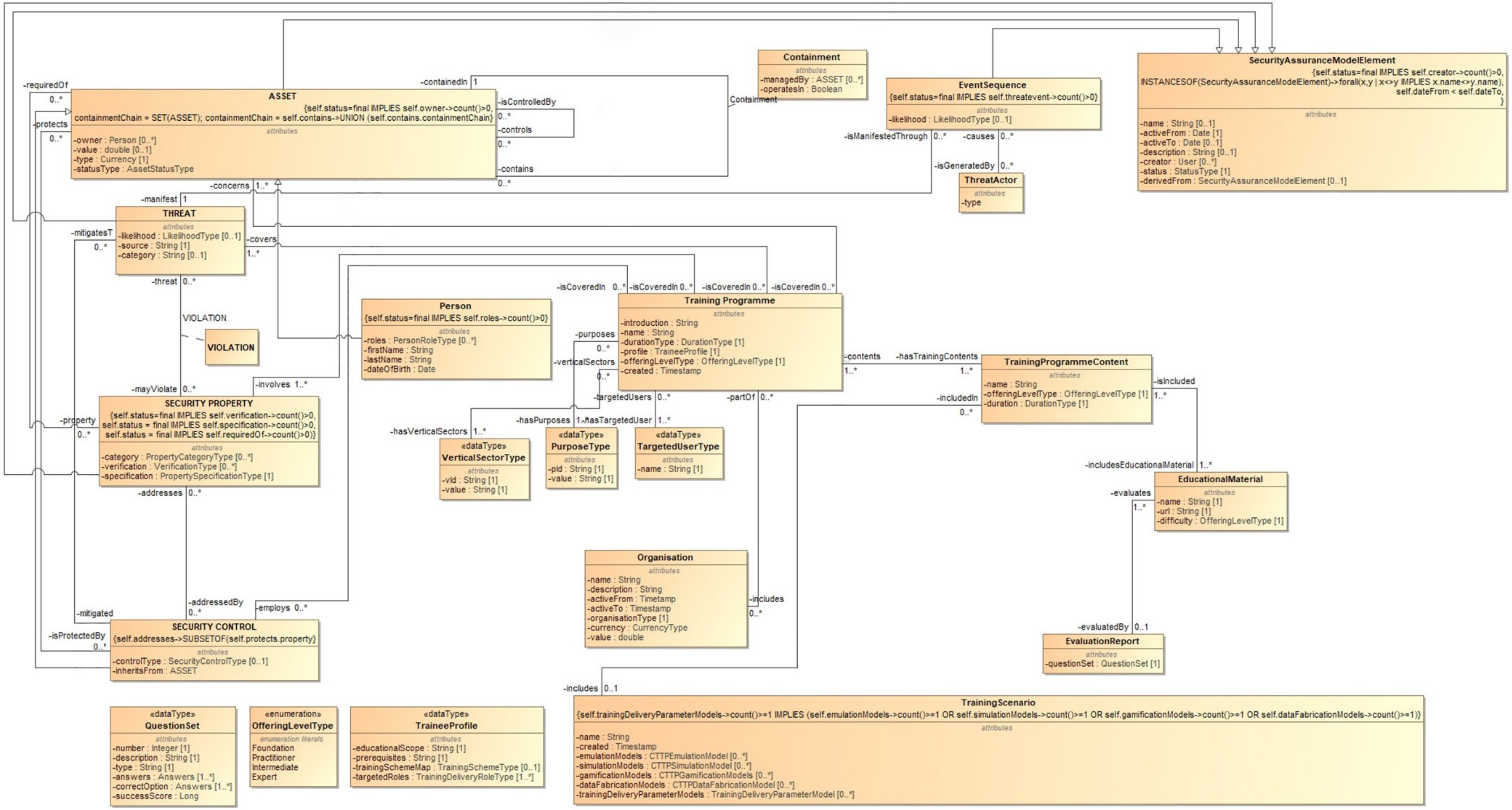

SecurityAssuranceModelElement
{self.status=final IMPLIES self.creator->count()>0,
INSTANCESOF(SecurityAssuranceModelElement)->forall(x,y | x<>y IMPLIES x.name<>y.name),
self.dateFrom < self.dateTo,
}
attributes
-name : String [0..1]
-activeFrom : Date [1]
-activeTo : Date [0..1]
-description : String [0..1]
-creator : User [0..*]
-status : StatusType [1]
-derivedFrom : SecurityAssuranceModelElement [0..1]
Containment
attributes
-managedBy : ASSET [0..*]
-operatesIn : Boolean
EventSequence
{self.status=final IMPLIES self.threatevent->count()>0}
attributes
-likelihood : LikelihoodType [0..1]
-isManifestedThrough 0..*
-causes 0..*
-isGeneratedBy 0..*
ThreatActor
attributes
-type
ASSET
{self.status=final IMPLIES self.owner->count()>0,
containmentChain = SET(ASSET); containmentChain = self.contains->UNION (self.contains.containmentChain)}
attributes
-owner : Person [0..*]
-value : double [0..1]
-type : Currency [1]
-statusType : AssetStatusType
-containedIn 1
Containment
-isControlledBy
0..*
-controls
0..*
-contains
0..*
-requiredOf
0..*
-protects
0..*
-concerns 1..*
-manifest 1
THREAT
attributes
-likelihood : LikelihoodType [0..1]
-source : String [1]
-category : String [0..1]
-mitigatesT
0..*
-covers
1..*
-threat 0..*
VIOLATION
VIOLATION
-mayViolate 0..*
-involves 1..*
SECURITY PROPERTY
{self.status=final IMPLIES self.verification->count()>0,
self.status = final IMPLIES self.specification->count()>0,
self.status = final IMPLIES self.requiredOf->count()>0)}
attributes
-category : PropertyCategoryType [0..*]
-verification : VerificationType [0..*]
-specification : PropertySpecificationType [1]
-property
0..*
-addresses 0..*
-addressedBy
0..*
-employs 0..*
-mitigated
-isProtectedBy
0..*
SECURITY CONTROL
{self.addresses->SUBSETOF(self.protects.property)}
attributes
-controlType : SecurityControlType [0..1]
-inheritsFrom : ASSET
Person
{self.status=final IMPLIES self.roles->count()>0}
attributes
-roles : PersonRoleType [0..*]
-firstName : String
-lastName : String
-dateOfBirth : Date
-isCoveredIn 0..*
-isCoveredIn 0..*
-isCoveredIn 0..*
-isCoveredIn 0..*
Training Programme
attributes
-introduction : String
-name : String
-durationType : DurationType [1]
-profile : TraineeProfile [1]
-offeringLevelType : OfferingLevelType [1]
-created : Timestamp
-purposes
0..*
-verticalSectors
0..*
-targetedUsers 0..*
-partOf 0..*
-hasVerticalSectors 1..*
-hasPurposes 1..*
-hasTargetedUser 1..*
«dataType»
VerticalSectorType
attributes
-vId : String [1]
-value : String [1]
«dataType»
PurposeType
attributes
-pId : String [1]
-value : String [1]
«dataType»
TargetedUserType
attributes
-name : String [1]
-contents
1..*
-hasTrainingContents
1..*
TrainingProgrammeContent
attributes
-name : String
-offeringLevelType : OfferingLevelType [1]
-duration : DurationType [1]
-includedIn
0..*
-isIncluded
1..*
-includesEducationalMaterial 1..*
EducationalMaterial
attributes
-name : String [1]
-url : String [1]
-difficulty : OfferingLevelType [1]
-evaluates
1..*
-evaluatedBy 0..1
EvaluationReport
attributes
-questionSet : QuestionSet [1]
Organisation
attributes
-name : String
-description : String
-activeFrom : Timetamp
-activeTo : Timestamp
-organisationType [1]
-currency : CurrencyType
-value : double
-includes
0..*
-includes 0..1
TrainingScenario
{self.trainingDeliveryParameterModels->count()>=1 IMPLIES (self.emulationModels->count()>=1 OR self.simulationModels->count()>=1 OR self.gamificationModels->count()>=1 OR self.dataFabricationModels->count()>=1)}
attributes
-name : String
-created : Timestamp
-emulationModels : CTTPEmulationModel [0..*]
-simulationModels : CTTPSimulationModel [0..*]
-gamificationModels : CTTPGamificationModels [0..*]
-dataFabricationModels : CTTPDataFabricationModel [0..*]
-trainingDeliveryParameterModels : TrainingDeliveryParameterModel [0..*]
«dataType»
QuestionSet
attributes
-number : Integer [1]
-description : String [1]
-type : String [1]
-answers : Answers [1..*]
-correctOption : Answers [1..*]
-successScore : Long
«enumeration»
OfferingLevelType
enumeration literals
Foundation
Practitioner
Intermediate
Expert
«dataType»
TraineeProfile
attributes
-educationalScope : String [1]
-prerequisites : String [1]
-trainingSchemeMap : TrainingSchemeType [0..1]
-targetedRoles : TrainingDeliveryRoleType [1..*]

Figure 3. CYRA's UML representation.

4.1. Training Programme

A training programme provides a structured learning path for a trainee, as it includes training programme content focusing on particular threats, cyber system components, and assessment tools of a CTTP model and is being used to drive (along with the CTTP Models) the execution of the simulation, emulation, and serious gaming processes.

A training programme includes a number of parameters (required or optional) used to serve different purposes. The basic information of a Programme is: (a) its name, (b) an introduction that allows the trainee to understand the scope of the programme, (c) its purposes (based on ECSO's taxonomy [35], (d) its vertical sectors (based on ECSO's Domains), (e) its targeted users (based on NIST NICE Work Roles (https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center (accessed on 20 April 2021))), (f) its offering level (based on Bloom's Taxonomy [36], and (g) its duration. Then, each training programme includes a trainee profile and learning pathway section where the: (a) roles per targeted users, (b) prerequisites, (c) education scope, and (d) mapping against training schemes (such as ISACA (https://www.isaca.org/ (accessed on 20 April 2021)), SANS (https://www.sans.org/ (accessed on 20 April 2021)), CompTIA (https://www.comptia.org/home (accessed on 20 April 2021)), (ISC)^2 (https://www.isc2.org/ (accessed on 20 April 2021))) are identified. Lastly, a training programme can be assigned to one or more organisations.

4.2. Training Programme Content

Training programme content is part of one training programme and includes one or more types of educational material and zero or one training scenario. The basic information of a piece of content allows the user to understand its scope such as, the content's (a) name, (b) offering level (based on CISCO's certification schemes), ranging from easy to hard difficulty levels, also known as foundation, practitioner, intermediate, and expert), and (c) duration. Both (b) and (c) are subsets of the corresponding training programme's fields. For instance, a training programme of the "intermediate" offering level cannot include contents of the "expert" offering level.

4.3. Educational Material

Educational material is a subset of guidelines and brochures, etc., which allows the trainee to better understand the substance of the training programme content. It has the following attributes: (a) a name, (b) a difficulty level (also based on CISCO certification schemes), and (c) a URL that points to the online reference of the educational material. Lastly, educational material can have an online evaluation report (i.e., questionnaire with closed-ended questions) that will be used to automatically evaluate the trainee.

4.4. Training Scenario

A training scenario is made up of zero or one core cyber system asset model (i.e., the model that contains the different assets of an organisation as well as their relations) and one or more CTTP models, and it is used to set up the virtual environment that will be used for a specific training programme.

4.5. CTTP Models

CTTP models will determine: (a) the cyber system components and cyber threats covered by a CTTP programme, (b) the ways of simulating components of a cyber-system and the cyber-attacks against it, (c) the components of the system that may be emulated and the ways of emulating them, and (d) the real system operational events that should be monitored and analysed to assess the operational security status of a cyber-system in real-time. The full specification of the CTTP Models is available in [1]. The next subsections include updates that occurred after writing the above-mentioned paper.

4.5.1. Emulation Model

An emulation model includes information for the automated generation and interconnection of emulated cyber system components and is intended to be dynamically parsed by an emulation tool (e.g., virtual infrastructure management solutions based on OpenStack (https://www.openstack.org/ (accessed on 23 April 2021)) or Kubernetes (https://kubernetes.io/ (accessed on 23 April 2021)). The updates that occurred to the emulation model included the specification of two new attributes, namely (a) actual trace, an attribute that allows an emulation tool to know the structure of an action that the trainee is expected to perform, and (b) a Boolean value called linkAvailable that allows an emulation tool to understand whether a deployed VM should be visible to the trainee or not.

4.5.2. Simulation Model

A simulation model includes information for the simulation of different layers in the cyber systems implementation stack and is intended to be dynamically parsed by simulation components (e.g., NS-3 https://www.nsnam.org/ (accessed on 23 April 2021)). Unlike the emulation sub-model, the simulation one underwent a number of structural updates. More specifically, the updated simulation model structure is as follows:

```
rootComponent
    Name: String
    Type: Enum (String, Integer, Double, Boolean, Instant)
    Attributes
            Name: String
            Value: String
            Type: Enum (String, Integer, Double, Boolean, Instant)
```

That being said, a simulation model has the following attributes: (a) a name, (b) the involved tool's name, (c) a template (optional), (d) the simulation duration (in minutes), (e) the execution speed, (f) a random seed, (g) the initial simulation time, and (h) the deployment mode. Moreover, from a structural perspective, a simulation model consists of a root component (with a unique name and type), which, in turn, consists of some sub-components or attributes.

4.5.3. Serious Game

A serious game model includes information about the following two types of games: PROTECT [37] or Awareness Quiz [38]. Updates occurred only on the creation of the latter. An Awareness Quiz Serious Game model includes the following attributes: (a) the quiz mode, (b) the available lives, (c) the question time, (d) the points added to the score, (e) the points removed from the score, and (f) specific attributes corresponding to the respective quiz mode. If a game shall be played with a predefined quiz (predefined quiz mode), a specific attribute represents the unique identifier of the quiz. If the set of questions for a quiz shall be compiled on the fly for a certain thematic context (context quiz mode), the following specific attributes are included: (a) the number of questions that shall be asked, (b) a minimum difficulty for the considered questions, (c) a maximum difficulty for the considered questions, (d) one or more quiz topics, on the basis of which the thematic selection of relevant questions takes place. A quiz topic is represented by metadata values of a corresponding metadata type.

4.5.4. Data Fabrication

A data fabrication model includes information that will be used for the creation of synthetic events and is intended to be provided to data fabrication tools, e.g., the IBM Data Fabrication Platform developed by IBM Israel [39]. The data fabrication model did not undergo any substantial updates. Its core component is the scenario, which consists of one or more actions/activities, one or more constraints, one or more sub-nets, one or more connections, and one or more applications.

4.5.5. Training Delivery Parameter Model

The training delivery parameter (TDPM) model (previously mentioned as the training programme) is the "orchestrator" of the above-mentioned models.

Content-wise, the updated TDPM consists of the following attributes: (a) a name, (b) a programme type (e.g., single user, red/blue team, etc.), (c) a difficulty (scaling from 1 to 20), (d) a bonus (added to the trainee's final score if he/she successfully finalised the training earlier than expected), (e) a penalty (subtracted from the trainee's final score if he/she failed to finalise the programme within the time), (f) the targeted scenario actor(s), (g) a flag value called "follow sequence" that allows the training tool to identify whether the TDPM's executions need to follow a specific order, (h) the linked vulnerabilities (based on CVE's) and weaknesses (based on CWE's), (i) the prerequisites, (j) the mitigation controls, (k) the background legal context, and (l) the involved assets.

It also contains the scenario's storyline and course of actions as well as the duration. Moreover, it contains the training standards it was based on (e.g., CSA (https://cloudsecurityalliance.org/ (accessed on 20 April 2021)), ISO (https://www.iso.org/home.html (accessed on 20 April 2021)), NIST (https://www.nist.gov/ (accessed on 20 April 2021)), etc.), the action types (based on several frameworks such as MITRE ATT&CK (https://attack.mitre.org/ (accessed on 20 April 2021)), the Cyber Kill Chain (https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (accessed on 20 April 2021)), and NIST's Incident Response [40]), and the targeted roles (based on the NIST NICE (https://www.nist.gov/itl/applied-cybersecurity/nice (accessed on 20 April 2021)) and e-CF Framework (https://www.ecompetences.eu/ (accessed on 20 April 2021))).

Lastly, from a structural point of view, a TDPM includes one or more pieces of execution information. Each piece of execution information can include one or more screens (that will be presented to the trainee). A screen includes the tool that will be presented to the trainee, whether it will be visible (or not), the targeted role (for instance, if a red/blue team TDPM is created, one screen can be presented to the blue team members whereas another to the red/blue team ones), a brief description of a screen, a hint and its impact (if enabled), the max allowed time a trainee could spend on this screen and a flag value that terminates the whole training session, if the trainee fails to successfully finalise the content of the screen within the requested time limit. Lastly, a screen includes one or more expected traces.

An expected trace can be: (a) an evaluation report that the trainee is asked to fill after he/she finalises the tasks presented to the screen, (b) an event captor, which allows the training tool to understand if the expected actions were a result of the trainee, and (c) a serious game report.

5. Cyber Threat and Training Models and Programmes Adaptation Tool

The CTTP models and programmes adaptation tool covers primary forms of analysis of the impact that specific changes in some parts of the programme have on other parts and checks about the completeness (coverage) and consistency of the entire specification of CTTP models and programmes when some parts of the change. CTTP programme adaptation may be along: (a) the scope of the attacks that they cover (e.g., component specific attacks, system-wide attacks); (b) the sophistication of the attacks (e.g., attacks that explicitly or implicitly affect the asset that they compromise); and (c) the type of response expected from the trainee (e.g., preparedness, analysis, immediate incident response, post-incident response). The general principle underpinning the adaptation of CTTP programmes will be to vary the degree of difficulty that the programme presents to the trainee (e.g., going from component specific to system wide attacks, from asset explicit to asset implicit compromising attacks, from preparedness to analysis). Such levels and corresponding adaptations will depend on the type of system, attack, asset, and security property and will be specified explicitly in the CTTP programme. CTTP programme adaptation is being driven by trainee performance (e.g., increasing/maintaining/reducing the difficulty of a programme if trainees meet/fail (marginally)/fail current action expectations). Furthermore, CTTP programmes will be improved based on a continuous process involving including: (a) automatically recorded performance measures regarding the undertaking of the CTTP programme (e.g., programme completion time) and (b) assessing the level of compliance of these actions to expectations set by the cyber system asset model. The CTTP model and programmes adaptation tool is offered as a web application.

In general, the CTTP models and programmes adaptation is separated into three phases. The first phase, namely, pre-evaluation, includes the training programme that was solely based on a cyber system asset model. Thus, they are based on a theoretical background (asset model) where there was no interaction with an actual cyber system. The second phase, namely, pre-adaptation, includes creating new training programmes based on the security assessments conducted in a cyber systems through Sphynx's Security Assurance Platform (SAP) (https://www.sphynx.ch/products/#assurance-platform (accessed on 18 April 2021)) or the updates of existing ones. Lastly, the third and final phase, namely, post adaptation, includes the adaptation of the phase two programmes based on changes in the asset model (e.g., insertion of a new asset or security control), the introduction of new vulnerabilities as well as changes on an existing vulnerability's likelihood (i.e., a likelihood's shift from LOW to HIGH) and finally, the adaptation based on a trainee's performance.

5.1. *Adaptation Based on Sphynx's Security Assurance Platform*

As above-mentioned, a CTTP models and programmes adaptation will be based on the utilisation of Sphynx's Security Assurance Platform. Four prominent cases that are based on the outcomes of the platform and trigger adaptation actions were identified, (a) when a new security control is inserted to the system, i.e., "a safeguard or countermeasure prescribed for an information system or an organisation designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements", (b) when a vulnerability is detected on an asset that was not vulnerable before (based on SAP's Vulnerability Loader Component), (c) when a new vulnerability is detected on an existing asset, and (d) when the likelihood of a vulnerability changes from low to high, making it a higher priority training target.

5.1.1. Adaptation Based on Security Controls

An adaptation is triggered when a new security control asset is detected (see Algorithm 1). The condition for this adaptation is checked every time a new asset is inserted (by using SAP's Asset Loader). If the condition is true, the adaptation tool searches for existing training delivery parameters models that involve the said security control to identify if training programmes that take into consideration if such controls exist. If such models are found, it generates an alert to notify the trainer of their existence. The generated notification also includes information for the training programme content that is assigned (if any), so that it can be assigned to a trainee (via the training tool). Otherwise, the adaptation tool first creates the training delivery parameter model and then creates an alert prompting the trainer to assign to a training programme content. If the condition is false, no adaptation actions are produced.

Algorithm 1: Adaptation based on security controls

```
Input  : asset
Output : Produce an alert notifying the trainer for the adaptation action
begin
    Fetch all from assurance_db based on $tdpm_involved_assets.asset_id, asset.asset_id, security_control_type.id into tdpm;
    if tdpm is True then
        #Alert Trainer;
        Alert("The Training Delivery Parameter Models, [tdpm_list], is/are already linked with $asset.sec_control_name");
    else
        Create a new Training Delivery Parameter Model to include the identified $asset.sec_control_name;
    end
end
```

5.1.2. Adaptation Based on Vulnerable Assets

New Vulnerabilities on Existing Assets

This adaptation action is triggered when a result of the dynamic testing or the vulnerability assessment module detects vulnerabilities on an asset that was not affected before (see Algorithm 2). This adaptation's condition is checked by the adaptation tool every time a new result is generated. If the condition is true, the adaptation tool searches for training delivery parameters models that involve the said asset. If such models are found, it generates an alert to notify the trainer of their existence. The generated notification also includes information for the training programme content that is assigned (if any), so that it can be assigned to a trainee (via the training tool). Otherwise, the adaptation tool first creates the training delivery parameter model and then creates an alert prompting the trainer to assign to a training programme content. If the condition is false, no adaptation actions are produced.

Algorithm 2: Adaptation based on existing asset vulnerabilities

```
Input  : Assessment Result (ar)
Output : Produce an alert notifying the trainer for the adaptation action
begin
    if ar.model is equal to 'Dynamic_Testing_Assessment model OR 'Vulnerability_Assessment then
        fetch all from assurance_db based on ar.id into dtr;
        fetch all from assurance_db based on dtr.cve into r;
        #If the response is true then the assessed asset has vulnerabilities;
        if r is True then
            fetch all from assurance_db based on dtr.cve, tdpm_involved_cves into tdpm;
            if tdpm is True then
                #Alert Trainer;
                Alert("The Training Delivery Parameter Models, [tdpm_list], is/are already linked with $dtr.cve");
            else
                if dtr.cwe is not Empty then
                    Create Training delivery parameter model to train the user on identifying, mitigating and preventing vulnerability with id
                      $dtr.cve and weakness with id $dtr.cwe;
                else
                    Create Training delivery parameter model to train the user on identifying, mitigating and preventing vulnerability with id
                      $dtr.cve;
                end
            end
        else
            #No vulnerabilities were identified;
            exit();
        end
    else
        #Assessment out-of-scope;
        exit();
    end
end
```

New Vulnerable Asset

This adaptation action is triggered when a new asset is inserted (through the cyber system's asset model) in the assurance tool's database and the dynamic testing or vulnerabilities assessment component identifies vulnerabilities on it (see Algorithm 3). If the condition is true, the adaptation tool searches for training delivery parameters models that involve the said asset. If such models are found, an alert is generated to notify the trainer of their existence and includes information for the training programme content that is assigned (if any), so that it can be assigned to a trainee. Otherwise, the adaptation tool first creates the training delivery parameter model and then creates an alert prompting the trainer to assign to a training programme content. If the condition is false, no adaptation actions are produced.

Algorithm 3: Adaptation based on a newly inserted vulnerable asset

```
Input  : Assessment Result (ar)
Output: Produce an alert notifying the trainer for the adaptation action
begin
    if ar.model is equal to 'Dynamic_Testing_Assessment' OR 'Vulnerability_Assessment' model then
        fetch all from assurance_db based on ar.id into dtr;
        fetch all from assurance_db based on dtr.cve into r;
        if r is True then
            #In this case we search if we have any TDPM that involves this asset;
            fetch all from assurance_db based on dtr.cve, tdpm_involved_cves into tdpm;
            if tdpm is True then
                #Alert Trainer;
                Alert("The Training Delivery Parameter Models, [tdpm_list], is/are already linked with $ dtr.cve");
            else
                if dtr.cwe is not Empty then
                    Create Training delivery parameter model to train the user on identifying, mitigating and preventing vulnerability with id $
                      dtr.cve and weakness with id $ dtr.cwe;
                else
                    Create Training delivery parameter model to train the user on identifying, mitigating and preventing vulnerability with id $
                      dtr.cve;
                end
            end
        else
            # No identified vulnerabilities;
            exit();
        end
    else
        # Assessment out-of-scope;
        exit();
    end
end
```

Increased Likelihood of an Existing Vulnerability

This adaptation action is triggered when a result from the dynamic testing or the vulnerability assessment indicates that a previously discovered vulnerability has changed its likelihood level from low to high (see Algorithm 4). If the action is true, the adaptation tool searches for training delivery parameter models that are linked to the said vulnerability. If such models are found, it generates an alert to notify the trainer of their existence. The generated alert also includes information for the training programme content that is assigned (if any), so that it can be assigned to a trainee. Otherwise, the adaptation tool first creates the training delivery parameter model and then creates an alert prompting the trainer to assign to a training programme content. If the condition is false, no adaptation actions are produced.

Algorithm 4: Adaptation based on a likelihood alteration

```
Input  : Assessment Result (ar)
Output: Produce an alert notifying the trainer for the adaptation action
begin
    if ar.model is equal to 'Dynamic_Testing_Assessment model OR 'Vulnerability_Assessment then
        fetch all from assurance_db based on ar.id into dtr;
        fetch all from assurance_db based on dtr.cve into r;
        fetch one ar.likelihoodLevel from assurance_db based on last_dtr.ar_id into oldLikelihoodLevel;
        if $oldLikelihoodLevel is LOW then
            fetch all from assurance_db based on dtr.cve, tdpm_involved_cves into tdpm;
            if tdpm is True then
                #Alert Trainer;
                Alert("The Training Delivery Parameter Models, [tdpm_list], is/are already linked with $dtr.cve");
            else
                if dtr.cwe is not Empty then
                    Create Training delivery parameter model to train the user on identifying, mitigating and preventing vulnerability with id
                      $dtr.cve and weakness with id $dtr.cwe;
                else
                    Create Training delivery parameter model to train the user on identifying, mitigating and preventing vulnerability with id
                      $dtr.cve;
                end
            end
        else
            #Vulnerability's likelihood LEVEL was not LOW;
            exit();
        end
    else
        #Assessment out-of-scope;
        exit();
    end
end
```

5.1.3. Adaptation Based on Trainee's Performance

The adaptation based on the trainee's performance is triggered when a trainee completes an evaluation report or finalises a training programme's content. By doing that, a message is being generated and published to a message broker's predefined channel that the adaptation tool is listening to in order to initiate the adaptation phase. The message includes information for the completed component (evaluation report or content), the trainee's expertise, the completion time, and the final score (normalised in 100).

Completion of an Educational Material's Evaluation Report

Upon the completion of an evaluation report (of an existing educational material), the adaptation tool consumes the correspondent message and initiates the adaptation phase. More specifically, the adaptation tool checks the evaluation report's difficulty (available in the assurance tool's database) and the trainee's expertise (provided in the consumed message) and, based on the algorithm presented in Algorithm 5, it produces an adaptation alert. In general, the adaptation tool can either be used as an alert mechanism where it will notify the trainer of the need to create a new evaluation report or assign an existing evaluation report with different difficulty.

Algorithm 5: Adaptation based on the evaluation report's score

```
Input  : Trainee's performance (m), Evaluation Report Difficulty (e)
Output: Adaptation alert notifying the trainer for the adaptation action
begin
    traineeExpertise = m.getTraineExpertise();
    if traineeExpertise is greater than e then
        if m.score is greater than or equal to 90 then
            if traineeExpertise less than 'Expert' then
                #Generate a random number from 3 to 20;
                int random = generateRandonNumber();
                #Create a set of questions more difficult than the evaluation report's difficulty;
                List<QuestionPool> questions=getQuestionsFromQuestionPool(random,e.difficulty+1);
                #Create new evaluation report;
                createNewEvaluation Report (questions);
                #Alert Trainer for the creation of the report;
                alert();
            else
                #Alert Trainer that the examined evaluation report is already of an 'Expert' level;
                alert();

        else if m.score is greater than or equal to 50 AND m.score less than 90 then
            #Alert Trainer that no further actions are needed. Trainee's score is within the appropriate scoring range [50,80).;
            alert();

        else
            #Alert Trainer that the trainee needs to be evaluated for his/her performance.;
            alert();

    else if traineeExpertise is equal to e then
        if m.score is greater than or equal to 80 then
            if traineeExpertise less than 'Expert' then
                #Generate a random number from 3 to 20;
                int random = generateRandonNumber();
                #Create a set of questions more difficult than the evaluation report's difficulty;
                List<QuestionPool> questions=getQuestionsFromQuestionPool(random,e.difficulty+1);
                #Create new evaluation report;
                createNewEvaluation Report (questions);
                #Alert Trainer for the creation of the report;
                alert();
            else
                #Alert Trainer that the examined evaluation report is already of an 'Expert' level;
                alert();

        else if m.score is greater than or equal to 50 AND m.score less than 80 then
            #Alert Trainer that no further actions are needed. Trainee's score is within the appropriate scoring range [50,80).;
            alert();

        else
            if traineeExpertise not equal to 'Foundation' then
                #Generate a random number from 3 to 20;
                int random = generateRandonNumber();
                #Create a set of questions easier than the trainee's expertise;
                List<QuestionPool> questions = getQuestionsFromQuestionPool(random,e.difficulty-1);
                #Create new evaluation report;
                createNewEvaluationReport (questions);
                #Alert Trainer for the creation of the report;
                alert();
            else
                #Alert Trainer that the examined evaluation report is of an 'Foundation' level;
                alert();

    else
        if m.score is greater than or equal to 80 then
            if traineeExpertise is equal to 'Expert' then
                #Generate a random number from 3 to 20;
                int random = generateRandonNumber();
                #Create a set of questions more difficult than the evaluation report's difficulty;
                List<QuestionPool> questions=getQuestionsFromQuestionPool(random,e.difficulty+1);
                #Create new evaluation report;
                createNewEvaluation Report (questions);
                #Alert Trainer for the creation of the report;
                alert();
            else
                #Alert Trainer that the examined evaluation report is already of an 'Expert' level;
                alert();
        else
            #Alert Trainer that no further actions are needed. Trainee's score is within the appropriate scoring range [50,80).;
            alert();
```

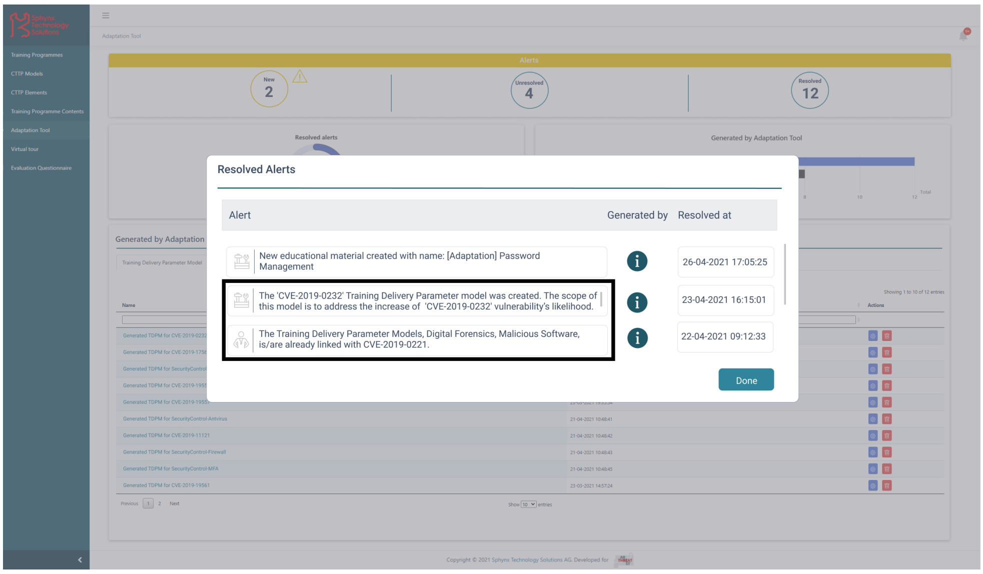
Completion of a Training Programme Content

Upon the completion of a training programme content, the adaptation tool consumes the correspondent message and initiates the adaptation phase. In general, a training programme content's session can last for a predefined amount of time and is of particular difficulty. That being said, the adaptation tool checks the completion time, success score, and trainees' expertise as received from the consumed message and the content's difficulty as stored in the assurance tool's database, and based on the algorithm presented in Algorithm 6 it produces the adaptation results. As before, the adaptation tool can either be used as an alert mechanism where it will notify the trainer of the need to create a new evaluation report or assign an existing evaluation report with different difficulty.

5.2. Demonstrator

5.2.1. Adaptation Based on Security Controls and New Threats

This subsection provides a demonstration of the "existing asset vulnerability" (see Algorithm 5) adaptation procedures. For the former (see Figure 4), the initial step was to execute a dynamic testing assessment based on a cyber system asset model deployed in the cyber range platform. The assessment results (produced by the execution of the dynamic testing assessment), indicated that several new vulnerabilities were identified for the Apache Tomcat. Based on these results, the adaptation tool checked if a training delivery parameter model with the newly identified vulnerabilities exist. As it did not find one, it proceeded with the automatic creation of a new training delivery parameter model adaptation and pre-populated with a number of parameters such as the involved assets, the CVE and CWE (based on the adaptation scenario) and a few additional parameters including the model's storyline, the difficulty, the duration, and the scenario actors.



Resolved Alerts

Alert	Generated by	Resolved at
New educational material created with name: [Adaptation] Password Management	i	26-04-2021 17:05:25
The 'CVE-2019-0232' Training Delivery Parameter model was created. The scope of this model is to address the increase of 'CVE-2019-0232' vulnerability's likelihood.	i	23-04-2021 16:15:01
The Training Delivery Parameter Models, Digital Forensics, Malicious Software, is/are already linked with CVE-2019-0221.	i	22-04-2021 09:12:33

Figure 4. Existing asset vulnerability demonstration.

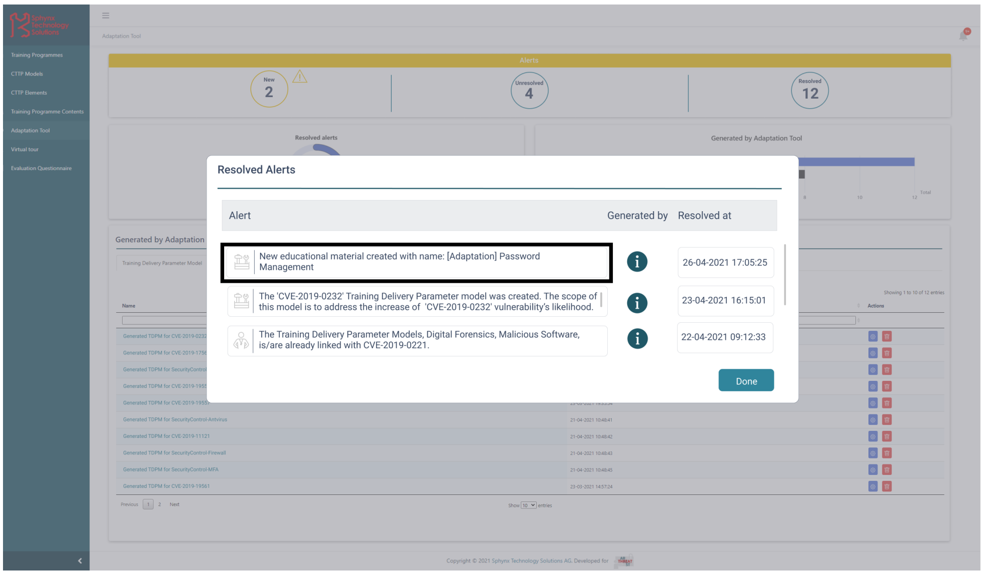
5.2.2. Adaptation Based on Trainee's Performance

Next, the CTTP models and programmes adaptation tool received a notification that a trainee of "practitioner" expertise finalised the existing "password management" educational material's evaluation report (of "practitioner" offering level). The trainee's final score (45) was below the expected score range (greater than or equal to 50). Given that both the trainee and the evaluation report was of "practitioner" level, the CTTP models and programmes adaptation tool automatically created a new evaluation report of "foundation" level, assigned to a new educational material and notified the trainer of the need to re-assess the trainee based on the newly created educational material (see Figure 5).

Algorithm 6: Adaptation based on the completion time and score of a Training

```
Input   : Trainee's performance (m), Evaluation Report Difficulty (e)
Output: Adaptation alert notifying the trainer for the adaptation action
begin
    trainingProgrammeContent = findTrainingProgrammeContentById(m.getId());
    contentName = trainingProgrammeContent.getName();
    adaptationTotalTime = m.getTotalTime();
    trainingProgrammeTime = training ProgrammeContent.getTime();
    contentDifficulty = training ProgrammeContent.getDifficulty();
    traineeScore = m.getScore();
    traineeExpertise = m.getTraineeExpertise();
    tpcOfferingLevel = trainingProgrammeContent.getOfferingLevelType().getValue();
    if traineeScore is greater than or equal to 50 then
        if adaptationTotalTime is less than or equal to trainingProgrammeTime OR adaptationTotalTime is less than or equal to (trainingProgrammeTime + 10) then
            #Alert Trainer that the Training Programme Content time is within the requested time range;
            alert();
        end
        else if adaptationTotalTime is less than or equal to (trainingProgrammeTime+10) then
            if traineeExpertise is equal to 'Foundation' then
                if contentDifficulty is equal to 'Foundation' then
                    if traineeScore is less than 60 then
                        #Alert Trainer that the Trainee's score is not within the requested range (less than 60) thus a performance evaluation will be needed;
                        alert();
                    else
                        Create Training Programme Content of 'Foundation' difficulty and assign it to trainee;
                    end
                end
                else
                    #Alert Trainer to assign an existing Training Programme Content of 'Foundation' difficulty to trainee;
                    alert();
                end
            end
            else if traineeExpertise is equal to 'Practitioner' then
                if contentDifficulty is equal to 'Foundation' then
                    if traineeScore is less than 60 then
                        #Alert Trainer that the Trainee's score is not within the requested range (less than 60) thus a performance evaluation will be needed;
                        alert();
                    else
                        Create Training Programme Content of 'Foundation' difficulty and assign it to trainee;
                    end
                end
                else if contentDifficulty is equal to 'Pracititioner' then
                    #Alert Trainer to assign an existing Training Programme Content of 'Foundation' difficulty to trainee and re-evaluate him/her;
                    alert();
                end
                else
                    #Alert Trainer to assign an existing Training Programme Content of 'Practitioner' difficulty to trainee and re-evaluate him/her;
                    alert();
                end
            end
            else if traineeExpertise is equal to 'Intermediate' then
                if contentDifficulty is equal to 'Foundation' then
                    #Alert Trainer that the Trainee's score is not within the requested range (less than 60) thus a performance evaluation will be needed;
                    alert();
                end
                else if contentDifficulty is equal to 'Pracititioner' then
                    if traineeScore is less than 60 then
                        #Alert Trainer that the Trainee's score is not within the requested range (less than 60) thus a performance evaluation will be needed;
                        alert();
                    else
                        #Alert Trainer to assign an existing Training Programme Content of 'Practitioner' difficulty to trainee and re-evaluate him/her;
                        alert();
                    end
                end
                else if contentDifficulty is equal to 'Intermediate' then
                    if traineeScore is less than 60 then
                        Create Training Programme Content of 'Practitioner' difficulty and assign it to trainee;
                    else
                        #Alert Trainer to assign an existing Training Programme Content of 'Practitioner' difficulty to trainee and re-evaluate him/her;
                        alert();
                    end
                end
            end
            else
                if contentDifficulty is equal to 'Foundation' OR 'Practitioner' then
                    #Alert Trainer that the trainee is of 'Expert' level. He/she should've finalise the Training Programme Content within the requested time range, thus he/she will need to be evaluated in
                      terms of performance.;
                    alert();
                end
                else if contentDifficulty is equal to 'Intermediate' then
                    if traineeScore is less than 60 then
                        #Alert Trainer that the Trainee's score is not within the requested range (less than 60) thus a performance evaluation will be needed;
                        alert();
                    else
                        #Alert Trainer to assign an existing Training Programme Content of 'Practitioner' difficulty to trainee and re-evaluate him/her;
                        alert();
                    end
                end
                else
                    if traineeScore is less than 60 then
                        Create an easier Training Programme Content of 'Expert' difficulty and assign it to trainee;
                    else
                        Ok();
                    end
                end
            end
        end
        else
            Ok()
        end
    end
    else
        # Alert Trainer that the trainee failed to successfully pass the Training Programme Content. He/she will need to be evaluated in terms of performance;
        alert();
    end
end
```

The above-mentioned procedures were also part of the CTTP models and programmes adaptation tool executed for the smart home use case described in Section 6.



Resolved Alerts

Alert	Generated by	Resolved at
New educational material created with name: [Adaptation] Password Management	i	26-04-2021 17:05:25
The 'CVE-2019-0232' Training Delivery Parameter model was created. The scope of this model is to address the increase of 'CVE-2019-0232' vulnerability's likelihood.	i	23-04-2021 16:15:01
The Training Delivery Parameter Models, Digital Forensics, Malicious Software, is/are already linked with CVE-2019-0221.	i	22-04-2021 09:12:33

Done

Figure 5. Adaptation based on educational material's evaluation report score.

6. The IoT-enabled Smart Home Use Case

6.1. Outline

For the evaluation of CYRA, a complete training programme for an operational backend ICT system was performed. The organisation that took part in the evaluation offers a smart energy solution, where energy is collected in smart homes with solar panels, and the energy distribution is recorded and administrated by the backend system at the company's premises [41]. This backend system (the cyber system that CYRA was evaluated) is composed of a set of working and backup servers that host the main organisation's applications.

At the pre-set phase, the system's architecture was recorded via short interviews with the system's users and operators. Thereupon, the main digital assets were identified and were uploaded to CYRA through the cyber system asset loader (see Figure 6). Next, an initial vulnerability assessment was executed (through the vulnerabilities loader component) to understand the basic vulnerabilities that the assessed cyber system has. In general, the vulnerabilities loader searches for known vulnerabilities of the asset's uploaded through the cyber system asset loader obtained from relevant repositories (i.e., NIST's National Vulnerability Database (NVD) (nvd.nist.gov (accessed on 22 May 2021)). The Common Vulnerability Scoring System (CVSS) (www.first.org/cvss (accessed on 22 May 2021)) of each identified Common Vulnerabilities and Exposures (CVE) record (cve.mitre.org (accessed on 22 May 2021)) was then normalised (in CYRA) in the range of 0–100. Next, three dynamic testings (i.e., through the Dynamic Testing Tool) were performed, disclosing automatically the exact technical details of the running system (e.g., database version) and further discovering services, applications, and configurations of the system that the interviewers were not aware of (i.e., a running instance of telnet on one of the servers). This was the first step of the supported adaptation approaches.

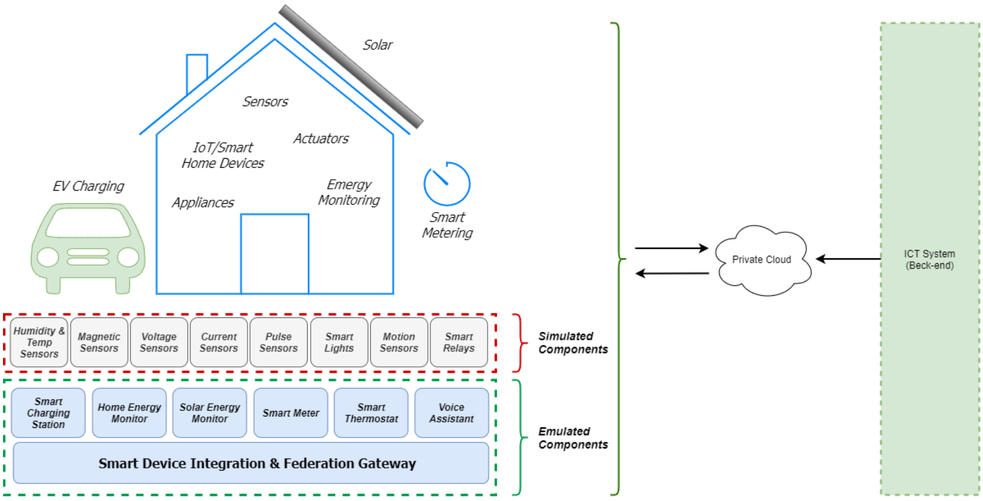
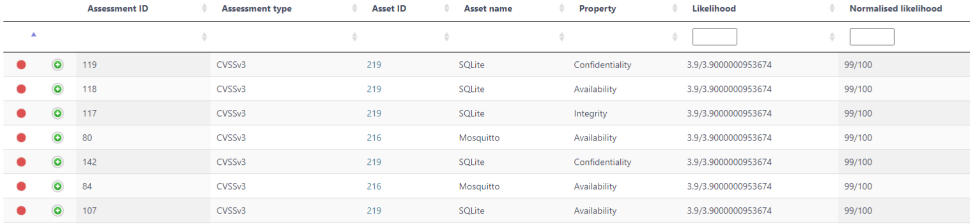


Figure 6. IoT-enabled smart home training scenario.

The results from the above-mentioned sources were then prioritised based on their severity and impact as low, medium, high (as described in the previous section). In total, 40 assets were defined for the smart energy ecosystem and 100 CVEs were identified.

Next, the threat landscape for the specific sector and organisation was revisited and a set of the most severe vulnerabilities was concluded. As 10 of the identified vulnerabilities were of HIGH impact and severity, the training was concentrated on them (see this list in Figure 7).



		Assessment ID	Assessment type	Asset ID	Asset name	Property	Likelihood	Normalised likelihood
●	⊕	119	CVSSv3	219	SQLite	Confidentiality	3.9/3.9000000953674	99/100
●	⊕	118	CVSSv3	219	SQLite	Availability	3.9/3.9000000953674	99/100
●	⊕	117	CVSSv3	219	SQLite	Integrity	3.9/3.9000000953674	99/100
●	⊕	80	CVSSv3	216	Mosquitto	Availability	3.9/3.9000000953674	99/100
●	⊕	142	CVSSv3	219	SQLite	Confidentiality	3.9/3.9000000953674	99/100
●	⊕	84	CVSSv3	216	Mosquitto	Availability	3.9/3.9000000953674	99/100
●	⊕	107	CVSSv3	219	SQLite	Availability	3.9/3.9000000953674	99/100

Figure 7. Security assessments.

To monitor for potential exploitation of these vulnerabilities, event captors were deployed in the system in order to capture events that could lead to a detection of the violation of the security property these 10 vulnerabilities might violate as well as monitor the real-time behaviour of the systems' users, as such elements are not disclosed by the aforementioned automated security analysis tools. Generally, the captors continuously gather events for specific and measurable security aspects, including alerts from the anti-virus/anti-malware software or the warnings from the web browser, as well as occurrence frequency of specific operations in the system's log-files (e.g., how often a user changed its access credentials). Based on these events, the monitoring tool (part of Sphynx's Security Assurance Platform), gathers the information and continuously evaluates individual users and the overall organisation's posture. Specific KPIs are defined for the monitored security properties along with the thresholds that we want to satisfy via training. For example, the organisation has set a security policy, where for organisation of critical services, the employees have to change their password every month. An event captor gathers the events of the relevant application log-files and estimates the password update frequency.

Based on the above-mentioned findings, the learning path of a complete training programme was defined in order to cover all these security-related KPIs. The training programme is called "Backend Security Manager" and consists of seven types of training programme content, as detailed in Table 1.

Following the assignment of the above-mentioned training programme to multiple trainees, their performance was continuously evaluated by the training evaluator module [20], while CYRA's (a) security assurance platform and (b) CTTP models and programmes adaptation tool, continuously evaluated the trainees' compliance on the operational system and the potential effects on the KPIs' status, as well as provided adaptation alerts based on the overall trainee's performance.

Table 1. Backend security manager training programme.

Content	**CTTP Models**	**Covered Threats/Vulnerabilities and Defence Techniques**
Introduction to Cyber Security	Main lecture and educational material	Introductory knowledge of general security-related issues and the aspects of confidentiality, integrity, availability, authentication, authorisation, non-repudiation, and privacy.
Password management	-Main lecture and educational material -Emulation of a virtual lab for the installation and utilisation of a password manager (i.e., KeePass)	Password management issues, including the problems from weak or easily guessed ones and password cracking, as well as aspects of creating strong passwords, password ageing and update policies, and practical and user-convenient practices for password maintenance.
Phishing and social engineering	-Main lecture and educational material -Emulation of a virtual lab with an email phishing scenario and the use of OpenPGP software (Kleopatra) -Serious game for targeted social engineering on system administrators with the PROTECT game [37]	The everlasting effects of social-engineering with a focus on phishing attacks, as well as email security authentication, integrity, and confidentiality.
Malicious software and patching	-Main lecture and educational material -Emulation of a virtual lab for malicious software analysis and the examination of malware samples with relevant static binary analysis tools (e.g., PEView, EDx, TUBS library analysis [42], etc.)	Software flaws, vulnerabilities, and attacks, as well as relevant protection mechanisms, the need for regular patching, and analysis tools of malicious software and attacker's tactics.
Network monitoring and security	-Main lecture and educational material -Emulation of a virtual lab for secure network configuration and monitoring of networking traffic with the tool Head(er) Hunter [43]	Networking manipulation and attacks, as well as secure configuration, administration, and operation, with a focus on continuous traffic monitoring and classification.
Digital Forensics (CTF)	-Main lecture and educational material -Emulation of a virtual lab for the examination of a performed attack on the server (i.e., data breach, crypto-mining, or ransomware based on the activated CTTP model) and the utilisation of forensics software (e.g., glogg, volatility, Wireshark, Nmap, etc.)	Advance attacker's tactics and familiarisation with actual malware and emulated attacks, including tools and methodologies to conduct a digital forensics analysis as a first-responder to security-related incidents.
Attacks on the backend system (Red/Blue team scenario)	-Main lecture and educational material -Emulation of a virtual lab with a vulnerable server that the blue team has to defend (the populated vulnerabilities are defined in the selected CTTP model and are correlated with the defined KPIs) -The red team can be either performed by the trainees via a similar emulated setting or can be completely simulated and triggered automatically or activated manually by the trainer	Acquire advance skills and hands-on experience as the defender and the attacker of a vulnerable system, including tactics and tools to discover the underlying threats and fix them or exploit them, respectively. The red team training involves ethical hacking perspectives and the main benefit for the trainee is to better understand the impacts of attacks on an insecure or poorly safeguarded system and learn how to block or mitigate them in the real working environment.

6.2. Training and Compliance

Based on our first iterations of the overall security monitoring and adaptation of training for the accomplishment of the designed KPIs, the authors observed similar trainees' behaviours as in the literature (see Section 2.1). For instance, the fact that a trainee completed the ″password management″ content and successfully covered the learnt material, does not mean that he/she is going to adopt the working behaviour and update the password-related habits right away [17,18].

On the other hand, it could take several weeks or even months for the event captors to capture events regarding password updates that should have been performed by the trainees for organisation-critical services (as presented on the learnt password policy). Moreover, some of the trainees never updated their passwords within the monitoring period [12,18].

Therefore, two elements drastically improved the compliance factor, as well as the educational aspects [20]; the CTTP models and programmes adaptation tool and the so-called "discussion sessions". Such a session usually occurs at the beginning and the end of each training programme and the end of each content (lesson). Within the first session, the trainer summarises the baseline security assessment results. There, it is made clear to the trainees that the goal of the programme is not only the training part but the achievement of a specific improvement for each monitored KPI. The trainees are becoming part of the organisation's security culture and are becoming aware that their compliance will be assessed throughout the process. Thereupon, the training starts and everyone is familiar with the long-term view. Training evaluation is not the main factor as in a professional certification exam. Here, the educational and compliance aspects are essential. Thus, after each content, the trainer analyses its main concepts and discusses with trainees how they encountered these issues and what problems they faced. At the end of these sessions, any potential misconceptions and open issues are resolved and everyone is aware of the next steps that must be taken. The final discussions are performed at the end of the training, where the current KPIs' status is assessed and any potential subsequent actions are settled.

As for the CTTP models and programmes adaptation tool, it played an important role in the overall compliance of the learnt materials as, by continuously adapting the educational material's evaluation reports (either by automatically creating new ones or updating the existing ones) based on the trainee's performance, helped the trainee to better understand the content described inside the materials, and then apply what he/she learnt, to the examined ICT system.

Concluding, by examining the above-mentioned steps and procedures, one can understand that CYRA incorporates a series of technical and procedural mechanisms that not only helps to train a user but also examines whether the learnt material was applied to an operational cyber system. As for the presented use case, the authors reached the defined KPIs thresholds and the desired compliance level within the monitoring period. Moreover, all 10 severe CVEs were successfully resolved. This period included two weeks for the baseline analysis, four weeks for training (3 h of training per week for each trainee), and two weeks for post-training evaluation and overall feedback.

7. Evaluation Results

7.1. Platform Statistics

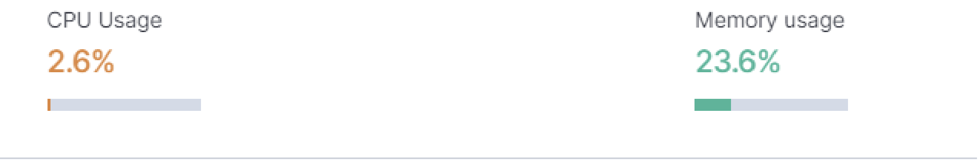
CYRA is currently deployed on a virtual machine with its hardware specifications presented in Table 2. Although not a priority, the authors intend to create a more lightweight and portable version of the platform before its final release.

Table 2. CYRA's hardware requirements.

No of. vCPUs	RAM	Storage (Gb)	Bandwidth (Mbps)
8	32	120	50

To provide meaningful statistics of CYRA's performance, the authors used Kibana (https://www.elastic.co/kibana (accessed on 26 May 2021)) and Apache JMeter (http://jmeter.apache.org/ (accessed on 26 May 2021)). The former was used to continuously monitor the platform's performance in terms of resource usage, while the latter was used to test the performance of the exposed REST APIs.

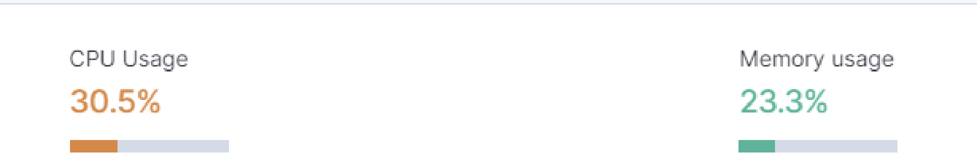
As depicted in Figure 8, CYRA's mean CPU usage while the platform is at a normal use (e.g., creation and retrieval of new CTTP models and training programmes) is only at 3%, whereas its memory usage is equal to 24.9%. When the CTTP Models and Programmes adaptation tool and Sphynx's Security Assurance Platform were utilised, one can observe that the mean CPU usage was increased to 30.5% while the memory usage remained at the same levels (see Figure 9). In general, CYRA's CPU and memory usage was observed to increase to around 70% only when dynamic testing and monitoring assessments were executed simultaneously.



CPU Usage
2.6%

Memory usage
23.6%

Figure 8. Mean CPU and memory usage (normal platform usage).

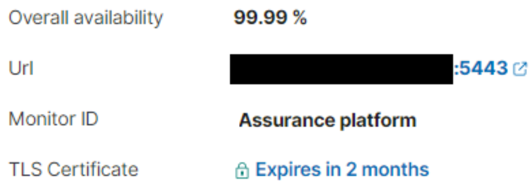


CPU Usage
30.5%

Memory usage
23.3%

Figure 9. Mean CPU and memory usage (heavy platform usage).

CYRA's availability (excluding planned downtime) for the monitored period is at 99.99% (see Figure 10) with around four pings per minute (see Figure 11).



Overall availability	99.99 %
Url	[redacted]:5443
Monitor ID	Assurance platform
TLS Certificate	Expires in 2 months

Figure 10. CYRA's availability.

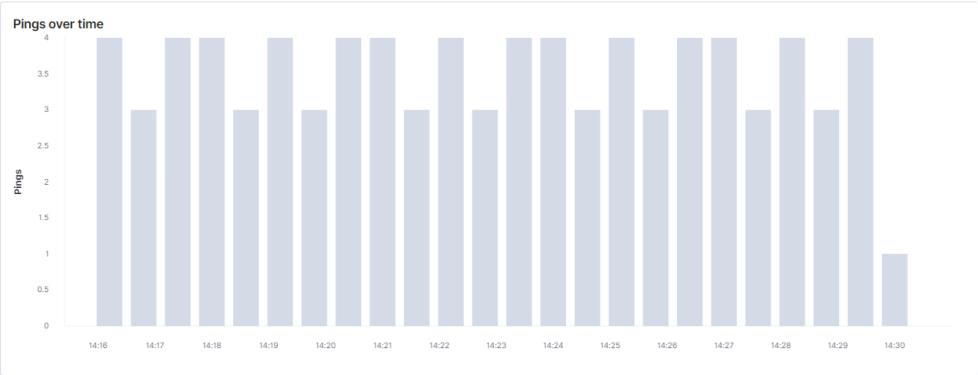


Figure 11. Pings per minute.

As for the user's interaction with the platform, it is observed that CYRA receives around 2000 hits every roughly 15 min (see Figure 12).

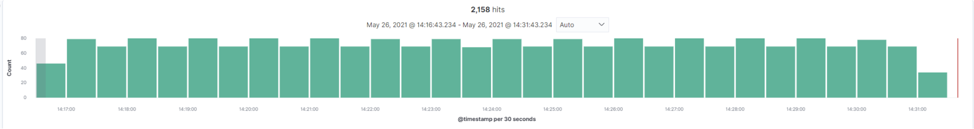
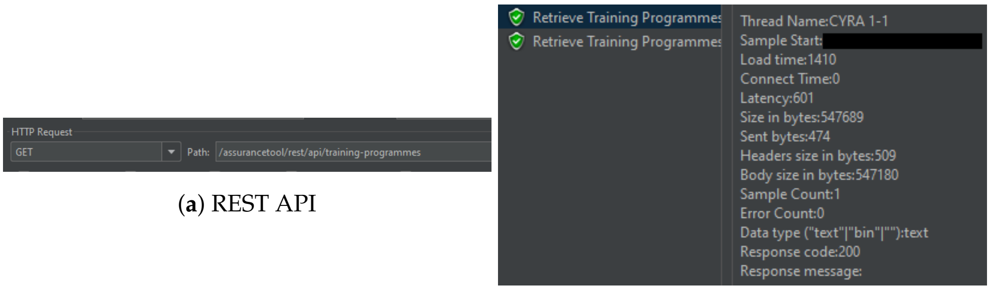


Figure 12. User's interactions with CYRA.

Lastly, JMeter is used to measure the elapsed time per CYRA's API. JMeter's Glossary [44] states that it measures the "load time" as the difference between the time when the request was sent and the time once a response has been completely received and the "latency" as the time from just before sending the request to just after the first response has been received. For the sake of brevity, only two REST API metrics are presented. The first one is responsible for retrieving all the training programmes, while the latter is responsible for retrieving all the training scenarios.

As presented in Figure 13, the load time to fetch 547,689 bytes of data for the training programme's REST API is 1410 ms.



/assurancetool/rest/api/training-programmes

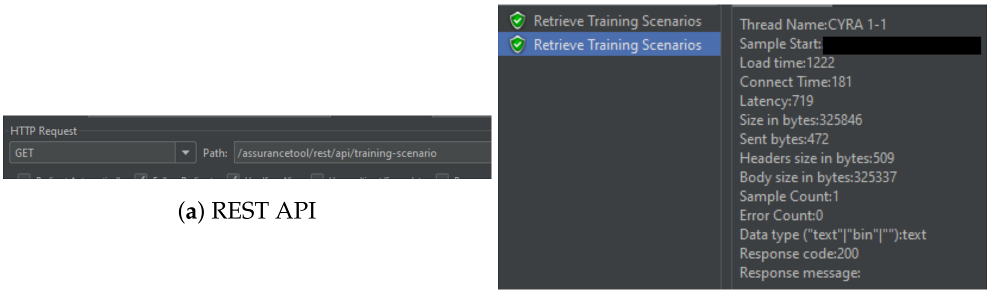
(**a**) REST API

```
Thread Name:CYRA 1-1
Sample Start:[redacted]
Load time:1410
Connect Time:0
Latency:601
Size in bytes:547689
Sent bytes:474
Headers size in bytes:509
Body size in bytes:547180
Sample Count:1
Error Count:0
Data type ("text"|"bin"|""):text
Response code:200
Response message:
```

(**b**) Response Time

Figure 13. Training Programme's REST API (**a**) and its metrics (**b**).

Lastly, as for the training scenarios, the load time to fetch 325,846 bytes of data for the Training Scenario's REST API is 1222 ms (see Figure 14).



/assurancetool/rest/api/training-scenario

(**a**) REST API

```
Thread Name:CYRA 1-1
Sample Start:[redacted]
Load time:1222
Connect Time:181
Latency:719
Size in bytes:325846
Sent bytes:472
Headers size in bytes:509
Body size in bytes:325337
Sample Count:1
Error Count:0
Data type ("text"|"bin"|""):text
Response code:200
Response message:
```

(**b**) Response Time

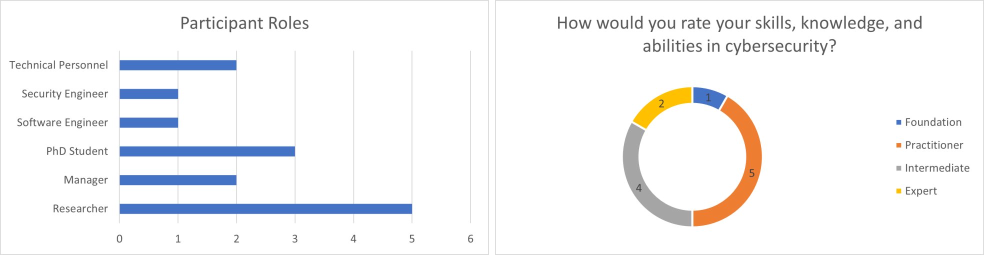
Figure 14. Training Scenarios' REST API (**a**) and its metrics (**b**).

7.2. CTTP Model Editor Evaluation

At the time of writing, 12 external trainers and 20 trainee's of different sectors (e.g., healthcare, maritime, IoT and 5G) and expertise (foundation, practitioner, intermediate, expert) evaluated the CTTP models and programmes editor (part of the cyber range assurance platform). Only the trainers were asked to submit an evaluation report, as they were responsible for presenting the CTTP Models and programmes editor to the trainee's, and incorporate their comments into the final report. Most of the users (10 out of 12) have a technical background, while the rest are general IT personnel (see Figure 15a). Five of the participants considered themselves of "practitioner" level in terms of their cyber-security skills, knowledge and abilities, one as “foundation”, four as “intermediate” and two as “expert” (see Figure 15b).

The four levels of expertise are:

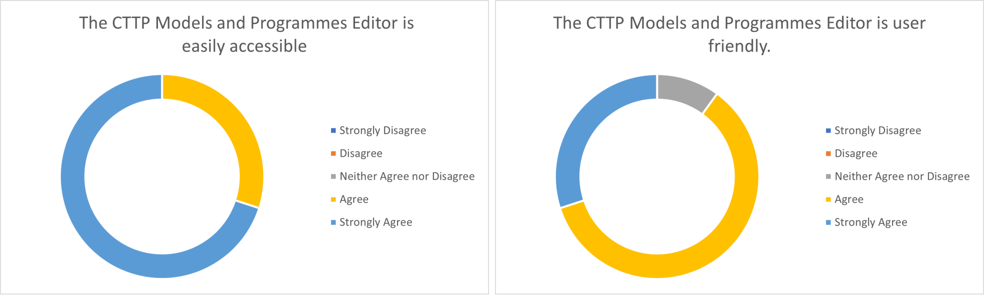
1. Foundation: The trainer has a basic security knowledge and no experience in creating cyber range programmes.
2. Practitioner: The trainer has an advanced security knowledge and limited experience in creating cyber range programmes.
3. Intermediate: The trainer is a security expert with limited expertise in creating cyber range programmes.
4. Expert: The trainer is a security expert with high expertise in creating cyber range programmes.



(**a**) Participant Roles (**b**) Participant expertise

Figure 15. Participant roles (**a**) and cyber-security expertise (**b**).

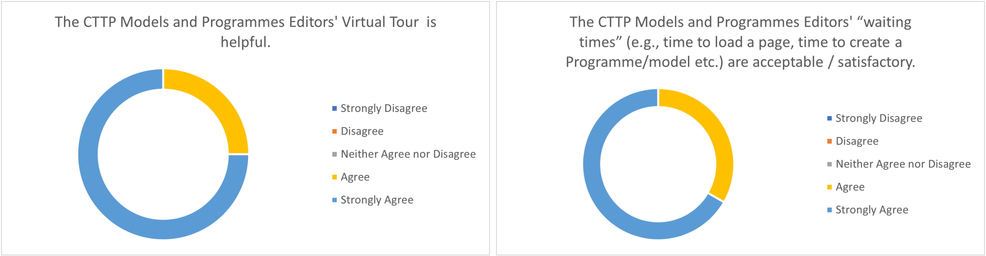
The participants were asked a total of 14 questions in order to evaluate the usefulness of the CTTP models, programmes and the editor. As shown in Figure 16, most of the participants found the CTTP models and programmes editor both easily accessible and user friendly.



(**a**) Ease of access (**b**) User Friendly

Figure 16. CTTP models and programmes editor’s usage. (**a**) and (**b**) presents the participants response regarding the Editors’ Ease of access and user-friendliness respectively.

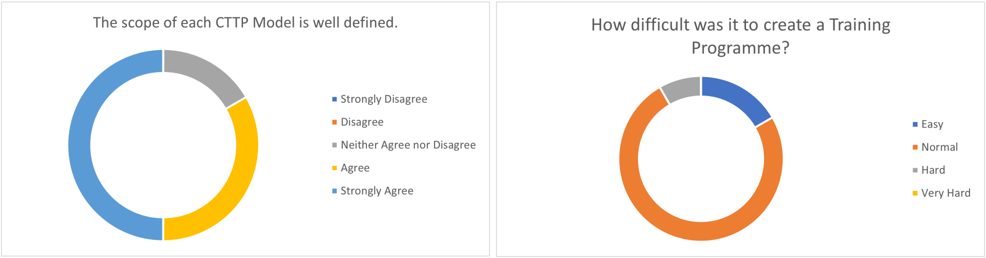
Next, the participants were asked about the virtual tour feature of CTTP models and programmes editor as well as the editor’s waiting times. The former was created to facilitate a user on the creation of the CTTP models and programmes. This was deemed necessary as elsewhere, the user would need to go through several documents to be in a position to create CTTP models and programmes. As shown in Figure 17a, all of the participants either agreed (4 out of 12) or strongly agreed (8 out of 12) that this feature is useful. As for the waiting times, all the participants either agreed or strongly agreed that the waiting times were acceptable (see Figure 17b). In general, it took an experienced participant around 8 min to fully define a training programme.



(**a**) Virtual Tour (**b**) Waiting Times

Figure 17. Participants response to the usefulness of the Virtual Tour feature (**a**) and level of acceptance for the Editor's waiting times (**b**).

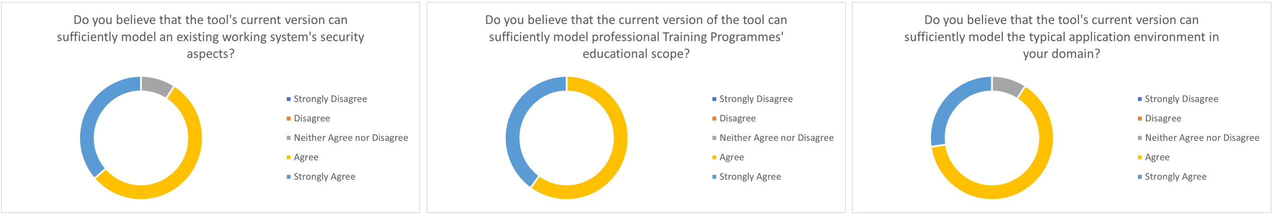
Following, the participants were asked about the scope of each CTTP model and the difficulty of creating a training programme through the CTTP model editor (see Figure 18). For the former, most of the participants (10 out of 12) either agreed or strongly agreed that the scope of CTTP models is well defined, while 2 out of 12 kept a neutral stance (see Figure 18a). As for the latter, 11 out of 12 found it either easy or normal to create a training programme, whereas one participant found it difficult (see Figure 18b).



(**a**) Scope of CTTP Model (**b**) Creation of training programme

Figure 18. Participants response to the CTTP Model's clear Scope (**a**) and the Training Programme's creation difficulty (**b**).

Succeeding, the participants were asked if the CTTP model and programmes editor can sufficiently model (a) existing working system's security aspects (see Figure 19a), (b) professional training programmes' educational scope ((see Figure 19b) and (c) the typical application environment in the participants' domain (see Figure 19c). The participants seemed to form a common view for all three questions as they either agreed or strongly agreed that the CTTP model and programmes editor has sufficient modelling capabilities.



(**a**) Security Aspects (**b**) Education Scope (**c**) Participant's Domain

Figure 19. CTTP Models and programmes editors' modelling capabilities. The subfigures present the responses on whether the CTTP model and programmes editor can sufficiently model (**a**) existing working system's security aspects (**a**), (**b**) professional training programmes' educational scope (**b**) and (**c**) the typical application environment in the participants' domain (**c**).

Lastly, almost all the participants were extremely satisfied with their interaction with the CTTP models and programmes editor (see Figure 20).

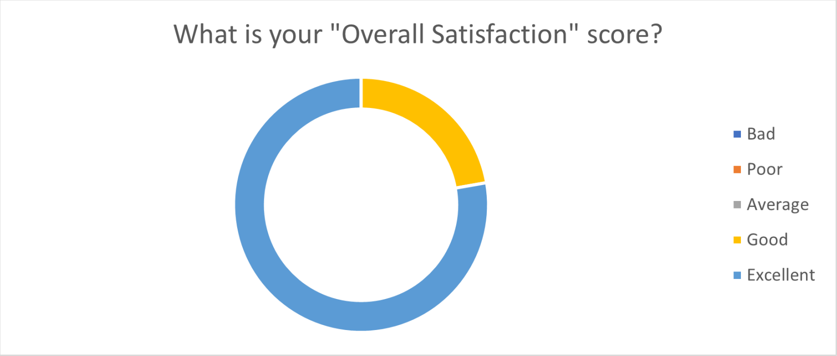


Figure 20. Overall satisfaction score.

8. Conclusions and Future Work

This paper presented our novel model-driven Cyber Range approach by introducing CYRA, a Cyber Range assurance platform that includes: (a) the CTTP models and programmes editor, a tool that supports the specification of CTTP models and programmes that are at the core of the platform's model-driven cyber range training approach, (b) Sphynx's security assurance platform that enables customised and continuous assessment of the security and privacy of a cyber system and comprehensive risk management and (c) the CTTP models and programmes adaptation tool, a tool that covers primary forms of analysis of the impact that specific changes in some parts of the programme have on other parts and checks about the completeness (coverage) and consistency of the entire specification of CTTP models and programmes when some parts of it change.

In addition to the above, the manuscript included a validation of CYRA in an operational backend ICT system of a THREAT-ARREST pilot. The results presented in the use case shows the organisation increased its security posture by utilising (a) the CTTP models and programmes editor to create organisation-specific training programmes, (b) Sphynx's security assurance platform to enable customised and continuous assessment of the organisation's backend ICT system and (c) the CTTP models and programmes adaptation tool to adapt to the newly identified threats.

In general, the overarching objective of these efforts is to create a platform that would allow an organisation to increase its security posture or maintain it at the highest possible level by: (a) creating training programmes that would enable its personnel to understand the continually intensifying threat landscape regardless of the personnel's security background, (b) continually assess the security and privacy of the organisation's cyber systems and (c) adopt to the threat landscape and trainee's skills by creating new training programmes or modifying existing ones.

In terms of the next steps, efforts will focus on (a) extending the CTTP models to support the specification of models for a wider range of emulation and simulation tools, (b) extending the CTTP models and programmes adaptation tool to support multiple forms of adaptation, including the introduction of machine learning algorithms that will allow the tool to proactively adapt to the ever-increasing threat landscape and (c) defining adaptation procedures based on user and entity behavioural analytics (UEBA). The authors plan to provide a number of training programmes in an open repository to which interested parties can refer and retrieve the programmes of interest.

Finally, the authors aim to assess the usability of CYRA by extending the evaluation invitations to the whole THREAT-ARREST consortium and its personnel after the final release of the platform, as well as external parties.

Author Contributions: Conceptualisation, M.S., I.S., G.S., G.H. and S.I.; methodology, G.S. and S.I.; software, M.S.; validation, I.S., G.H.; formal analysis, G.S.; investigation, M.S. and G.H.; data curation, M.S.; writing—original draft preparation, M.S. and G.H.; writing—review and editing, M.S., G.H., G.S. and S.I.; visualisation, M.S. and G.H.; supervision, G.S. and S.I.; funding acquisition, G.S. and S.I. All authors have read and agreed to the published version of the manuscript.

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

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

Abbreviations

The following abbreviations are used in this manuscript:

CCDCOE	Cooperative Cyber Defence Centre of Excellence
CTF	Capture The Flag
CTTP	Cyber Threat and Training Preparation
CVSS	Common Vulnerability Scoring System
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
CYRA	CYber Range Assurance platform
IoT	Internet of Things
KPI	Key Performance Indicator
ICT	Information and Communications Technology
UEBA	User and Entity Behavioural Analytics
VM	Virtual Machine

References

1. Smyrlis, M.; Fysarakis, K.; Spanoudakis, G.; Hatzivasilis, G. Cyber Range Training Programme Specification Through Cyber Threat and Training Preparation Models. In *International Workshop on Model-Driven Simulation and Training Environments for Cybersecurity*; Springer: Guilford, UK, 2020; pp. 22–37.
2. Somarakis, I.; Smyrlis, M.; Fysarakis, K.; Spanoudakis, G. Model-driven cyber range training: A cyber security assurance perspective. In Computer Security; Springer: Cham, Switzerland, 2019; pp. 172–184.
3. Hatzivasilis, G.; Kunc, M. Chasing Botnets: A Real Security Incident Investigation. In *2nd Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), LNCS*; Springer: Guilford, UK; Berlin/Heidelberg, Germany, 2007; Volume 12512, pp. 111–124.
4. Soultatos, O.; Papoutsakis, M.; Fysarakis, K.; Hatzivasilis, G.; Michalodimitrakis, M.; Spanoudakis, G.; Ioannidis, S. Pattern-driven Security, Privacy, Dependability and Interoperability management of IoT environments. In Proceedings of the 24th IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD 2019), Limassol, Cyprus, 11–13 September 2019; pp. 1–6.
5. Department for Digital, Culture, Media & Sport Cyber Security Breaches Survey 2021. Available online: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021 (accessed on 30 April 2021).
6. Milkovich, D. 15 Alarming Cyber Security Facts and Stats. Available online: https://www.cybintsolutions.com/cyber-security-facts-stats/ (accessed on 30 April 2021).
7. Velada, R.; Caetano, A.; Michel, J.W.; Lyons, B.D.; Kavanagh, M.J. The effects of training design, individual characteristics and work environment on transfer of training. *Int. J. Train. Dev.* **2007**, *11*, 282–294. [CrossRef]
8. Cascio, W.F. Costing Human Resources. In *The Financial Impact of Behavior in Organizations*, 4th ed.; South-Western Publishing Co.: Nashville, TN, USA, 2000; pp. 1–322.
9. Mathis, R.L.; Jackson, J.H. Human Resource Management. In *Gaining a Competitive Advantage*, 6th ed.; McGraw-Hill Irwin: Boston, MA, USA, 2006; pp. 1–322.
10. Peretiatko, R. International Human Resource Management: Managing People in a Multinational Context. *Manag. Res. News* **2009**, *32*, 91–92. [CrossRef]
11. Manifavas, C.; Fysarakis, K.; Rantos, K.; Hatzivasilis, G. DSAPE—Dynamic Security Awareness Program Evaluation. In *Human Aspects of Information Security, Privacy and Trust (HCI International 2014), LNCS*; Springer: Heraklion/Crete, Greece, 2014; Volume 8533, pp. 258–269.
12. Abraham, S.; Chengalur-Smith, I. Evaluating the effectiveness of learner controlled information security training. *Comput. Secur.* **2019**, *87*, 1–12. [CrossRef]
13. Spanoudakis, G.; Damiani, M. Maña Certifying services in cloud: The case for a hybrid, incremental and multi-layer approach. In Proceedings of the IEEE 14th International Symposium on High-Assurance Systems Engineering, Omaha, NE, USA, 25–27 October 2012; pp. 17–19.

14. Burg, D.; Compton, M.; Harries, P.; Hunt, J.; Lobel, M.; Loveland, G.; Nocera, J.; Panson, S.; Waterfall, G. US Cybersecurity: Progress Stalled-Key Findings from the 2015 US State of Cybercrime Survey. 2015. Available online: https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf (accessed on 30 April 2021).
15. Robinson, A. Using Influence Strategies to Improve Security Awareness Programs. 2021. Available online: https://www.sans.org/reading-room/whitepapers/awareness/influence-strategies-improve-security-awareness-programs-34385 (accessed on 30 April 2021).
16. Spitzner, L.; de Beaubien. D.; Ideboen, A; Xu, H.; Zhang, N.; Andrews, H.; Sonaike, A. Cyber Security Breaches Survey 2021. 2019. Available online: https://adcg.org/wp-content/uploads/2020/02/SANS-Security-Awareness-Report-2019.pdf (accessed on 30 April 2021).
17. Chouliaras, N.; Kittes, G.; Kantzavelou, I.; Maglaras, L.; Pantziou, G.; Ferrag, M.A. Cyber ranges and testbeds for education, training, and research. *Appl. Sci.* **2021**, *11*, 1809. [CrossRef]
18. Chowdhury, N.; Gkioulos, V. Cyber security training for critical infrastructure protection: A literature review. *Comput. Sci. Rev.* **2021**, *40*, 1–20. [CrossRef]
19. Gustafsson, T.; Almroth, J. Cyber range automation overview with a case study of CRATE. In *25th Nordic Conference on Secure IT Systems (NordSec), LNCS*; Virtual Event; Springer: Guilford, UK, 2021; Volume 12556, pp. 192–209.
20. Hatzivasilis, G.; Ioannidis, S.; Smyrlis, M.; Spanoudakis, G.; Frati, F.; Goeke, L.; Hildebrandt, T.; Tsakirakis, G.; Oikonomou, F.; Leftheriotis, G.; et al. Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. *Appl. Sci.* **2020**, *10*, 5702. [CrossRef]
21. Puhakainen, P.; Siponen, M. Improving employees' compliance through information systems security training: An action research study. *MIS Q.* **2010**, *34*, 757–778. [CrossRef]
22. Baldwin, T.T.; Ford, J.K. Transfer of training: A review and directions for future research. *Pers. Psychol.* **1988**, *41*, 63–105. [CrossRef]
23. Frank, M.; Leitner, M.; Pahi, T. Design considerations for cyber security testbeds: A case study on a cyber security testbed for education. In Proceedings of the 15th Intl Conf on Pervasive Intelligence and Computing, Orlando, FL, USA, 6–10 November 2017; pp. 38–46.
24. Leitner, M.; Frank, M.; Hotwagner, W.; Langner, G.; Maurhart, O.; Pahi, T.; Reuter, L.; Skopik, F.; Smith, P.; Warum, M. AIT Cyber Range: Flexible Cyber Security Environment for Exercises, Training and Research. In Proceedings of the European Interdisciplinary Cybersecurity Conference (EICC 2020) ACM, Rennes, France, 18 November 2020; pp. 1–6.
25. Melon, F.; Vaisanen, T.; Pihelgas, M. EVE and ADAM: Situation Awareness Tools for NATO CCDCOE Cyber Exercises. In *Systems Concepts and Integration (SCI) Panel SCI- 300 Specialists' Meeting on Cyber Physical Security of Defense Systems*; NATO: Shalimar, FL, USA, 2018; pp. 1–15.
26. Pihelgas, M. Design and implementation of an availability scoring system for cyber defence exercises. In Proceedings of the 14th International Conference on Cyber Warfare and Security (ICCWS) ACI, Stellenbosch, South Africa, 28 February–1 March 2019; pp. 329–337.
27. Joonsoo, K.; Youngjae, M.; Moonsu, J. Becoming invisible hands of national live-fire attack-defense cyber exercise. In Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Stockholm, Sweden, 17–19 June 2019; pp. 77–84.
28. Pham, C.; Tang, D.; Chinen, K.; Beuran, R. CyRIS: A cyber range instantiation system for facilitating security training. In Proceedings of the 7th Symposium on Information and Communication (SoICT) ACM, Ho Chi Minh, Vietnam, 8–9 December 2016; pp. 251–258.
29. Tang, D.; Pham, C.; Chinen, K.; Beuran, R. Interactive cybersecurity defense training inspired by web-based learning theory. In Proceedings of the 9th International Conference on Engineering Education (ICEED), Kanazawa, Japan, 9–10 November 2017; pp. 90–95.
30. Davis, J.; Magrath, S. A survey of cyber ranges and testbeds. In *Defence Science and Technology Organisation (DSTO)*; Cyber Electronic Warfare Division (Australia): Edinburgh, South Australia, Australia, 2013; pp. 1–38.
31. Stoller, M.H.R.R.L.; Duerig, J.; Guruprasad, S.; Stack, T.; Webb, K.; Lepreau, J. Large-scale virtualization in the emulab network testbed. In *USENIX Annual Technical Conference*; USENIX: Boston, MA, USA, 2008; pp. 113–128.
32. Anderson, D.S.; Hibler, M.; Stoller, L.; Stack, T.; Lepreau, J. Automatic online validation of network configuration in the emulab network testbed. In Proceedings of the International Conference on Autonomic Computing, Dublin, Ireland, 12–16 June 2006; pp. 134–142.
33. Vykopal, J.; Ošlejšek, R.; Čeleda, P.; Vizvary, M.; Tovarňák, D. KYPO Cyber Range: Design and Use Cases. In *12th International Conference on Software Technologies (ICSOFT)*; Springer: Madrid, Spain, 2017; pp. 310–321.
34. Braje, T. Advanced tools for cyber ranges. *Linc. Lab. J.* **2016**, *22*, 24–32.
35. ECSO. Understanding Cyber Ranges: From Hype to Reality. 2020. Available online: https://ecs-org.eu/documents/publications/5fdb291cdf5e7.pdf (accessed on 30 April 2021).
36. Armstrong, P. *Bloom's Taxonomy*. 2016. Available online: https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/ (accessed on 1 June 2021).
37. Goeke, L.; Quintanar, A.; Beckers, K.; Pape, S. PROTECT—An easy configurable serious game to train employees against social engineering attacks. In *Computer Security*; Springer: Luxembourg City, Luxembourg, 2019; pp. 156–171.

38. Pape, S.; Goeke, L.; Quintanar, A.; Beckers, K. Conceptualization of a CyberSecurity Awareness Quiz. In *International Workshop on Model-Driven Simulation and Training Environments for Cybersecurity*; Springer: Guilford, UK, 2020; pp. 61–76.
39. D5.1: Real Event Logs Statistical Profiling Module and Synthetic Event Log Generator v1. 2020. Available online: https://www.threat-arrest.eu/html/PublicDeliverables/D5.1-Real_event_logs_statistical_profiling_module_and_synthetic_event_log_generator_v1.pdf (accessed on 1 June 2021).
40. Cichonski, P.; Millar, T.; Grance, T.; Scarfone, K. Computer security incident handling guide. *NIST Spec. Publ.* **2012**, *800*, 1–147.
41. Smyrlis, M.; Spanoudakis, G.; Fysarakis, K. Teaching Users New IoT Tricks: A Model-driven Cyber Range for IoT Security Training. *IEEE Internet Things (Iot) Mag.* **2021**, 1–10.
42. Tsandekidis, M.; Prevelakis, V. Efficient Monitoring of Library Call Invocation. In Proceedings of the 6th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Granada, Spain, 22–25 October 2019; pp. 387–392.
43. Papadogiannaki, E.; Deyannis, D.; Ioannidis, S. Head (er) Hunter: Fast Intrusion Detection using Packet Metadata Signatures. In Proceedings of the 25th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Virtual Conference, Pisa, Italy, 14–16 September 2020; pp. 1–6.
44. JMeter, A. Apache JMeter: Glossary. 2021. Available online: https://jmeter.apache.org/usermanual/glossary.html#:~:text=JMeter%20measures%20the%20latency%20from,be%20longer%20than%20one%20byte (accessed on 26 May 2021).