Project Title	Civil Cyber Range Platform for a novel approach to cybersecurity threats simulation and professional training
Project Acronym	CYBERWISER.EU
Project Number	786668
Type of instrument	Innovation Action
Topic	DS-07-2017 Cybersecurity PPP: Addressing Advanced Cyber Security Threats and Threat Actors
Starting date of Project	01/09/2018
Duration of the project	30
Website	www.cyberwiser.eu

D4.3 Cyber-training scenarios and scenario development method, initial version

Work Package	WP4 Training material, scenarios and evaluation
Lead author	Ioannis Kechaoglou (RHEA)
Contributors	Consuelo Colabuono (RHEA), Gencer Erdogan (SINTEF), Anže Žitnik (XLAB), Dario Varano (UNIPI), Liliana Ribeiro (EDP), Gonçalo Santos (EDP), Antonio Álvarez (ATOS)
Peer reviewers	Dario Varano (UNIPI), Silvia Garbin (AON)
Version	V1.0
Due Date	30/11/2019
Submission Date	29/11/2019

Dissemination Level:

X	PU: Public
	CO: Confidential, only for members of the consortium (including the Commission)
	EU-RES. Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)
	EU-CON. Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)
	EU-SEC. Classified Information: SECRET UE (Commission Decision 2005/444/EC)

The work described in this document has been conducted within the CYBERWISER project. This project has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 786668.

Version History

Revision	Date	Editor	Comments
0.1	27/02/2018	Ioannis Kechaoglou (RHEA), Consuelo Colabuono (RHEA)	First version
0.2	26/09/2019	Ioannis Kechaoglou (RHEA), Consuelo Colabuono (RHEA), Gencer Erdogan (SINTEF), Anže Žitnik (XLAB), Dario Varano (UNIPI), Liliana Ribeiro (EDP), Antonio Álvarez (ATOS)	Updated to include Scenario development workflow. Including feedback from Lisbon meeting and internal meetings.
0.3	14/10/2019	Ioannis Kechaoglou (RHEA), Gencer Erdogan (SINTEF), Anže Žitnik (XLAB), Dario Varano (UNIPI), Gonçalo Santos (EDP), Antonio Álvarez (ATOS)	Updates to include the Scenario Design Request structure and contents. Including feedback from internal meetings.
0.4	08/11/2019	Consuelo Colabuono (RHEA)	Addressed comments from Internal review performed by Dario Varano (UNIPI) and Silvia Garbin (AON)
0.5	18/11/2019	Ioannis Kechaoglou (RHEA)	Executive summary, Chapter 3 and conclusion integrated with ready to use scenarios
0.6	19/11/2019	Consuelo Colabuono (RHEA)	RHEA final review
1.0	29/11/2019	Ioannis Kechaoglou (RHEA), María Teresa García (ATOS)	Addressing Quality Check comments. Final version ready to be submitted

List of Contributors

The list of contributors to this deliverable are presented in the following table:

Section	Author(s)
Executive Summary	Ioannis Kechaoglou (RHEA), Consuelo Colabuono (RHEA)
1. Introduction	Ioannis Kechaoglou (RHEA), Consuelo Colabuono (RHEA)
2. Definitions	Ioannis Kechaoglou (RHEA), Consuelo Colabuono (RHEA)
3. Scenario development method (SDM)	Ioannis Kechaoglou (RHEA), Consuelo Colabuono (RHEA)
4. Ready-to-use scenarios	Ioannis Kechaoglou (RHEA), Consuelo Colabuono (RHEA)
5. Conclusions	Ioannis Kechaoglou (RHEA), Consuelo Colabuono (RHEA)

Keywords

Cyber training, cybersecurity, awareness, Scenario development method, Training, Cyber Range.

Disclaimer

Table of Contents

List of figures

List of tables

Executive Summary

This deliverable is the output of Task T4.2 “Cyber-training scenarios and scenario development method”. The Task started at M4 (December 2018) and will end at M24 (August 2020).

This task is part of WP4 entitled “Training material, scenarios and evaluation”, whose objectives are:

- Provide training material for developing/selecting risk models and real-time assessment and response proposal algorithms tailored to client needs, as well as for cyber-range testing and validation of such algorithms.
- Provide cyber-training scenarios that match the roles, skills and concerns of those being trained, and covering a variety of attack complexities. Also provide guidelines for developing new scenarios to ensure sustainability.
- Provide evaluation criteria for student performance.

Specifically, the output of this Task will produce two deliverables:

D4.3: Cyber training scenarios and scenario development method, initial version (M15 – November 2019). This is the initial version of the deliverable including a set of training scenarios developed by the project, as well as the method for training scenario development.

D4.5: Cyber-training scenarios and scenario development method, final version (M24 – August 2020). This is the final version of the deliverable documenting the set of training scenarios developed by the project, as well as the method for training scenario development.

This deliverable, D4.3, begins with an introductory section that states the purpose of the document and establishes a baseline of understanding of this document followed by the Scenario Development Method (SDM) and the ready-to-use scenarios.

The SDM developed is an iterative process initiated by the Scenario Design Request (SDR) which includes the scenario details as initially envisioned by the trainer. The scenario is developed with the continues interaction of all the participating actors requiring, in some cases, the partial of full deployment of the simulated environment multiple times. At the end of the process one scenario file is generated and the SDR contains all the necessary information required.

The two ready-to-use scenarios included in this version were selected to demonstrate the capabilities of the platform up to now and validate the SDM. The first scenario (4.1 Password cracking) was developed for the course B-05 Awareness of Password Weaknesses with hands-on training of the D4.1 [2] (Training material, initial version) and the second one (4.2 Network penetration: Phishing attack) was developed specifically for this deliverable scoping to demonstrate the current capabilities of the platform.

The next deliverable (D4.5) will focus on the update and improvement of the SDM, including the newly developed features, as well as the development of eight (8) more ready-to-use scenarios ad hoc or chosen from exercises developed under WP4 or WP5, in order to validate and demonstrate the development method.

1. Introduction

The CYBERWISER.eu project allows addressing of a variety of skill levels due to the advanced simulation capabilities and the flexibility of the platform.

This task is performed under WP4 Training material, scenarios and evaluation, which main objectives are:

- Provide training material for developing/selecting risk models and real-time assessment and response proposal algorithms tailored to client needs, as well as for cyber-range testing and validation of such algorithms.
- Provide cyber-training scenarios that match the roles, skills and concerns of those being trained, and covering a variety of attack complexities. Also provide guidelines for developing new scenarios to ensure sustainability.
- Provide evaluation criteria for student performance.

Risk models capture the impact of cyber-attacks on business objectives, thereby bridging the gap between attacks understood at a technical level and the business level view. Since objectives and systems differ greatly from one organization to another, this calls for models that reflect the individual client organization and system. The training material will be aimed at different levels of student skills (basic and advanced). In order to address the variety of skill levels, roles and concerns of those being trained, the set configurable cyber-attack scenarios will cover a variety of scenarios, from simple well-known attacks like SQL injection to creative interdisciplinary attack methods and advanced persistent threats. In order to facilitate the sustainability of the CYBERWISER.EU approach as the cyber threat landscape evolves, this task will also provide guidelines for developing new cyber-training scenarios.

We need clear criteria for evaluating the real-time response of students during cyber-range exercises, as well as the degree to which risk models and algorithms selected and/or developed by the students reflect the cyber-risk posture of the (simulated) target system and provide support for real-time response. In WP4, criteria, relevance, coverage, correctness, and response preparedness support will be established.

1.1 Purpose and scope of the document

The purpose of this document is to help the users of the platform to create cyber training scenarios (called “scenarios” hereafter) and provides also an initial set of ready-to-use scenarios. To do so, we will introduce a method to create scenarios covering a variety of complexity including guidelines and simple examples for better comprehension. Finally, the document will provide a sample of ready-to-use cyber-attack scenarios for cyber-range training of students and professionals (called “trainees” hereafter).

1.2 Structure of the document

Chapter 1 is the general introduction to the document containing the purpose and scope of the document, the relation to other work in the project and a glossary of acronyms.

Chapter 2 describes definitions used in the context of the development method.

Chapter 3 details the methodology to develop a scenario following a step-by-step approach starting with information gathering and continuing with the scenario design and the accessibility/visibility configuration. To allow better understanding the chapter begins with an overview of the scenario definition itself, the related roles, the workflow of the design and the analysis of the design methodology.

Chapter 4 presents a sample of ready-to-use scenarios as developed up to now as part of the validation of the process utilizing the currently available assets.

Chapter 5 states the main outcomes of this deliverable and the next steps for the final version.

1.3 Relation to other work in the project

The cyber-training scenarios will be used for cybersecurity training of trainees, while the method to be developed in task T4.2 and analyzed in this deliverable will be used for developing new cybersecurity training scenarios by the users of the platform.

1.4 Glossary of Acronyms

Acronym	Description
AM	Asset Manager
DNS	Domain Name Server
CPU	Central Processing Unit
GW	Gateway
ICT	Information and Communication Technologies
IP	Internet Protocol
NAT	Network Address Translation
OP	Operator
OS	Operating System
PLC	Programmable Logic Controller
SC	Scenario Creator
SDM	Scenario Development Method
SDR	Scenario Design Request
SDW	Scenario Design Workflow
TM	Training Manager
TR	Trainer
VM	Virtual Machine
WP	Work Package
WS	Work Station

Table 1. Table of acronyms

2. Definitions

In this section, preliminary notions are presented to establish a baseline of understanding for this document.

2.1 Scenario (Cyber-range exercise)

A **training scenario** (or “scenario”) is a multi-layered description of a cyber-range exercise, which is a trainees' activity pertaining a particular training scenario instance. In a cyber-range exercise, a trainee interacts with the simulated environment corresponding to a specific training scenario instance.

If not explicitly stated otherwise, the term training is used for “training”, “lab” or “exercise”

2.2 Training Manager Roles

The Training Manager (TM) uses a user-role access control mechanism to manage the access to its capabilities and assets. The following are the main roles that will be used for the scenario development. Other roles of the TM are presented in this document.

- **Trainer (TR):** An individual responsible for the design of the scenario. The design is conducted outside of the platform and it is taken as input from the Scenario Creator (SC). The TR is also responsible for some aspect of the scenario configuration. Details are included in the scenario development workflow.
- **Scenario Creator (SC):** An individual responsible for creating the scenario in the platform based on the design provided by trainer.
- **Operator (OP):** An individual responsible for validating and instantiating the scenario.
- **Asset Manager (AM):** An individual responsible for creation and modification Digital Library assets.

3. Scenario Development Method (SDM)

This deliverable describes the method to develop a scenario within the **Training Manager (TM),** the module responsible for providing an environment where users can design training scenarios and use those scenarios as part of training activities. A training activity can make use of multiple scenarios. The Training Manager facilitates users that want to design a scenario by providing a multi-layer Scenario Designer approach. It allows users to authorize other users to help design a scenario or take part in using the scenario once it has been instantiated. Fine grained access control rules allow us to expose only parts of the scenarios to individual users.

The scenario development method introduced in this document is composed of two major components:

- Scenario Design Workflow (SDW)

The SDW descripts the steps of the development method, the participating roles and their interaction.

- Scenario Design Request (SDR)

The SDR contains all the necessary information required to create a scenario.

3.1 Scenario Design Workflow (SDW)

The workflow of the scenario development method follows an iterative approach between its steps to allow the creation of complex scenarios. Figure 1 illustrates the workflow of the method which consists of the following high-level steps:

1) Designing
2) Creation
3) Validation
4) Instantiation
5) Configuration and Testing
6) Finalization

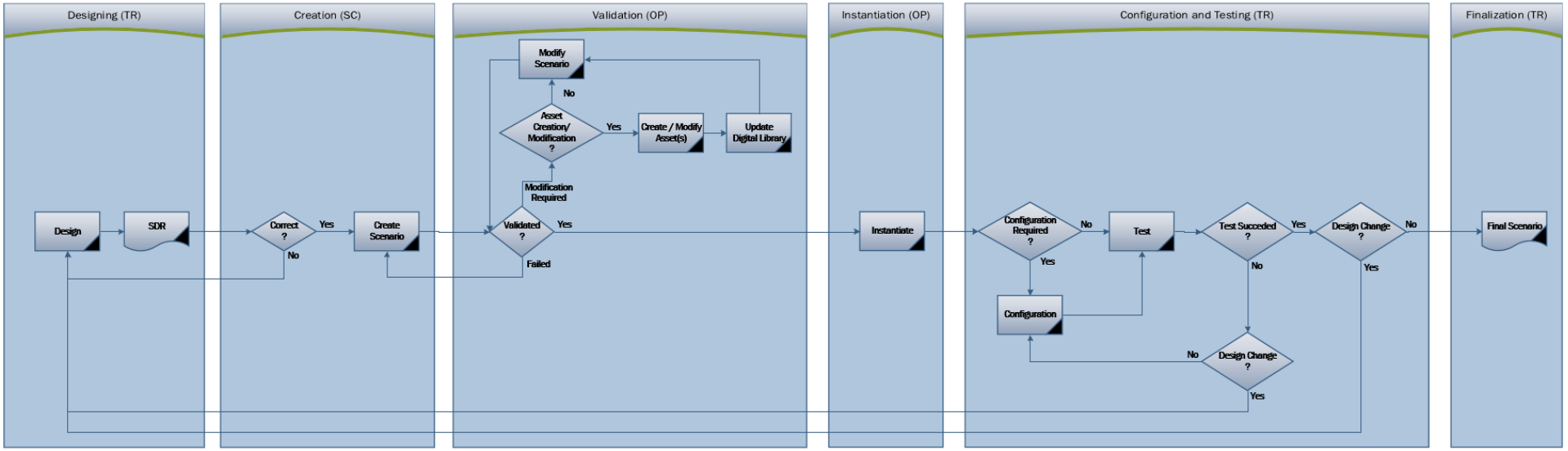

Figure 1: Scenario Development Workflow (SDW)

Following an analysis of each step:

1) Designing

The TR is responsible for designing the scenario in terms of network design, application configuration and timeline of events. The outcome is the Scenario Design Request (SDR).

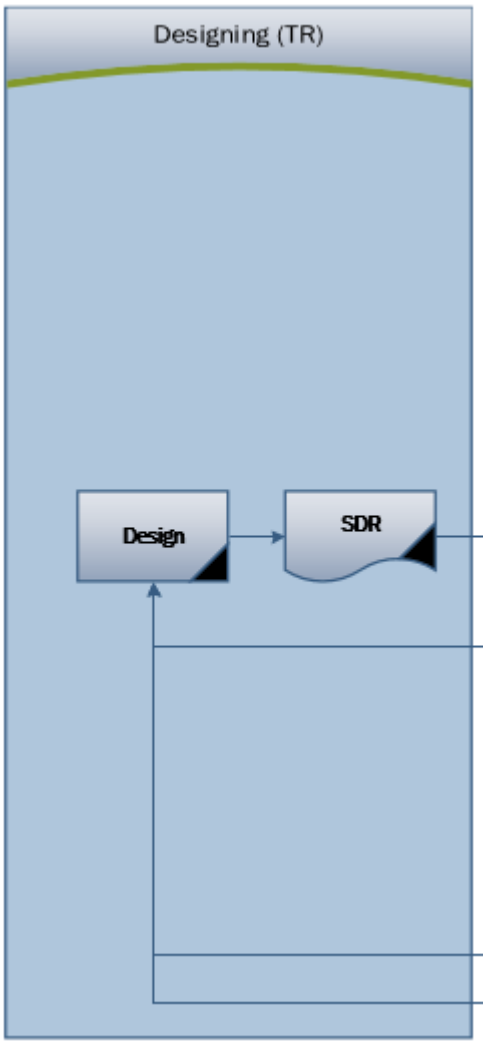

Figure 2: SDW - Designing

2) Creation

The SC is responsible for creating the scenario based on the description provided from the TR detailed in the SDR.

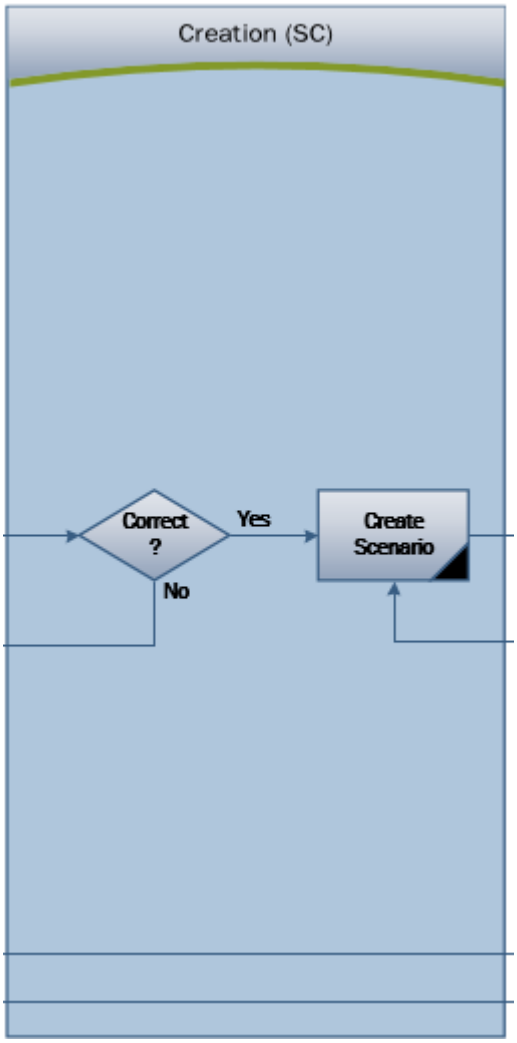

Figure 3: SDW - Creation

3) Validation

After scenario creation, the scenario is submitted to the OP for validation. At this step, the OP will check the scenario for completeness, correctness and any asset requests. Depending on the outcome of the validation:

a) Validation succeeded

If validation succeeds the scenario can be instantiated.

b) Validation failed (Rejected)

If validation failed, the scenario is rejected and returned to the SC along with relevant comments for correction and resubmission.

c) Modifications required

In this case either the changes required can be applied/resolved by the OP or the OP must create/modify Digital Library assets. Any changes to the Digital library will require collaboration with the AM.

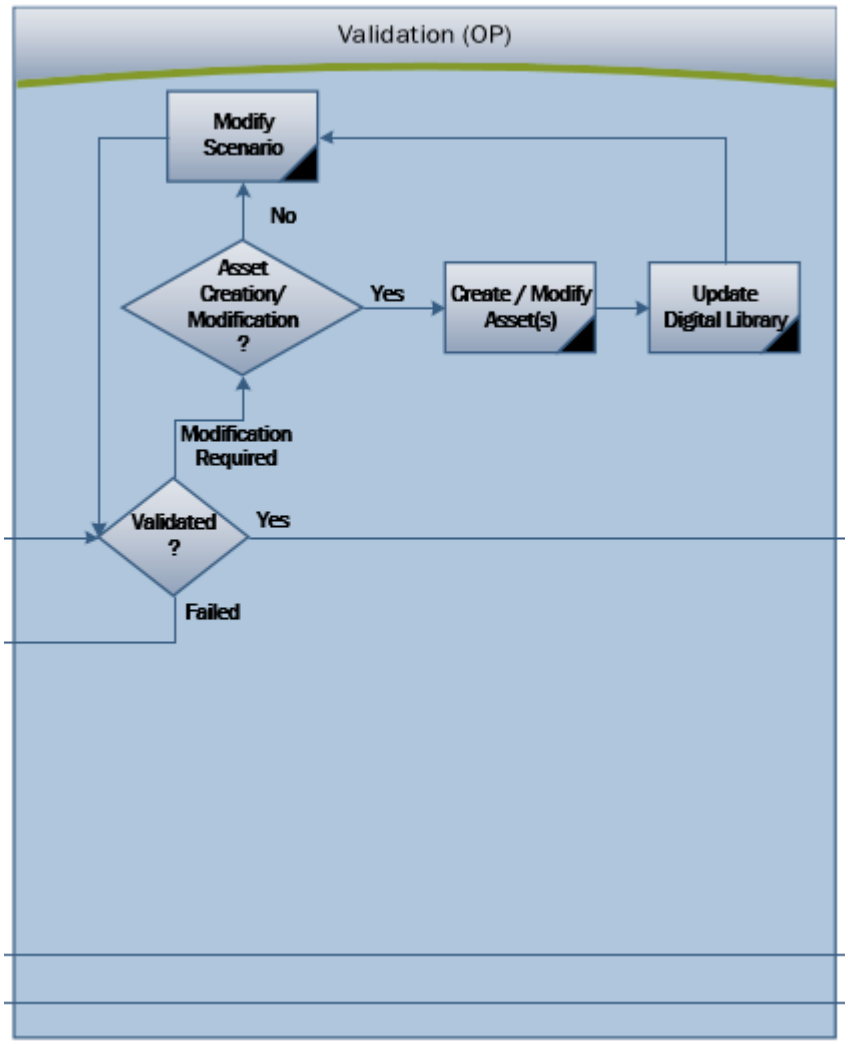

Figure 4: SDW - Validation

4) Instantiation

At this step the OP instantiates the scenario and notifies the TR.

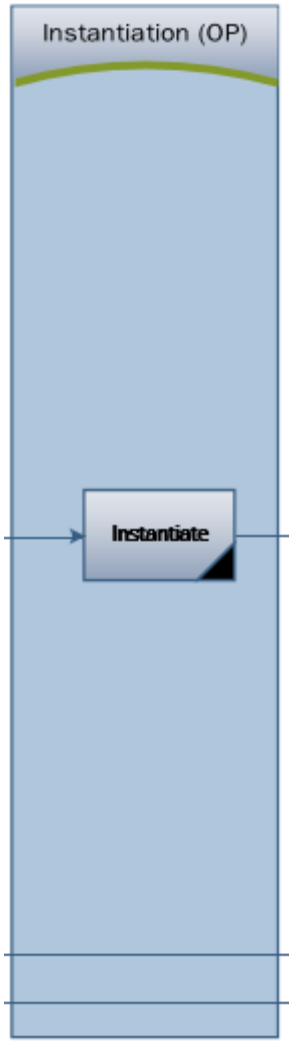

Figure 5: SDW - Instantiation

5) Test and Configuration

The instantiated scenario must be tested by the TR to verify that it meets the needs of the training. In some cases, the TR may require changing the configuration, test different use cases or/and create training material in the instantiated scenario. All of these actions are carried out under the configuration action.

There are two possible outcomes from the scenario testing:

a) Success

The scenario is ready to be finalized.

b) Fail

The scenario is not ready to be finalized and change(s) are required either in the SDR or in the configuration. In case of SDR change the workflow starts from step 1 and the scenario is terminated (un-instantiated). The iteration from step 1 to step 4 continues until the scenario testing succeeds and the scenario can be finalized.

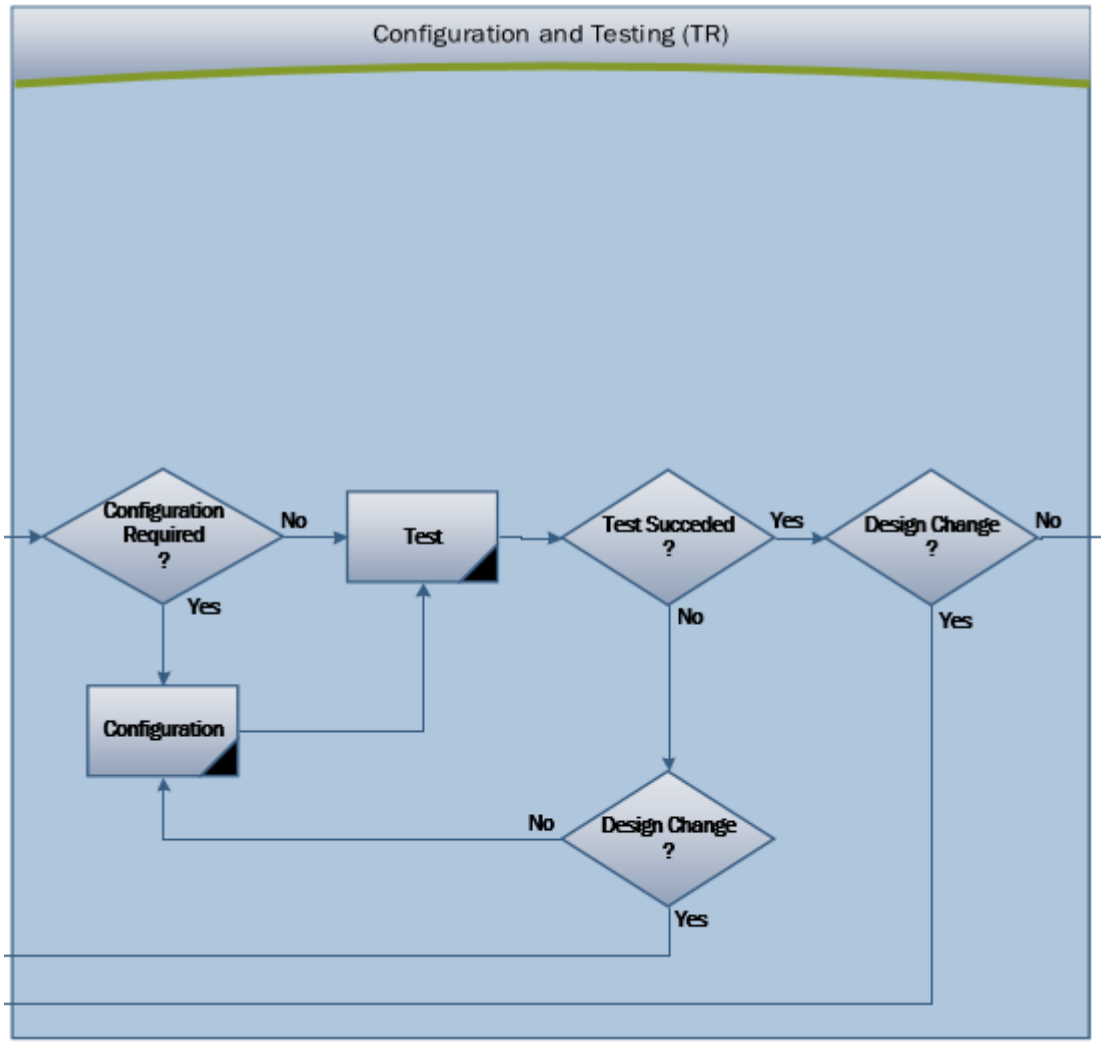

Figure 6: SDW – Configuration and Testing

6) Scenario finalization

After the successful testing of the scenario by the trainer the scenario can be finalized and saved. The scenario can be un-instantiated.

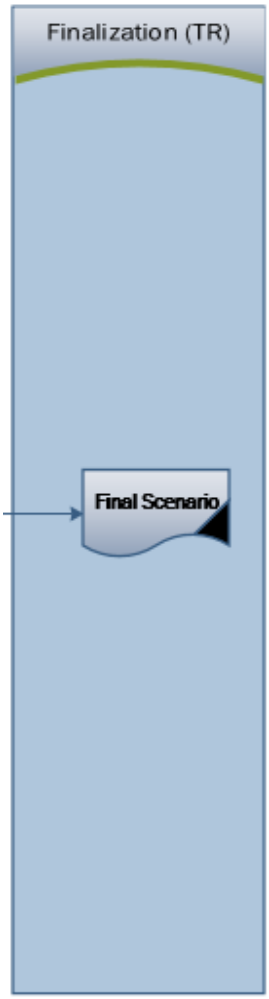

Figure 7: SDW - Finalization

3.2 Scenario Design Request (SDR)

The scenario design method is based on a step-by-step approach, composed by the following steps:

1) General Scenario information
2) Network topology
3) Application configuration
4) Timeline
5) Access control and visibility
6) Performance Evaluation

   [Will be completed as the evaluation method evolves and added in the final version of the deliverable. Includes the evaluation method and criteria, monitoring infrastructure, etc.]

7) Scenario files

Following an analysis of each step.

1) General Scenario information

It contains general information about the scenario in order to have an overview about its purpose and to categorize it accordingly.

Information required	Description of information required
*Scenario Name **	Name chosen for the specific scenario
*Description**	Description of the scenario. Can be as detailed or as simple as required. Keep in mind that detailed instructions and additional documentation can be uploaded and attached to various elements of the scenario.
Motivation	Brief description about the purpose of the scenario.
*Category**	The category of a scenario is the kind of service provided with the virtual environment. Not all services are "training" services. One of the following categories has to be selected: • Space System Software • Cyber Security Pen Testing • Cyber Training Lab • Hybrid environment
*Type**	The type of the scenario defines the available layers during the design. One of the following types of scenario has to be selected: • Business It enables the "**Business**" layer that introduces business processes elements • Training It enables the "**Training**" layer that introduces a timeline of the training activity

Table 2: General Scenario Information

2) Network topology

The network topology defines the infrastructural layout of the scenario. The TR must design the infrastructure to be simulated providing the network topology diagram and the required information for each component.

Following a definition of the components that can be simulated by the platform and the required information for their implementation. The TR can leave some of the information empty authorizing the SC to complete them as seems fit.

- **Gateway**
  Represents a gate between two or more networks. It can be a router, firewall or other device that enables/controls flow between different networks.

Information required	Description of information required
Name	Name of the component
Description	Brief description of how the GW will be used in the context of the scenario, and also the OS or applications installed.
Operating system	Operating system of the component. It can be as detailed as required for the needs of the scenario
Virtual Machine	Details the following features of the VM: • Number of CPUs (from 1 to 8) • Multiplicity (from 1 to 100)

Information required	Description of information required
	• Memory of the VM (a positive integer)
Policies	Description of policies to be applied to the Gateway type in terms of: • Source Network • Source VM • Target Network • Target VM • Action Port • Delete
Network Interface(s)	Description of Network Interface to be set

Table 3: Network Topology components - Gateway

- **Workstation**
  Represents an endpoint device serving one user at a time in contrast with the servers. Examples include Windows 10, Ubuntu Desktop, etc.

Information required	Description of information required
Name	Name of the component
Description	Brief description of how the WS will be used in the context of the scenario, and also the OS or applications installed.
Operating system	Operating system of the component. It can be as detailed as required for the needs of the scenario
Virtual Machine	Details the following features of the VM: • Number of CPUs (from 1 to 8) • Multiplicity (from 1 to 100) • Memory of the VM (a positive integer)
Network Interface(s)	Description of Network Interface to be set

Table 4: Network Topology components - Workstation

- **Server**
  Represents a computer program or a device that provides functionality for other programs or devices, called "clients". Examples include Windows and Linux server operating systems.

Information required	Description of information required
Name	Name of the component
Description	Brief description of how the WS will be used in the context of the scenario, and also the OS or applications installed.
Operating system	Operating system of the component. It can be as detailed as required for the needs of the scenario
Virtual Machine	Details the following features of the VM: • Number of CPUs (from 1 to 8) • Multiplicity (from 1 to 100) • Memory of the VM (a positive integer)
Network Interface(s)	Description of Network Interface to be set

Table 5: Network Topology components – Server

- **Network**
  Represents a switch used to connect multiple Information and Communication Technologies (ICT) devices simulated in the platform.

Information required	Description of information required
Name	Name of the component
Description	Brief description of how the Network will be used in the context of the scenario
Network details	Description of the network properties: • Start IP • Subnet Mask • Default Gateway • DNS

Table 6: Network Topology components - Network

- **External Network**
  Represents a switch used to connect simulated devices with real hardware devices. This capability is referred as "hybrid mode" where the simulated environment interacts with the "real world".
  The information required is the same as in Network component (Table 6).
- **Network Appliance**
  Represents a physical device that can be part of a scenario. The network appliance can be added to the scenario when required, utilizing the hybrid mode. As an example, a Programmable Logic Controller (PLC) that cannot be virtualized can be directly connect via the hybrid mode.
  The information required is the same as in Gateway (Table 3) or Workstation (Table 4) components.
- **Server Appliance**:
  Similar to Network Appliance this category is dedicated to physical servers.
  The information required is the same as in the Server (Table 5) component.

3) Application configuration

This section includes details about the applications needs to be installed in the components (VMs) described in the Network topology section. Any configuration details of those application (if required) must be included.

Information required	Description of information required
Name	Name of the application
Description	Description of how the application will be used in the context of the scenario.
Version	The version of the application (if required).
Configuration details	Specific configuration details need to be applied to the application

Table 7: Application Layer components – Application

4) Timeline

The TM supports the definition of scenario events and events triggers for the simulated environments leveraging the training scenario requests.

An event is an action executed by the CYBERWISER.eu Platform in the context of a cyber-range exercise. Example of an event is a scripted attack (performed by the Attack Simulator) towards the simulated infrastructure.

A trigger is an element of the training scenario that defines the start of an event. Triggers are defined with a time point or can be based on the state of the cyber-range exercise.

The Event is something that occurs during a training, either because a human Actor does something or because an automated Automaton does something. The automaton is therefore like the actor, not a human actor but rather something automated like for example a traffic generator, or an automated script that is running somewhere.

This layer contains nodes in the form of:

- **Start:** represents an element of the timeline that represents the moment (in minutes) of when Actor or an Automaton performs an Action according to the exercise, which is running.
- **Stop:** represents an element of the timeline that represents the moment (in minutes) of when an Action performed by an Actor or an Automaton has to finish according to the exercise, which is running.
- **Actor:** represents the user who is performing an action. Automation: represent a script that simulate a specific action that can be performed by a user.
- **Action:** represents the implementation of a specific interaction with the simulated environment; an Actor node or an Automaton node can trigger the Action.
- **Event**: represents the result of a specific action in the timeline or of a user.

5) Access control and visibility

The TM utilizes a Role Based Access Control mechanism to provide or restrict access based on the needs of the training for each participant and includes:

- Access to a specific VMs
- Access to supporting scripts (e.g. attack scripts)
- Visibility of components
  Specific aspects of the scenario can be hidden from specific trainees to provide more realistic training.

During the scenario development the TR must identify all the relevant roles and create the corresponding users to test the access control in place for each one of them.

6) Performance Evaluation

[Will be completed as the evaluation method evolves and added in the final version of the deliverable. Includes the evaluation method and criteria, monitoring infrastructure, etc.]

7) Scenario files

This includes any files necessary to the execution of the scenario.

Following a list (not inclusive) of possible files to be included:

- Exercise description
- Step-by-step instructions
- Packet captures
- Malwares
- Configuration files
- Disk images files
- Memory image files

4. Ready-to-use scenarios

In this section, two sample scenarios will be introduced. The scenarios were developed using the development method described in Section 2.

4.1 Password cracking

1) Description

In this scenario the trainee will be guided into a password cracking exercise.

Exercise features

Name	Password cracking
Requirements	Basic knowledge of computer operations.
Educational Objectives	After performing this exercise, trainees will be able to: • Understand the importance of a secure password. • Identify and produce a secure password.
Duration	30 minutes
Actual Specification	The trainee will have access to a standalone Kali Linux VM. The VM will contain 3 password files and a scenario instruction file. The file contains step-by-step instructions on password cracking using the brute force and dictionary attack method as well as required background information.
Virtualized Assets	The scenario will utilize a standard Kali Linux 2019 distribution without any additional configuration.
Evaluation Method	Not applicable

Table 8: Exercise features of the Password cracking scenario.

2) Network topology

A single standalone VM is deployed. Network configuration is not required.

3) Training flow

Training flow is comprised by step-by-step instructions in the accompanied scenario instructions' file.

4) Scenario files

The following files are required and provided with this document:

a. Scenario instructions
   S-01 - Password Cracking v1.0.pdf
b. Password files
   easy.txt, medium.txt, difficult.txt
c. Scenario file
   [CW] Password cracking.json)

4.2 Network penetration: Phishing attack

1) Description

The trainee will attempt a network penetration utilizing a phishing attack

Exercise features

Name	Network penetration: Phishing attack
Requirements	Intermediate knowledge of penetration testing/ethical hacking techniques.
Educational Objectives	After performing this exercise, trainees will be able to: • Create a typical remote reverse shell exploit. • Perform a phishing attack. • Understand the significance of phishing attack awareness training.
Duration	30 minutes
Actual Specification	The trainee will have access to a Kali Linux VM and a set of email addresses to use in the phishing attack. The target user will operate inside a typical corporate environment protected behind a FW. The user will represent a user with lack of cybersecurity awareness clicking any link he/she finds in his/her emails as well as executing/opening any attachments. The trainee must prepare a phishing attack, exploiting the aforementioned user behaviour with the end goal of establishing an interactive reverse shell access.

Virtualized Assets	The scenario will include the following virtualized assets:
	• Windows 7 operating system VMs
	  ○ Purely patched OS.
	  ○ No antivirus protection.
	  ○ Outlook email client installed.
	  ○ User simulation module installed “clicking” all links and executing/opening all attachments in the received emails.
	• VyOS FW
	  ▪ Only outbound traffic is allowed.
	  ▪ LAN traffic is NATed to the FW external IP
	• DNS
	Resolution of the email server: mail.citef.int
	• Email Server (mail.citef.int)
	  ○ Allows email exchange.
	  ○ Available accounts:
	  ▪ Corporate
	  - CEO: ceo@corp.com
	  - Sales Director: sales@corp.com
	  ▪ Attacker
	  - IT Corp: it.corp@evil.int (password: it.corp1)
	• Gateway router
	Allows network connectivity of the participating network
	• Kali Linux 2019 with no additional configuration

Evaluation Method	The trainee must retrieve and present the file “ConfidentialDocument.txt”, located in the CEO computer, to the trainer.

Table 9: Exercise features Network penetration: Phishing attack scenario.

2) Network topology

Figure 8 demonstrates the network topology of the scenario. Detailed network configuration is provided in Table 10.

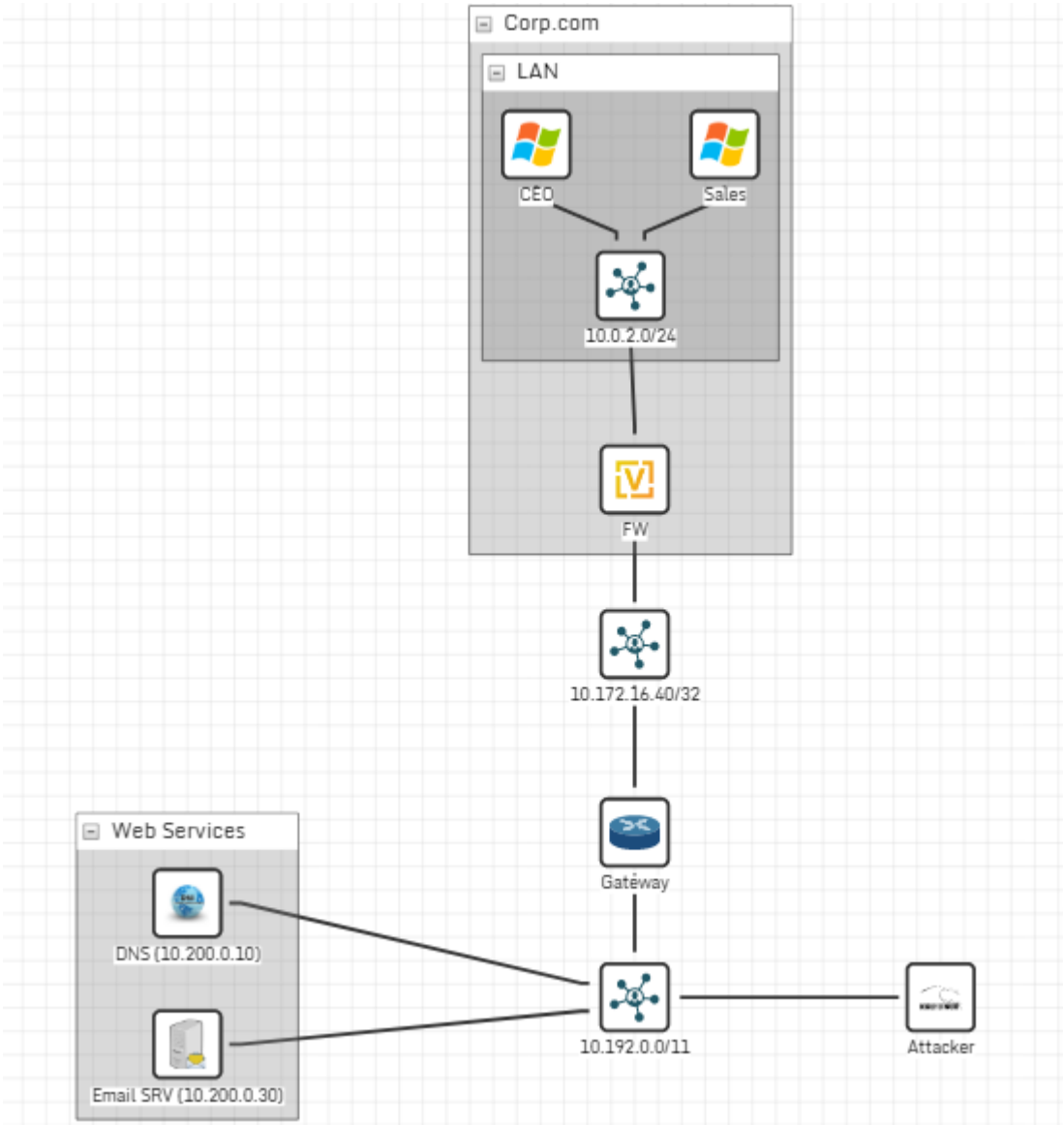

Figure 8: Scenario Network Topology

Network	VM	IP/Mask	Default Gateway	DNS
LAN	CEO	DHCP (net 10.0.2.0/24)	10.0.2.1	10.200.0.10
	Sales			
Internet	DNS	10.0.200.10/11	10.192.0.1	10.200.0.10
	Email Srv	10.0.200.30/11	10.192.0.1	10.200.0.10
	Attacker	10.195.28.116/11	10.192.0.1	10.200.0.10

Table 10: Network configuration

3) Training flow

Not applicable in this scenario.

4) Scenario files

The following files are required and provided with this document:

a. Scenario instructions:
   S-02 - Network Penetration Phishing Attack_v1.0.docx
b. Scenario file
   [CW] Network Penetration_ Phishing attack.json

5. Conclusions

Main outcome of this deliverable is the initial development method for cyber training scenarios and two ready-to-use scenarios.

The method allows design and configuration of cybersecurity scenarios to be used in cybersecurity training, based on specific requirements. The provided scenarios were developed using this method and include currently available features in the platform.

Next steps include the evolvement of the method to include new and improved features, as they are developed, as well as the development of new scenarios. The new scenarios will focus mainly in two areas, validation of the scenario development method and demonstration of the capabilities of the platform utilizing all available features/capabilities.

References

[1] Grant Agreement-786668-CYBERWISER_EU

[2] CYBERWISER.eu Project. D4.1 Training material, initial version. June 2019