CYBERWISER.eu

Cyber Range & Capacity Building in Cybersecurity

Niccolò Zazzeri

Trust-IT Services

The CYBERWISER.eu project

Cyber Range Network

Joint Webinar

Co-funded by the European Commission
Horizon 2020 – Grant # 786668

CYBERWISER.eu, in a nutshell

- An **H2020 Innovation Action** aiming to become the EU's reference, authoritative, independent ***cyber range platform for professional training***.
- From September 2018 through February 2021.
- Featuring an **open pilot stream**, for you to get to use the CYBERWISER.eu platform (for free!) – Book your own pilot at https://cyberwiser.eu/content/open-pilot-stream

Our main end user targets

1. Cybersecurity students at IHEs and Early Career Professionals

2. SMEs and Mid-caps

3. Large Enterprises and Operators of Critical Infrastructures

4. Public Sector Organisations

CYBERWISER.eu Objectives

- Deliver a European Platform for cybersecurity professional training
- 3 full-scale pilots in key vertical markets & education and activate and manage the “Open Pilots Stream”.
- Innovative cybersecurity training tools and materials
- Develop a sustainability model for the CYBERWISER.eu training platform.
- Create robust & insightful economic models for monetary exposure assessment to risk in virulent cyber climates
- Develop and run the "Cybersecurity Professional Register” to promote cybersecurity capacity building in Europe

Contribute to the continuous development of a cybersecurity culture across EU society.

CYBERWISER.eu Training Offer

PRIMER

- Created for students or beginner-level professionals.
- At the primer offering level you can experience the CYBERWISER.eu **e-learning & communication tools such as Web Portal, Cross-Learning Facilities**.
- The Primer Offering Level gives you an **overall introduction to the cyber-risk analysis process**.
- The topics covered within this offering level are the **most common threats like phishing, ransomware and some cases of data leakage**.
- Additional topics to be covered are best practices on reducing insider threats and how to manage and set passwords.

BASIC

- Created for professionals that already know the basic concepts and best practices of cybersecurity.
- The basic Offering Level lessons include a structured approach to identifying and documenting security assets and cyber risks.
- CYBERWISER.eu cyber range environment **includes a wide amount of high realistical practical simulations**.
- At the basic offering level **you can experience training scenarios composed by up to 10 elements**.
- A **set of monitoring sensors**.
- A **basic limited suite of pre-defined attack scripts**.

INTERMEDIATE

- Created for expert users from business context as SMEs or Large Enterprises as well as Public Sector.
- Within the intermediate Offering Level are developed also aspects of **context establishment, cyber-risk assessment, cyber-risk treatment, and cost/benefit analysis not covered at the Basic level**.
- At this level are available **training scenarios composed by up to 50 elements**.
- A set of **monitoring sensors tailored to specific exercises**,
- A **full suite of pre-defined attack with suggestions of possible countermeasures**.
- A **set of models that may be executed by Economic Risk Evaluator are also available**.

ADVANCED

- Created for large organisations or public administrations that have more advanced cybersecurity training needs.
- The advanced Offering Level covers all aspects of context establishment and cyber-risk assessment, as well as cyber-risk treatment and cost/benefit analysis.
- At this level are available **training scenarios composed by up to 500 elements**.
- The Digital Library offers a **full choice of virtual templates and the possibility of creating new ones**.
- A **set of monitoring sensors tailored to specific exercises**,
- A **full suite of pre-defined attack with suggestions of possible countermeasures**.
- **The risk assessment algorithm produces risk levels in terms of economical loss given that the risk materializes**.

3 Full Scale Pilots supporting validation

Energy Generation And Distribution

Railroad Transport

Professional And Academic Training

Practical use cases application in FSPs

Academic Pilot

- SQL Injection
- Firewall and Network Filtering
- Network and Vulnerability Scan
- Idle Scan
- Privilege Escalation
- AppArmor Defense
- Session Hijacking

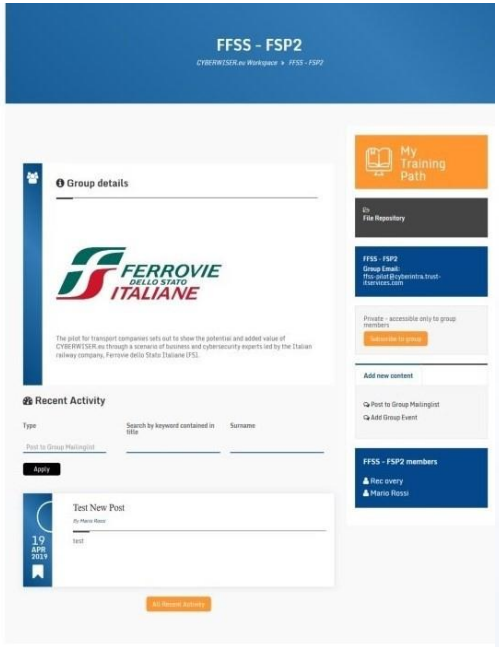
Transport Pilot

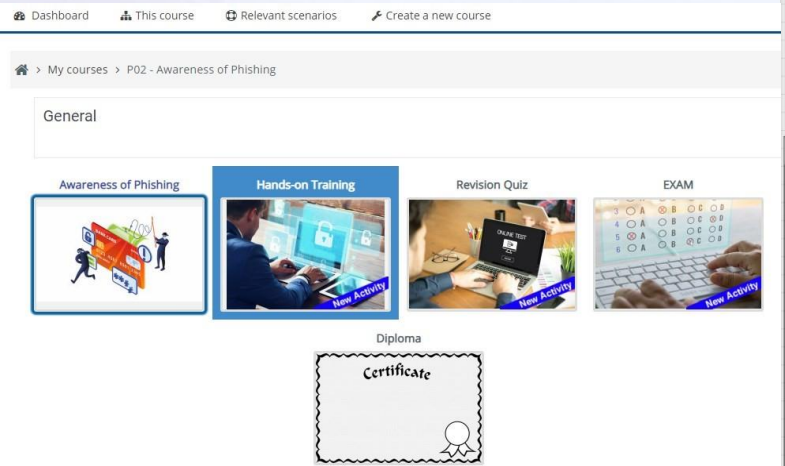
- SQL Injection
- Phishing attack
- Password Cracking
- Red team vs Blue Team (TBD)

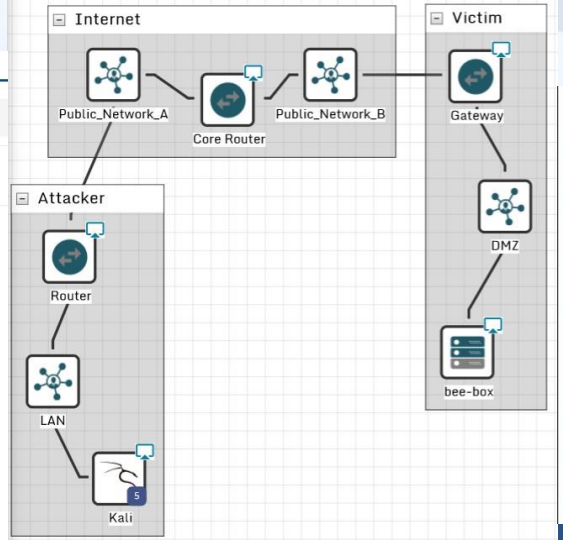
Energy Pilot

- SQL Injection
- Cross-Site Scripting
- Phishing Attack
- Targeted Malware
- Power outage

CYBERWISER.eu Training Path







Opportunity: the Open Pilots Stream

Open Pilots Stream

- Train your staff for free!
- Fully customizable cyber training to meet your cybersecurity needs
- Get access to one of the most advanced Cyber Range platforms in the world

What is it?

An Open Pilot is your opportunity to train your staff in cybersecurity, for free, on the CYBERWISER.eu Capacity Building Cyber Range Platform. You will benefit from a customisable learning path based on your organisation's needs!

Who is it for?

Our Open Pilot Stream is dedicated to **SMEs**, **Research & Academia**, **Large Companies** and **any organisation** interested in testing our platform

While our training is directed primarily towards **IT personnel** who need to develop advanced skills in cybersecurity, training pathways have also been created for **individuals** from other, **non-technical areas** of an organisation.

How does it work?

It is very easy! All you need to do is following the steps below. Please note that the duration of your Training Pilot will be determined by the customised specifications we agree on. An introductory workshop is the ideal place for these discussions but you can also get the ball rolling by completing the application form here. The average length of an open Pilot is between 3 and 6 months.

- ***Complete the form with the requirements of your own Pilot:*** https://www.cyberwiser.eu/content/cyberwisereu-open-pilot-scheme
- ***What we will grant you as Open Pilot?***
  - Onboarding package to use the platform (training material and dedicated interfaces)
  - Issued credentials to manage the instantiation of the platform for your specific Pilot
  - Continuous support by our Team

Thank you for your attention! *Questions?*

Main contact:

Niccolò Zazzeri, n.Zazzeri@trust-itservices.com

WP6 Leader

www.cyberwiser.eu @cyberwiser

© Copyright 2018 - CYBERWISER.eu has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement no 786668. The content of this document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content