#### Home > ... > H2020 >

Civil Cyber Range Platform for a novel approach to cybersecurity threats simulation and professional training



# Civil Cyber Range Platform for a novel approach to cybersecurity threats simulation and professional training

### **Results**

Project Information

CYBERWISER.EU

Grant agreement ID: 786668

Project website 🛃

DOI 10.3030/786668

Project closed

**EC signature date** 23 April 2018

Start date 1 September 2018 End date 28 February 2021

**Funded under** Secure societies - Protecting freedom and security of Europe and its citizens

**Total cost** € 5 323 407,50

**EU contribution** € 4 134 245,00

Coordinated by ATOS SPAIN SA Spain

### This project is featured in...



CORDIS provides links to public deliverables and publications of HORIZON projects.

Links to deliverables and publications from FP7 projects, as well as links to some specific result types such as dataset and software, are dynamically retrieved from OpenAIRE

### Deliverables

### Documents, reports (14)

Pilots - Experiences and results, initial version

This deliverable reports the design and the progress of implementation of the three full scale pilots.

#### Cyber training scenarios and scenario development method, initial version 🖸

This is the initial version of the deliverable documenting the set of training scenarios developed by the project, as well as the method for training scenario development.

#### Risk model templates, initial version [2]

This deliverable provides the initial version of the risk model templates to enable real-time analysis of cyber risks, threats and vulnerabilities of the systems being simulated in the cyber-range environment.

#### Platform design, final version [2]

This deliverable builds on top of D2.3 and incorporates the feedback received from the evaluation of the first platform prototype to describe the additional requirements and design for the final version of the CYBERWISER.EU platform.

Communication plan third & final iteration version

Third & final iteration of the communication strategy report, providing all the necessary detail on activities to be performed, vis-à-vis the targeted stakeholders, and related, measurable variables to be monitored.

#### Risk model templates, final version [2]

This deliverable builds on top of D2.6 to provide the final version of the risk model templates to enable real-time analysis of cyber risks, threats and vulnerabilities of the systems being simulated in the cyber-range environment

#### Communication plan second iteration version

Second of three iterations of the communication strategy report, providing all the necessary detail on activities to be performed, vis-à-vis the targeted stakeholders, and related, measurable variables to be monitored.

#### Cyber-training scenarios and scenario development method, final version [2]

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.

#### Platform design, initial version

This deliverable provides an early version of the CYBERWISER.EU platform design. The initial set of tools to be integrated is presented, as well as a detailed description of the platform architecture. This deliverable represents the basic input for WP3.

#### Training material, final version

This deliverable documents the final version of the training material for risk modelling and response preparedness.

#### General Requirements and Guidelines 12

This deliverable provides the requirements and the specifications of the three pilots.

#### Training material, initial version

This deliverable documents the initial version of the training material for risk modelling and response preparedness.

#### Communication & stakeholder plan first version [2]

First of three iterations of the communication strategy report, providing all the necessary detail on activities to be performed, vis-à-vis the targeted stakeholders, and related, measurable variables to be monitored.

Real-time performance and evaluation criteria C

This deliverable documents the criteria established by CYBERWISER.EU for evaluation of student performance in cyber-range exercises.

## **Publications**

Conference proceedings (3)

An Approach to Train and Evaluate the Cybersecurity Skills of Participants in Cyber Ranges based on Cyber-Risk Models 2

**Author(s):** Gencer Erdogan, Åsmund Hugo, Antonio Romero, Dario Varano, Niccolò Zazzeri, Anže Žitnik

**Published in:** Proceedings of the 15th International Conference on Software Technologies, 2020, Page(s) 509-520, ISBN 978-989-758-443-5 **Publisher:** SCITEPRESS - Science and Technology Publications **DOI:** 10.5220/0009892105090520

Developing Cyber-risk Centric Courses and Training Material for Cyber Ranges: A Systematic Approach

**Author(s):** Gencer Erdogan, Antonio Romero, Niccolò Zazzeri, Anže Žitnik, Mariano Basile, Giorgio Aprile, Mafalda Osório, Claudia Pani, Ioannis Kechaoglou

**Published in:** Proceedings of the 7th International Conference on Information Systems Security and Privacy, 2021, Page(s) 702-713, ISBN 978-989-758-491-6

**Publisher:** SCITEPRESS - Science and Technology Publications **DOI:** 10.5220/0010393107020713

Tool Support for Risk-driven Planning of Trustworthy Smart IoT Systems within DevOps C

Author(s): Andreas Thompson, Gencer Erdogan

**Published in:** Proceedings of the 6th International Conference on Information Systems Security and Privacy, 2020, Page(s) 742-753, ISBN 978-989-758-399-5

Publisher: SCITEPRESS - Science and Technology Publications DOI: 10.5220/0009189307420753

Last update: 5 September 2023