CYBERWISER.eu

Cyber Range & Capacity Building in Cybersecurity

CYBERWISER.eu Cyber Range

Pierluigi Cara

RHEA Group

RHEA GROUP

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

Cyber Range – Key Concepts

- What is a Cyber Range?
  - A recent concept
  - A multipurpose virtualization environment supporting three main needs:
    - Knowledge development and dissemination (training)
    - Improved system assurance in development (R&D)
    - Improved system assurance through test and evaluation (testing)
  - A safe environment for cyber attack scenario simulation and test

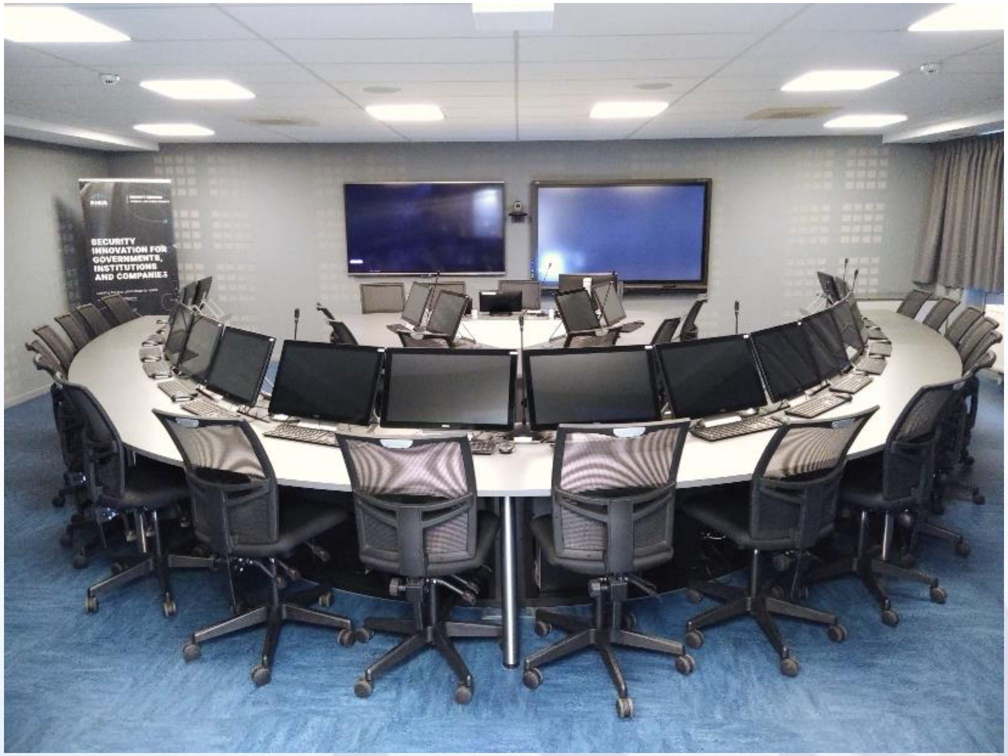
Research and Development
Training
Test and evaluation

Cyber Range – Training

Cyber ranges are extremely suited for security training purposes

- The virtual environments allow trainers and trainees to perform multiple realistic training scenarios with a fraction of cost and effort needed for building and configuring similar physical platforms

- On next-generation ranges, the freedom of configuring and monitoring the training scenario in real-time is invaluable for trainers

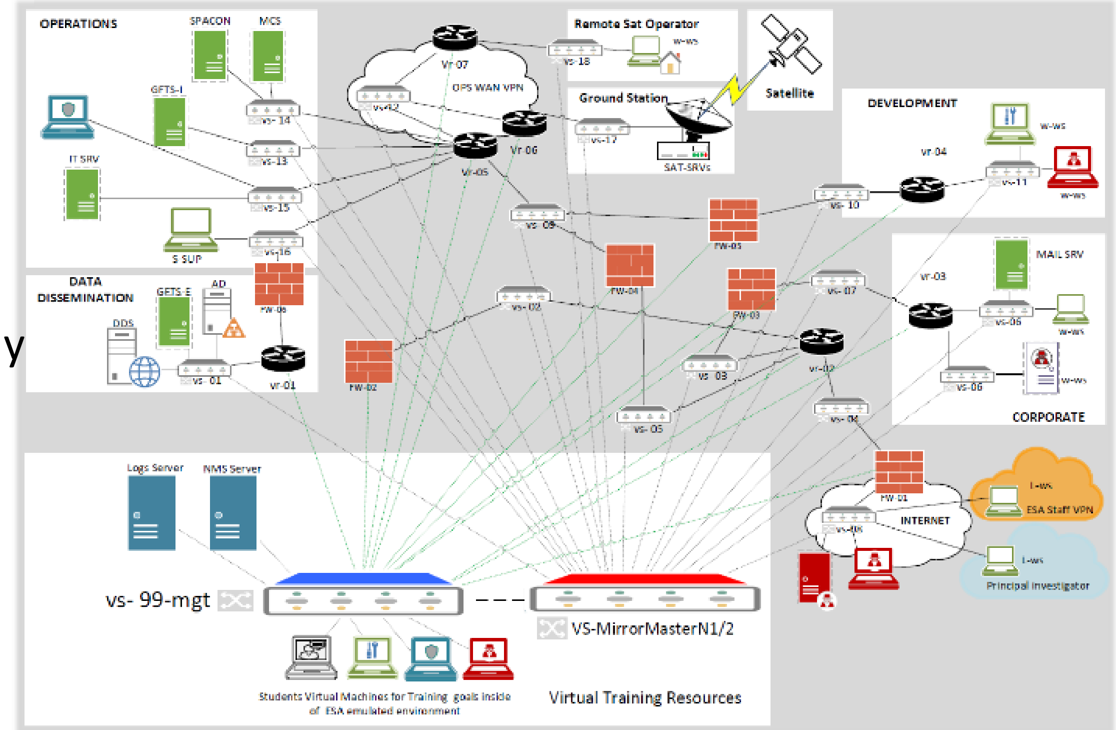


Cyber Range: Research and development

Reducing the cyber threat through emulation

- All critical infrastructure systems are at risk of cyber security attacks. Being aware of the risks from early stages of system and software development is vital for building secure infrastructure.

- The realistic emulation environment facilitates experimentation, evaluation of early prototypes and design verification testing.



Cyber Range: Test and evaluation

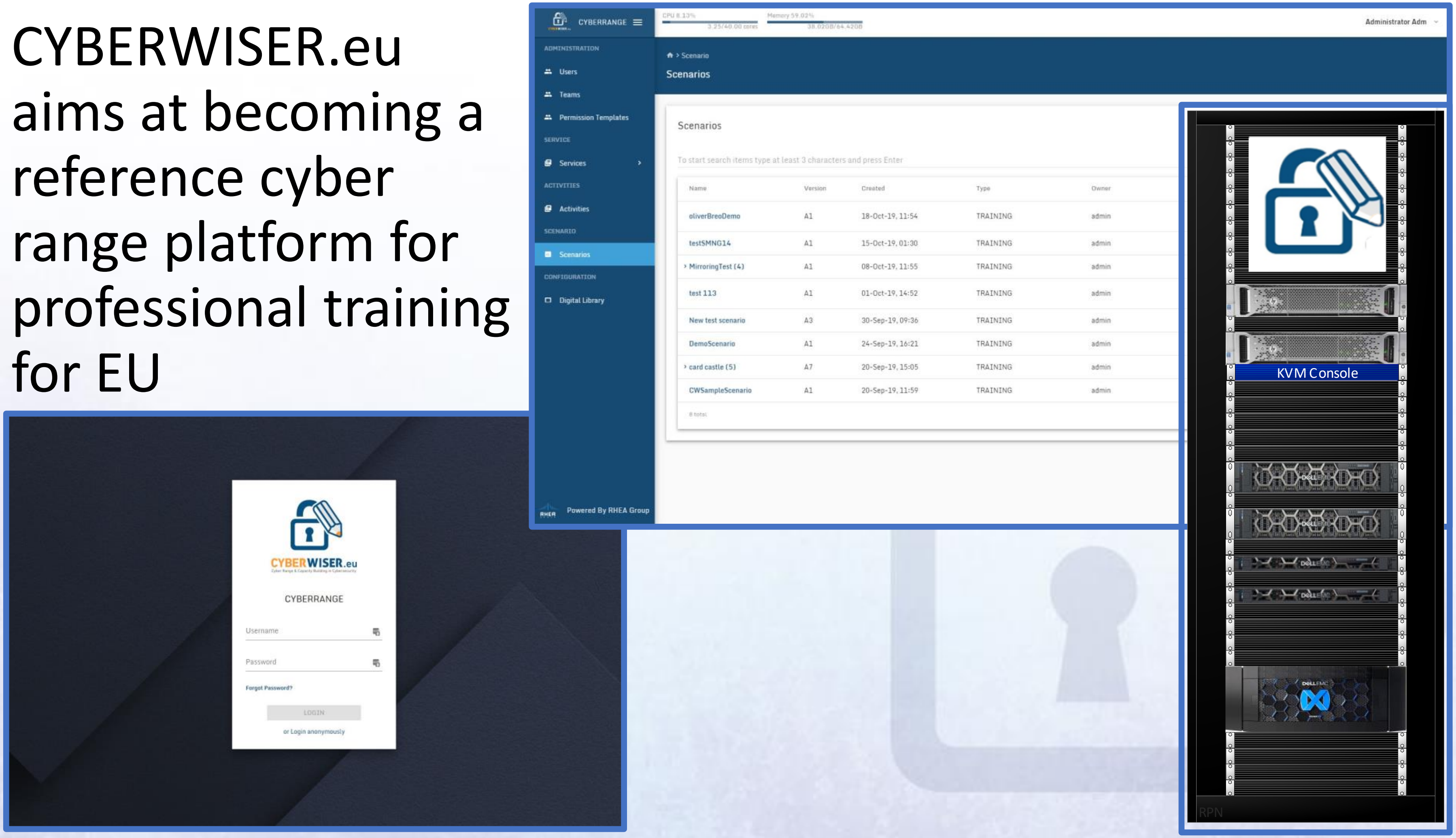
Anticipating cyber threats with a realistic test framework

- Cyber ranges provide frameworks where experts can analyse and examine cyber attack technologies under realistic conditions

- Critical systems can be tested securely in a realistic test framework that facilitates incident management and response

CYBERWISER.eu: a next generation cyber range

CYBERWISER.eu aims at becoming a reference cyber range platform for professional training for EU



Scenarios

To start search items type at least 3 characters and press Enter

Name	Version	Created	Type	Owner
oliverBreoDemo	A1	18-Oct-19, 11:54	TRAINING	admin
testSMNG14	A1	15-Oct-19, 01:30	TRAINING	admin
› MirroringTest (4)	A1	08-Oct-19, 11:55	TRAINING	admin
test 113	A1	01-Oct-19, 14:52	TRAINING	admin
New test scenario	A3	30-Sep-19, 09:36	TRAINING	admin
DemoScenario	A1	24-Sep-19, 16:21	TRAINING	admin
› card castle (5)	A7	20-Sep-19, 15:05	TRAINING	admin
CWSampleScenario	A1	20-Sep-19, 11:59	TRAINING	admin

8 total

CYBERWISER.eu
Cyber Range & Capacity Building in Cybersecurity

CYBERRANGE

Username

Password

Forgot Password?

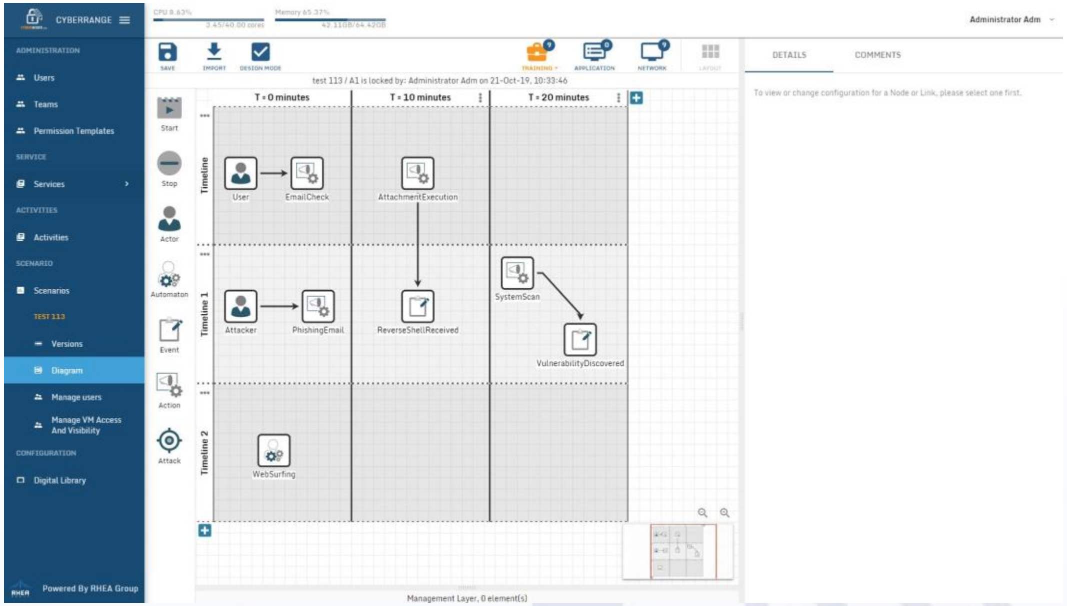
LOGIN

or Login anonymously

CYBERWISER.eu: a next generation cyber range

The platform already leverages advanced features of next generation cyber ranges:

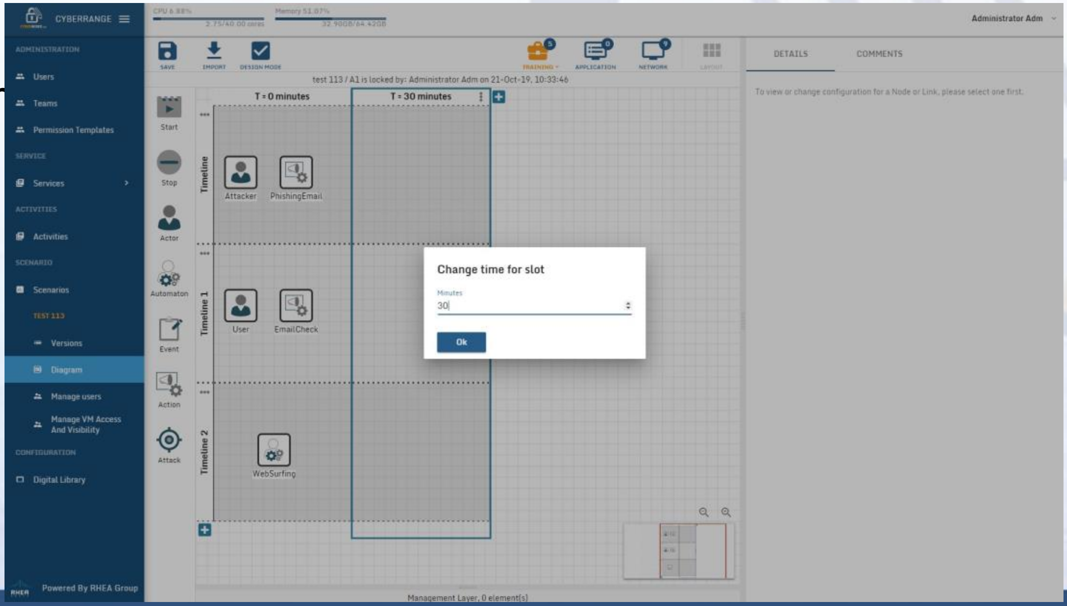
- Detailed scenario design for very complex network and application topologies
- Wide digital library for scenario variety
- Virtual networks and routing semi-automatic configuration
- Events scheduling during scenario design
- Events triggering during scenario execution
- Full suite of cross learning tools



test 113 / A1 is locked by: Administrator Adm on 21-Oct-19, 10:33:46

To view or change configuration for a Node or Link, please select one first.

Management Layer, 0 element(s)



test 113 / A1 is locked by: Administrator Adm on 21-Oct-19, 10:33:46

To view or change configuration for a Node or Link, please select one first.

Change time for slot

Minutes: 30

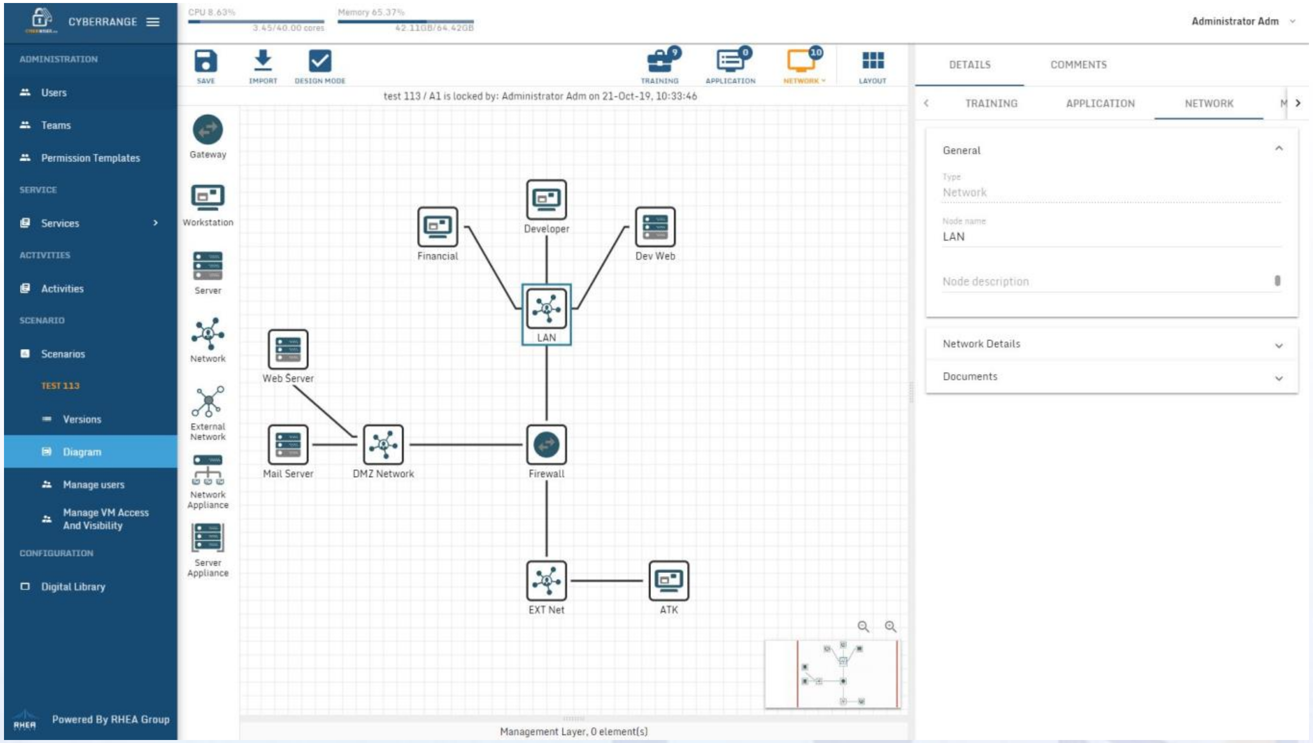
Ok

Management Layer, 0 element(s)

CYBERWISER.eu: a next generation cyber range

The platform will leverage additional advanced features of next generation cyber ranges:

- Real-time overview of events in active scenarios
- Automatic performance evaluation of trainees
- Full suite of attacking and protective tools for complex scenario



test 113 / A1 is locked by: Administrator Adm on 21-Oct-19, 10:33:46

Type: Network

Node name: LAN

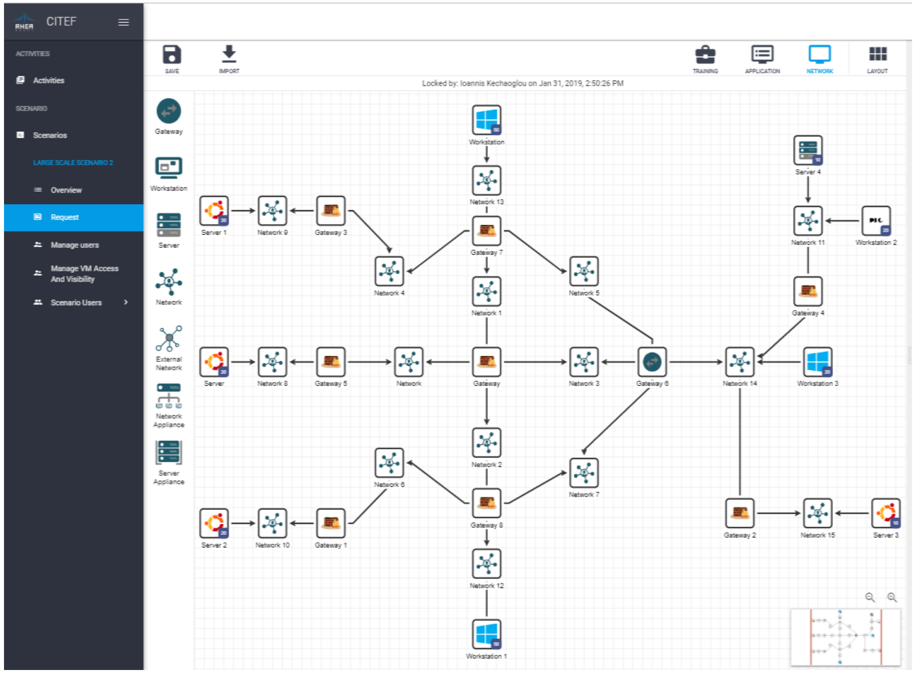
Node description

Management Layer, 0 element(s)

CYBERWISER.eu: based on existing advanced technologies

The core of CYBERWISER.eu is based on the Cyber Security, Test and Evaluation Framework (CITEF) platform

- Developed by RHEA Group in the context of the first Cyber Security Centre of Excellence for the European Space Agency
- A complete platform, CITEF allows CYBERWISER.eu to be already deployed on a preliminary version, leveraging on a set of consolidated features including
  - Detailed scenario design
  - Wide digital library for scenario variety
  - Virtual networks and routing semi-automatic configuration
  - Advanced flexibility on instantiation/deletion/update of complex scenario



CITEF

ACTIVITIES

Activities

SCENARIO

Scenarios

LARGE SCALE SCENARIO 2

Overview

Request

Manage users

Manage VM Access And Visibility

Scenario Users

Locked by: Ioannis Kechaoglou on Jan 31, 2019, 2:50:26 PM

CYBERWISER.eu: based on existing advanced technologies

- The advanced training scenario features are based on existing tools to be improved during the project:
    - Monitoring Sensors (ATOS)
    - XL-SIEM (ATOS) – anomaly detection
    - Risk Assessment Engine (ATOS) – based on economic models from SINTEF
    - Decision Support System (ATOS)
    - xOpera (XLAB) – to support alternative IaaS
    - xRuntime (XLAB) – full suite of attacking and scanning tools
    - Cross-learning platform (Trust-IT)

Thank you for your attention! *Questions?*

Main contact:

Matteo Merialdo, m.merialdo@rheagroup.com

Organisation:

RHEA Group

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