Cyber-MAR Final and Piraeus Pilot Event

Cyber-MAR Training Program

Monica Canepa, World Maritime University

16th December 2022

CONTENTS

- CHALLENGES IN MARITIME CYBER SECURITY TRAINING
- CYBER-MAR TRAINING OVERVIEW FINAL RESULTS

- Lack of cybersecurity educators
- Low interaction with the industry
- Little understanding of the labour market
- Outdated or unrealistic platforms in education environments
- Difficulties in keeping pace with the outside world

Training as a Cyber Risk Management Approach

• **Cyber awareness training** offers a cost-effective and meaningful cyber risk management approach (reduce system vulnerabilities and the potential loss)

• Lack of cybersecurity educators, low interaction with the industry, little understanding of the labour market, outdated or unrealistic platforms in education environments, and difficulties in keeping pace with the outside world

Making the implementation of quality cyber security training challenging

- *ISO31000:2009*
- *ISO/IEC27001:2013*
- *- IMO Resolution MSC.428*

There are many compelling reasons why cyber training should be implemented as a risk management practice:

1. Attacks are on the rise as more employees are working from home

2. Humans are a considered a weakness in an organization's cybersecurity

3. Compliance requirements for businesses and operations are increasingly focused on employee training

4. Providing basic training once is not enough to educate employees

5. Anyone can become the victim of a phishing attack

The IMO recommends companies use the *NIST Cybersecurity Framework*

Training as a Cyber Risk Management Approach: Cyber-MAR training

Studies show that the use of multiple methods of training produced the highest correlation to perceived security effectiveness in employees

The Cyber-MAR project aims to develop an “innovative cybersecurity simulation environment for accommodating the peculiarities of the maritime sector”

Training as a Cyber Risk Management Approach: Cyber-MAR training

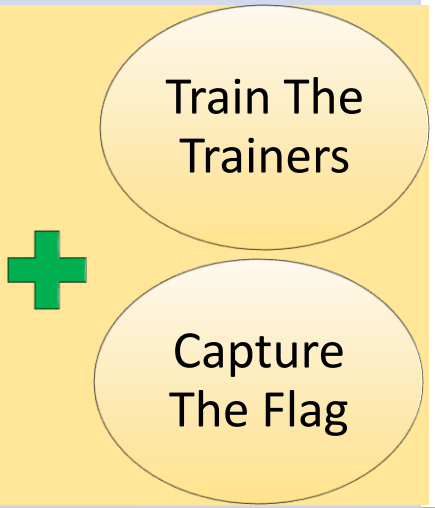
Awareness, Training, Synergies

- Familiarisation & Training with Cyber range platform
- Formulation of Cyber-MAR training packages with a focus on hands-on and practical training
- Exploring new Awareness Methods & Qualification Tracks
- Training activities / synergies with EU Agencies and other cyber-security EU projects

Implemented actions: Planned trainings

Entry Level

- EL01
  Cybersecurity Awareness
- EL02
  Managing Cybersecurity



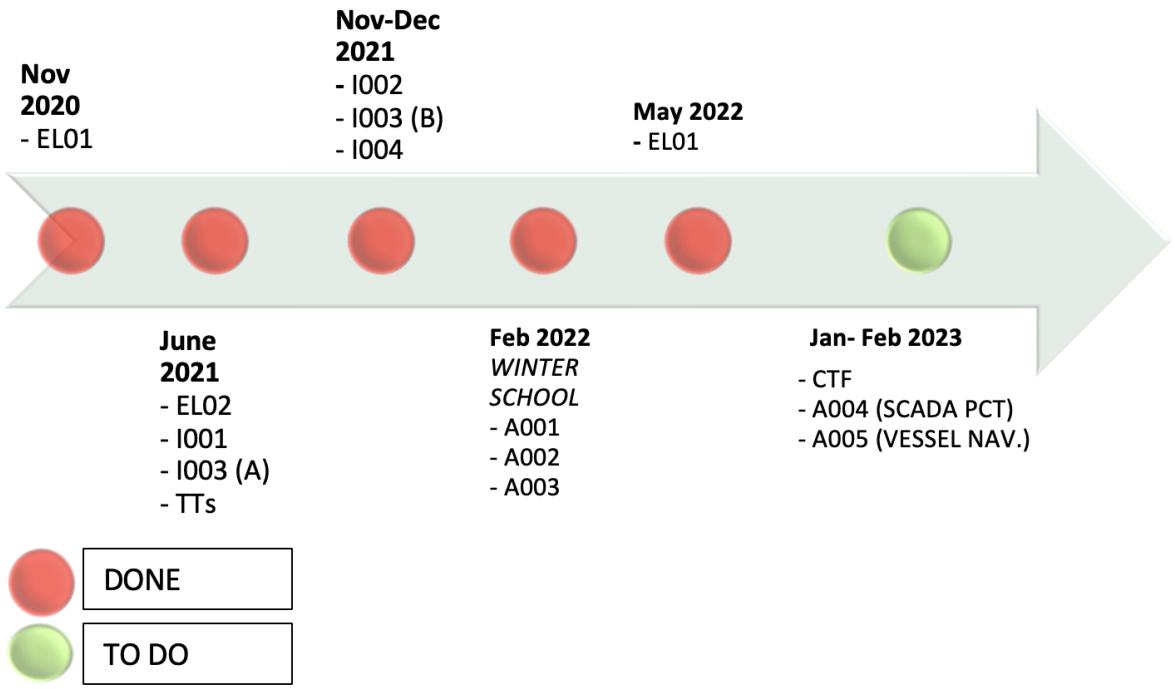
Intermediate Level

- I001
  Introduction to the Cyber Range
- I002
  Basic Tools for a Cyber Range
- I003
  Using a Cyber Range to Understand risk
- I004
  Lesson learned from Cyber MAR pilots: Cyber-attack scenario on the Valencia port authority's electrical grid

Advanced Level

- A001
  HNS Pro user training
- A002
  Crafting an Attack (Theory)
- A003
  Crafting an Attack (Practical)
- A004
  Lesson learned from Cyber-MAR pilots: SCADA system in Port Container terminal
- A005
  Lesson learned from Cyber-MAR pilots: Vessel navigation and automation systems

TRAINING IMPLEMENTED ACTIONS



DONE TO DO

EL01 - Cybersecurity Awareness
EL02 - Managing Cybersecurity

_____

I001 - Introduction to the Cyber Range
I002 - Basic Tools for a Cyber Range
I003 - Using a Cyber Range to Understand risk
I004 - Lesson learned from Cyber MAR pilots: Cyber- attack scenario on the Valencia port authority's electrical grid

_____

A001 -HNS Pro user training
A002 - Crafting an Attack (Theory)
A003 - Crafting an Attack (Practical)
A004 - Lesson learned from Cyber-MAR pilots: SCADA system in Port Container terminal
A005 - Lesson learned from Cyber-MAR pilots: Vessel navigation and automation systems

TRAIN THE TRAINERS
CTF

I002 –I003 – I004 NOVEMBER-DECEMBER 2021

One of the most important factors that influence the solidity of cybersecurity is the awareness of the cyber-threat, for increasing it Cyber-MAR offers training for all professionals (cyber-security/IT experts but also non-IT-expert personnel of ports, shipping operators, and linked entities influenced by possible cascading effects).

A series of online training courses, organized by the Cyber-MAR EU project, will be held between **the 29th of November and 1st of December 2021.**

Find below all the necessary information.

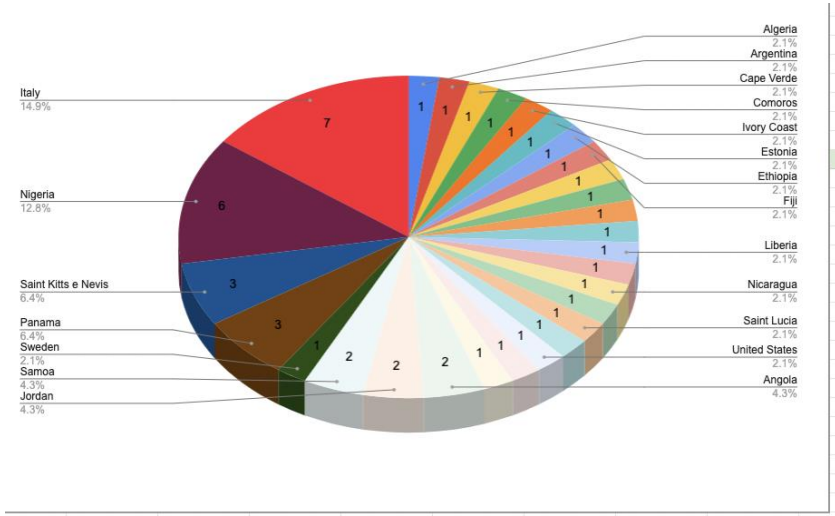
I002 - Basic Tools for a Cyber Range (4 hours)
I003 - Using a Cyber Range to Understand risk (1,5 hours)
I004 - Lesson learned from Cyber MAR pilots:
Cyber- attack scenario on the Valencia port authority's electrical grid (1 hour)

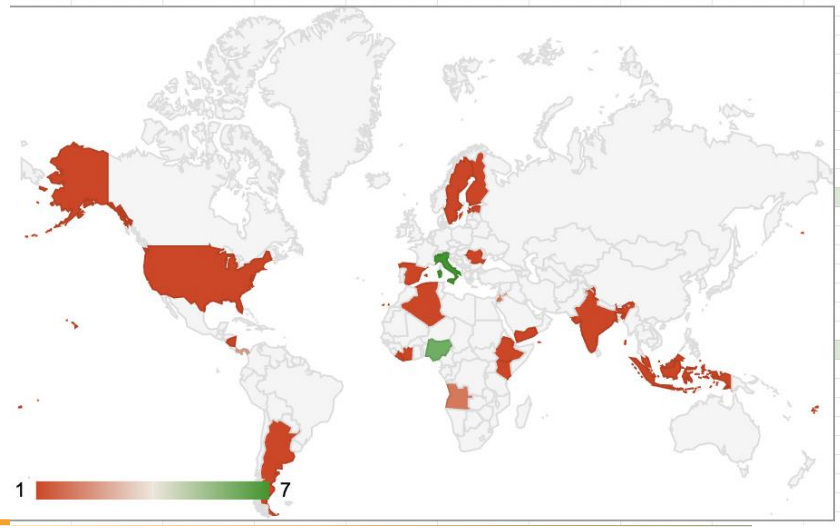
N° Participants

I002 – 47
I003 – 25
I004 – 25

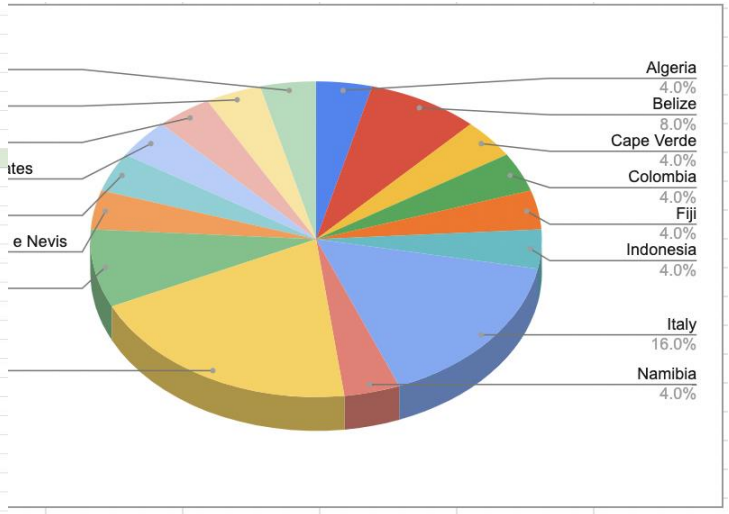
I002 –I003 – I004 NOVEMBER-DECEMBER 2021 – NATIONALITY COMPOSITION

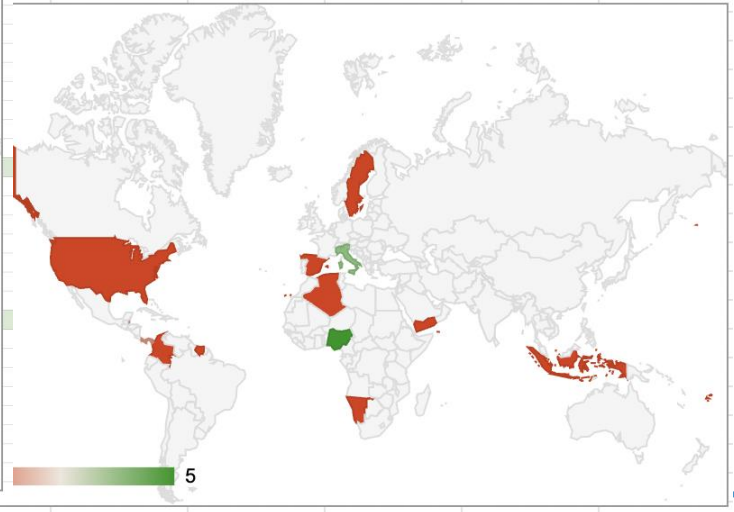
I002



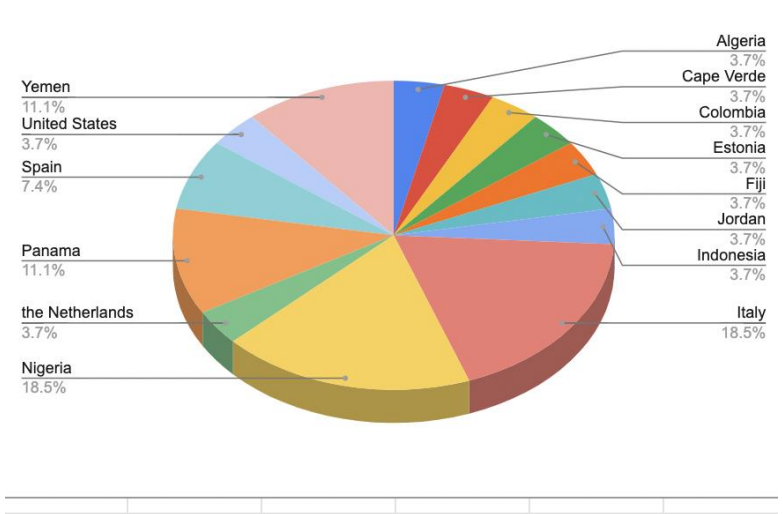


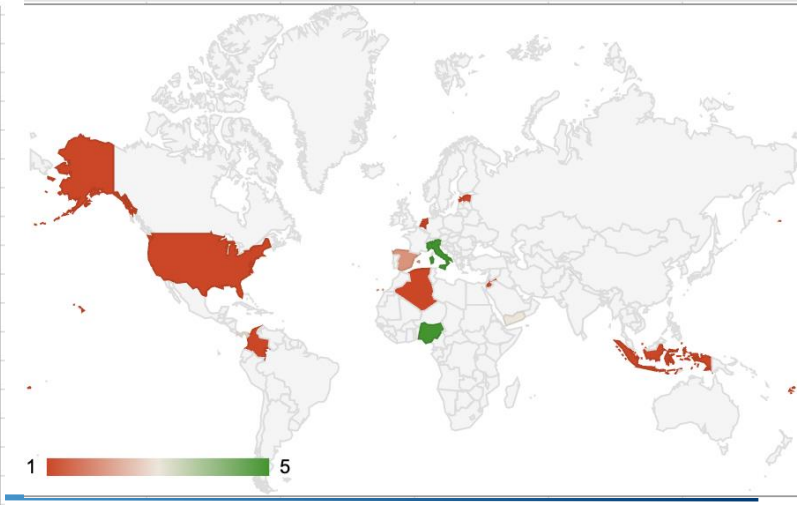
I003





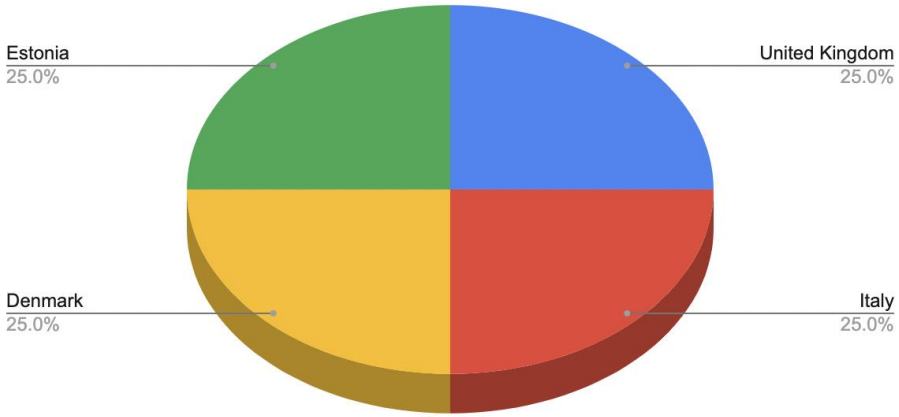
I004



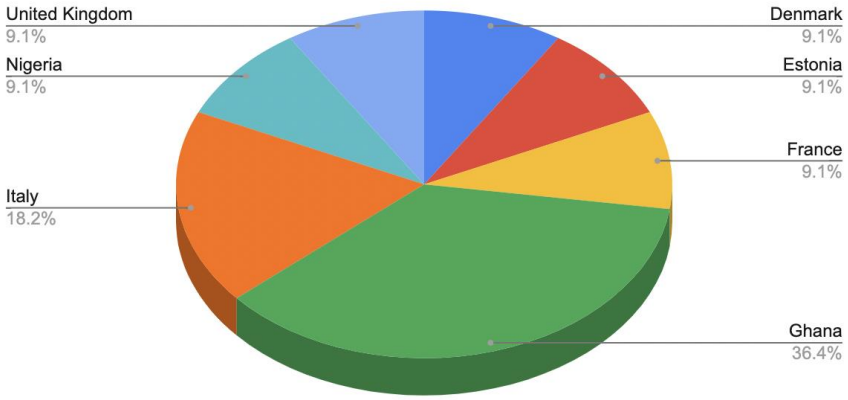


A001 –A002 – A003 FEBRUARY 2022 – NATIONALITY COMPOSITION (WINTER SCHOOL – FORESIGHT PROJECT)

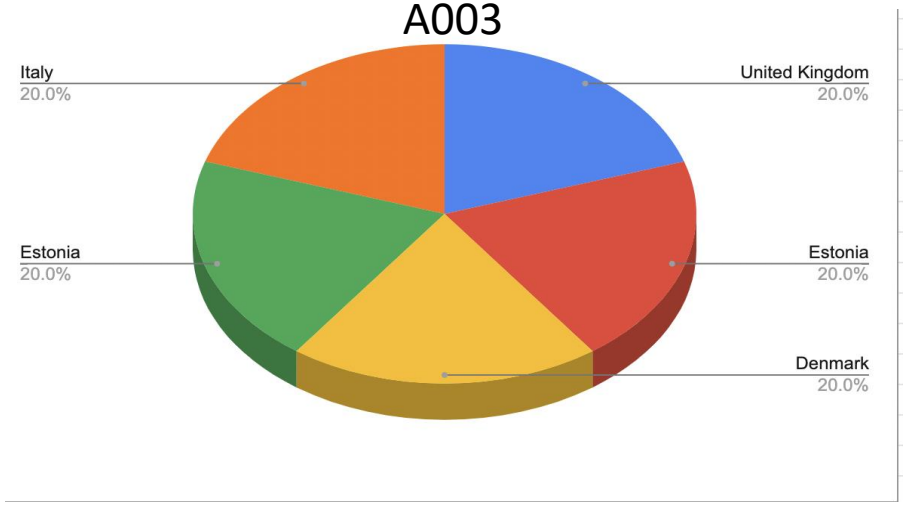
A001



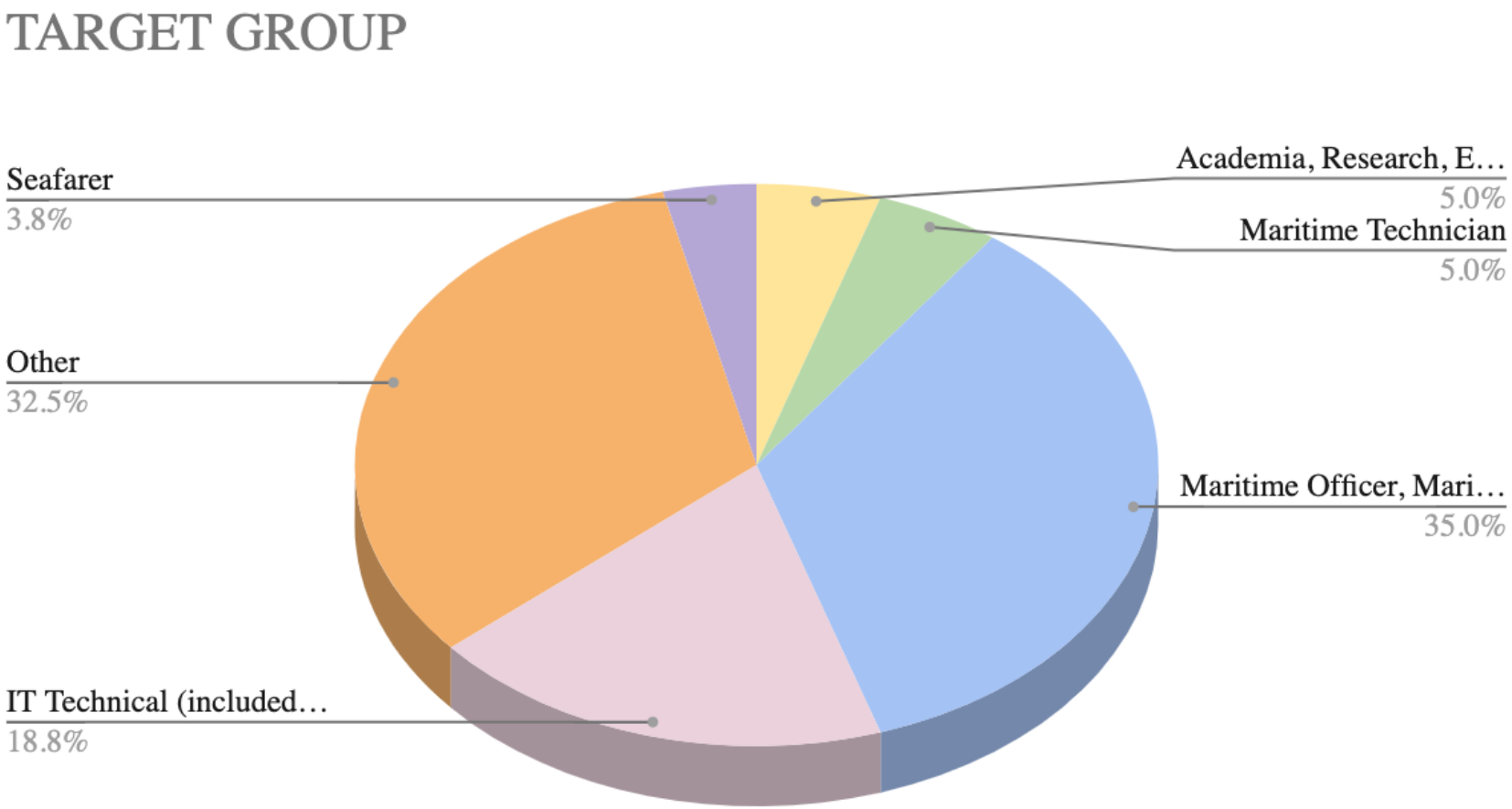
A002



A003

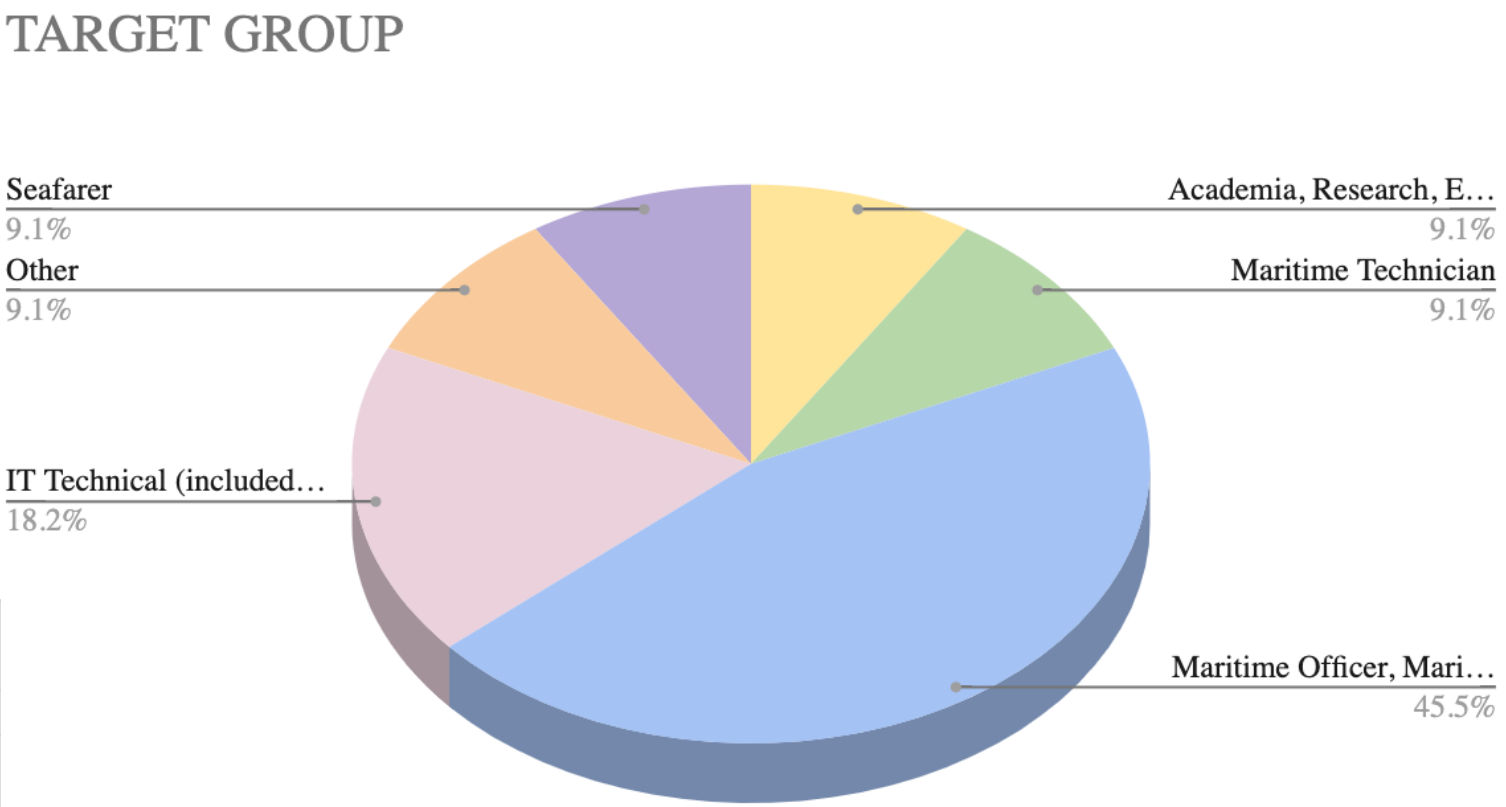


I002 – Attendees composition – Target groups



A/R/E	Academia, Research, Education
MT	Maritime Technician
MO/MM	Maritime Officer, Maritime Management
ITT	IT Technical (included management)
O	Other
S	Seafarer

A002 – Attendees composition – Target groups



A/R/E	Academia, Research, Education
MT	Maritime Technician
MO/MM	Maritime Officer, Maritime Management
ITT	IT Technical (included management)
O	Other
S	Seafarer

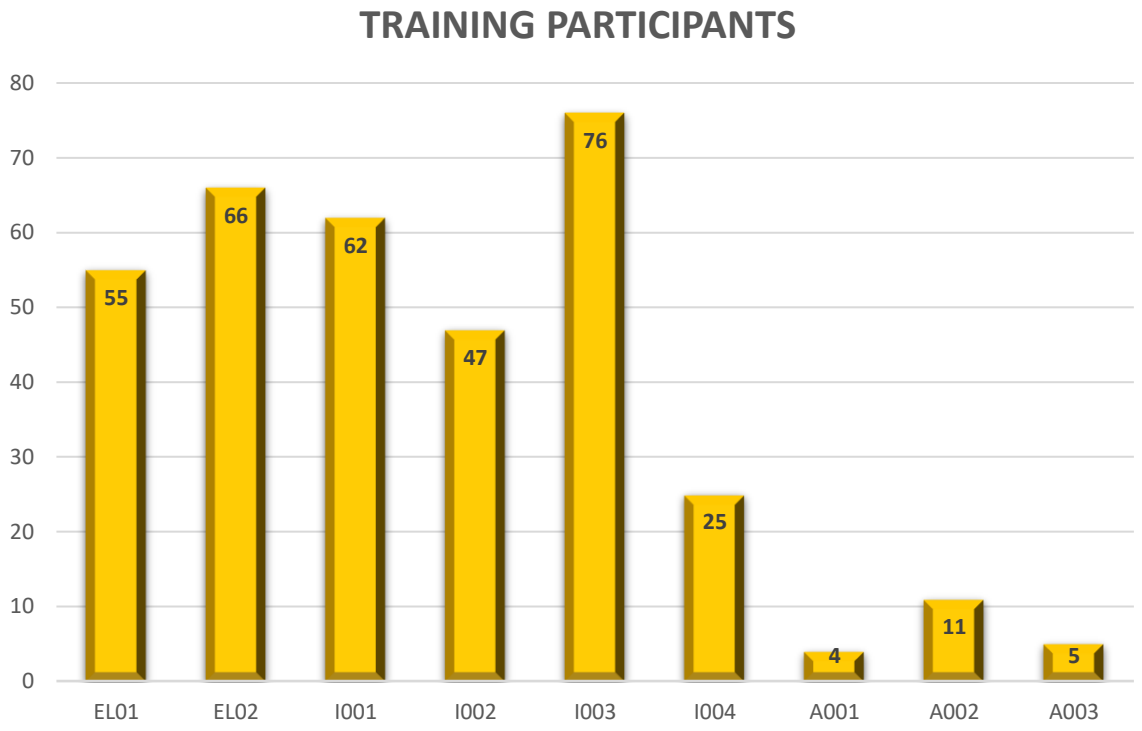
EL01 HYBRID TRAINING – GENOA

DAY 1 (09/05/22)

09.00 – 09.15	**INTRODUCTION**	
	Welcome and Introduction CyberMAR project	ICCS - IMSSEA
	CyberMAR training overview and LMS platform	Fabio Ballini/Monica Canepa (WMU)
09.15 – 13.15	**EL 01 - Introduce core cybersecurity themes and discuss their relevance to the maritime sector**	
09.15 -	Fundamentals of cyber security	Cristiano Cafferata (WMU)
11.30	Attacks issues in depth	Rory Hopcraft/Dr Kimberly Tam (UOP)
12.10	Mitigation and remediation	
PANELIST ROUNDTABLE DISCUSSION (12.50 – 13.15)		

Training WRAP UP

TRAINING	PARTICIPANTS
EL01	55
EL02	66
I001	62
I002	47
I003	76
I004	25
A001	4
A002	11
A003	5
TOTAL TILL DEC 2022	**351**



WEBINAR	PARTICIPANTS
Webinar "Cybersecurity at sea: real-life experiences"	46
Webinar with Foresight “Cyber-Security challenges and future perspectives”	56
TOTAL	**102**

Training WRAP UP – Participants features

- From all over the world

TARGET GROUPS REACHED

Academia, Research, Education
Maritime Technician
Maritime Officer, Maritime Management
IT Technical (included management)
Seafarer
Other

Training WRAP UP

Training effectiveness evaluation form

Q4

Customize Save as

The sessions delivered the information I expected to receive

Answered: 7 Skipped: 3

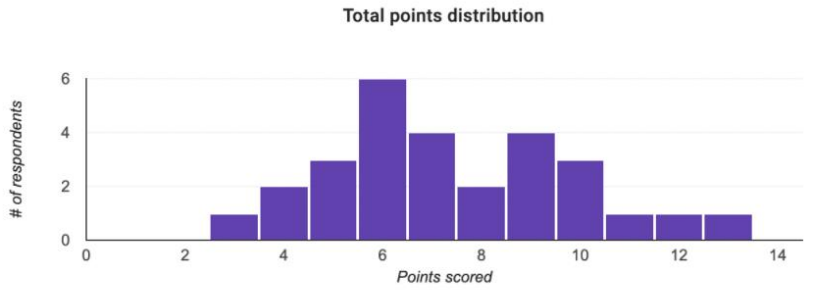
4.1★
average rating

	STRONGLY DISAGREE	DISAGREE	NEUTRAL	AGREE	STRONGLY AGREE	TOTAL	WEIGHTED AVERAGE
☆	0.00% 0	0.00% 0	14.29% 1	57.14% 4	28.57% 2	7	4.14

Evaluation Test (Pre and Post training)

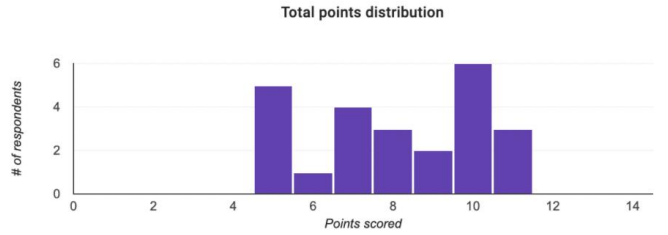
Pre-I002 Basic Tools for a Cyber Range (28 responses)

Average	Median	Range
7.43 / 14 points	7 / 14 points	3 - 13 points



Post-I002 Basic Tools for a Cyber Range (24 responses)

Average	Median	Range
8.08 / 14 points	8 / 14 points	5 - 11 points



CYBER-MAR LMS

- WMU installed a dedicated instance of Moodle LMS to host the trainings and we are actually configuring the LMS and uploading the training materials

- Diateam developed the software component allowing the connection between the cyber range and the Moodle LMS

Cyber-MAR moodle

test user

Entry level cyber preparedness training

Dashboard / My courses / Entry level cyber preparedness training

Course summary

An introductory course on cyber security with a special focus on maritime cyber security issues.

From the very basics of the attack&defence art in the cyber realm to the cyber risk management, the learner is introduced to

Video lessons (November 2020)

To do: View

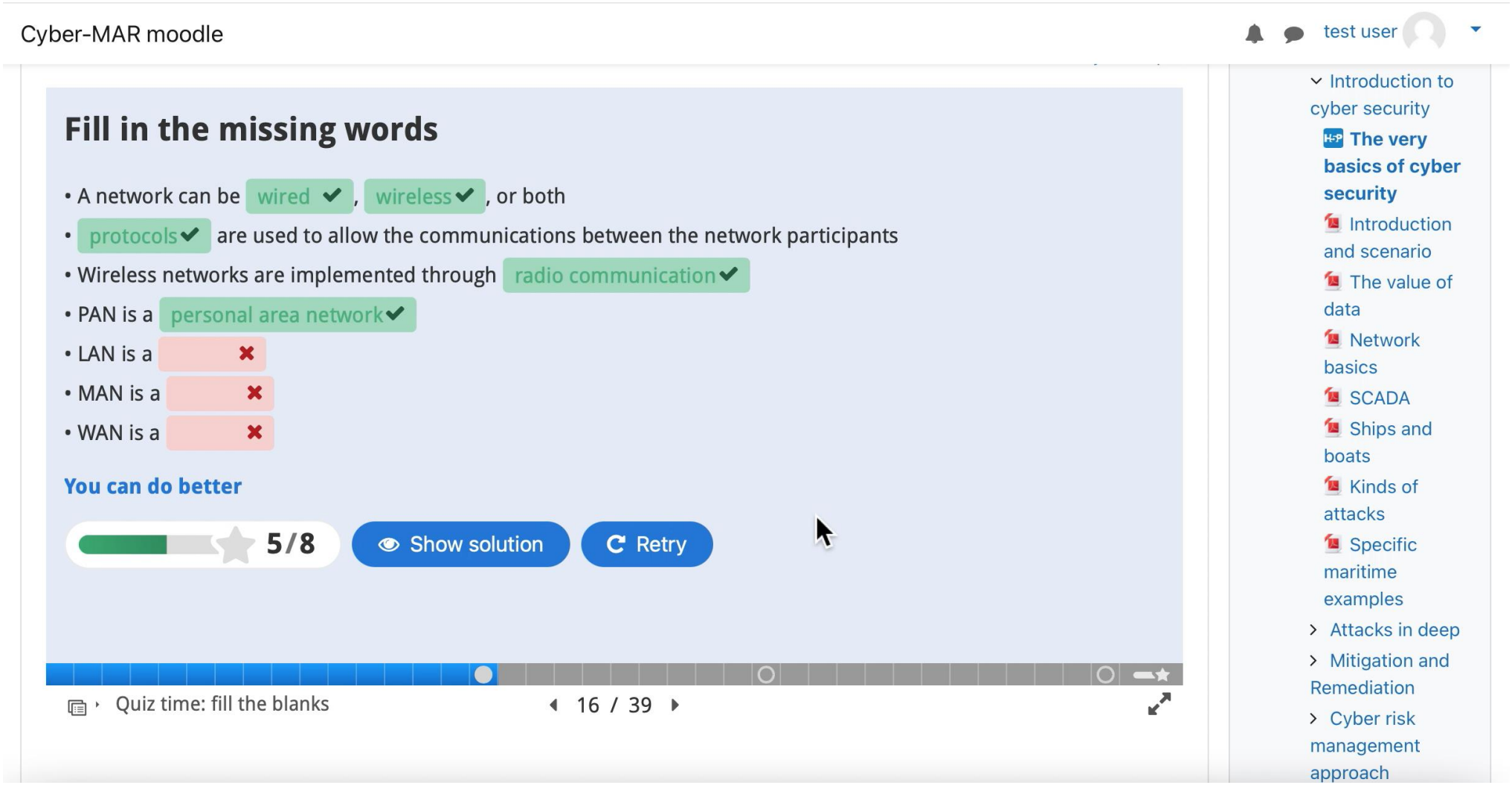
Video of the first part of the lesson held November, 2020 and covering the chapters:

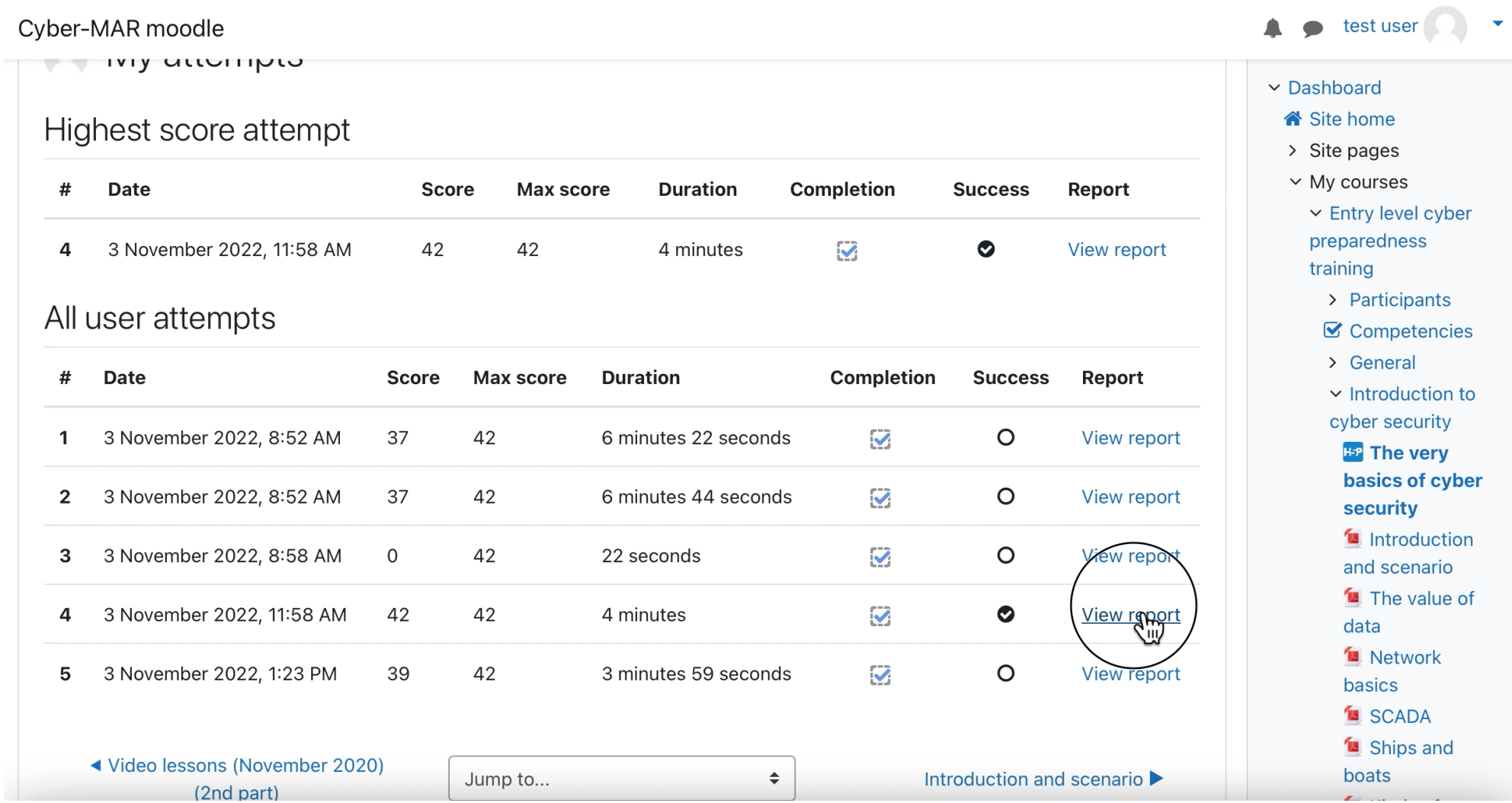
- Introduction to cyber security
- Attack in deep

Navigation

- Dashboard
  - Site home
  - Site pages
  - My courses
    - **Entry level cyber preparedness training**
      - Participants
      - Competencies
      - General
      - Introduction to cyber security
      - Attacks in deep
      - Mitigation and Remediation

CYBER-MAR LMS




Cyber-MAR moodle
test user
Highest score attempt
Date Score Max score Duration Completion Success Report
4 3 November 2022, 11:58 AM 42 42 4 minutes View report
All user attempts
Date Score Max score Duration Completion Success Report
1 3 November 2022, 8:52 AM 37 42 6 minutes 22 seconds View report
2 3 November 2022, 8:52 AM 37 42 6 minutes 44 seconds View report
3 3 November 2022, 8:58 AM 0 42 22 seconds View report
4 3 November 2022, 11:58 AM 42 42 4 minutes View report
5 3 November 2022, 1:23 PM 39 42 3 minutes 59 seconds View report
◀ Video lessons (November 2020) (2nd part)
Jump to...
Introduction and scenario ▶
Dashboard
Site home
Site pages
My courses
Entry level cyber preparedness training
Participants
Competencies
General
Introduction to cyber security
The very basics of cyber security
Introduction and scenario
The value of data
Network basics
SCADA
Ships and boats

www.Cyber-MAR.eu

Cyber_MAR

Cyber-MAR EU Project

Cyber-MAR

info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION

Monica Canepa

moc@wmu.se

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389