Vessel Pilot Event

Training & Awareness Raising

Monica Canepa & Yvette Agostini, World Maritime University

5th May 2022

CONTENTS

- FOCUS & OUTPUTS
- IMPLEMENTED ACTIONS
- ONGOING ACTIVITIES
- NEXT STEPS

FOCUS: 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

FINAL EXPECTED OUTPUT

At least 2 physical training per experience level (3 levels) **with 50 unique trainees**

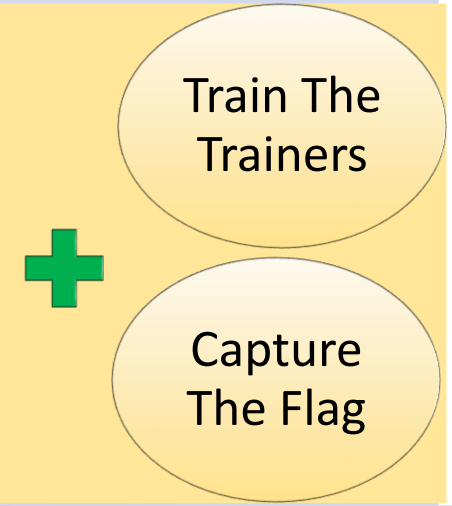
At least 2 Massive Open Online Courses (MOOCs) training per experience level (3 levels)

2 Capture The Flag

IMPLEMENTED ACTIONS: PLANNED TRAININGS

Entry Level

- EL01
  Cybersecurity Awareness
- EL02
  Managing Cybersecurity



Train The Trainers

+

Capture The Flag

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

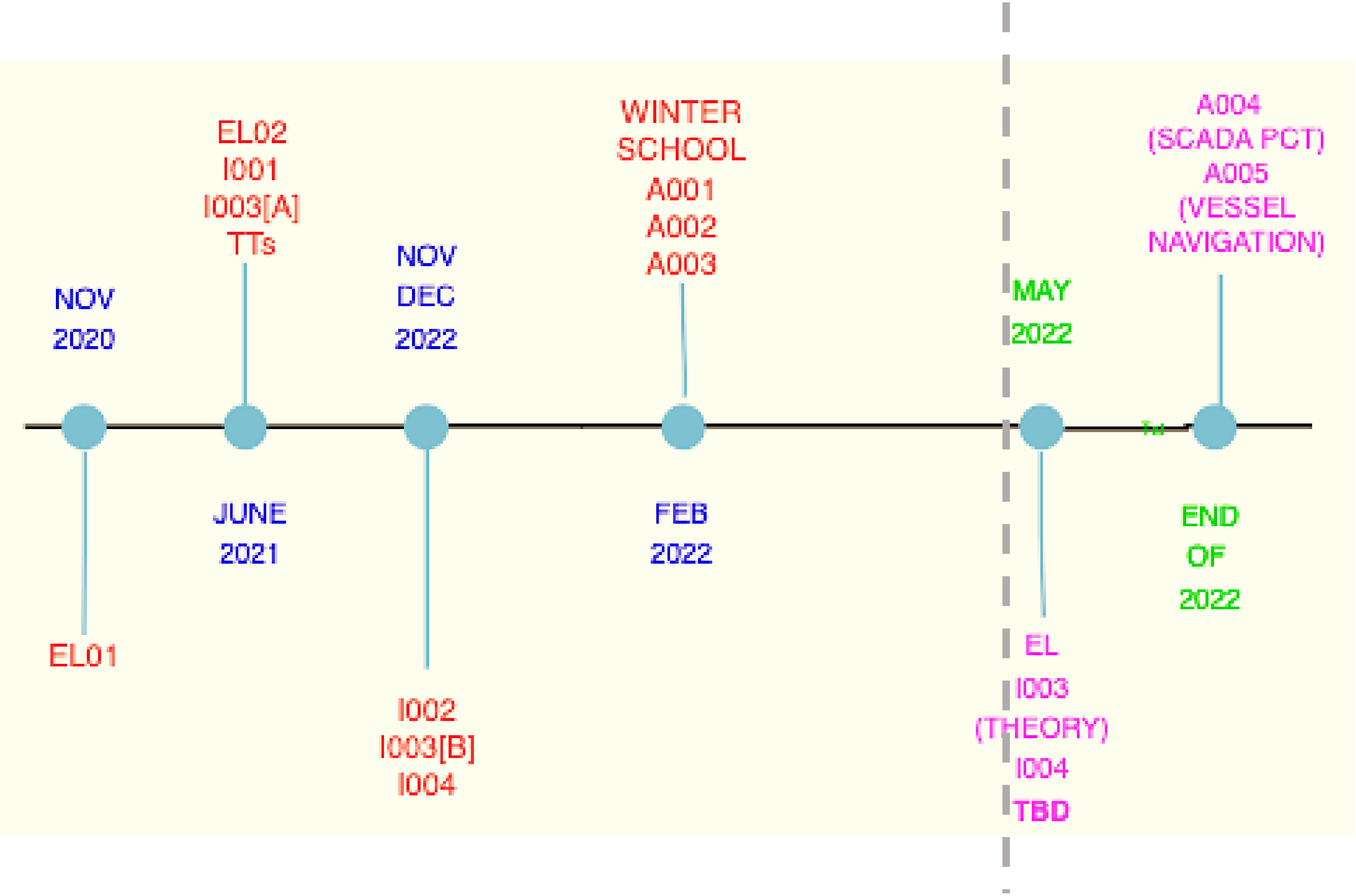
Advanced Level

- 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

IMPLEMENTED ACTIONS: TRAINING 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

IMPLEMENTED ACTIONS: TRAINING CALENDAR



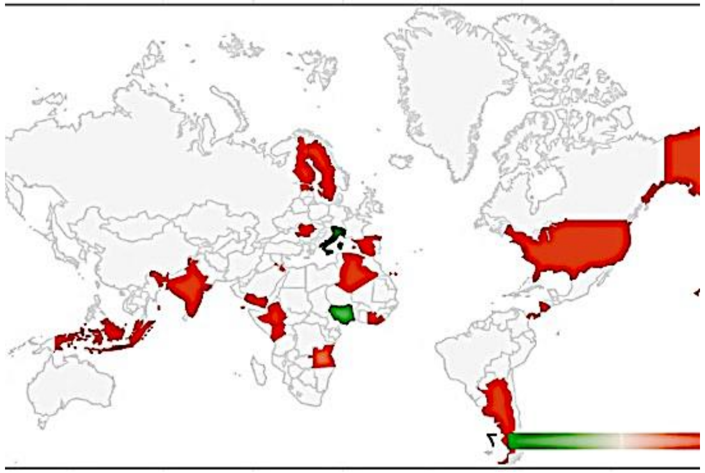
EL01 - Cybersecurity Awareness
EL02 - Managing Cybersecurity

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

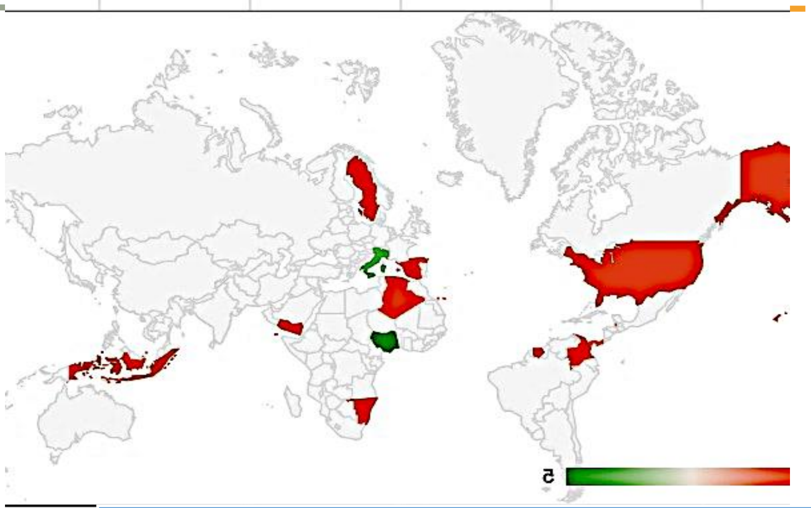
I002 –I003 – I004 NOVEMBER-DECEMBER 2021



I002

Basic tools for a Cyber Range [4h]

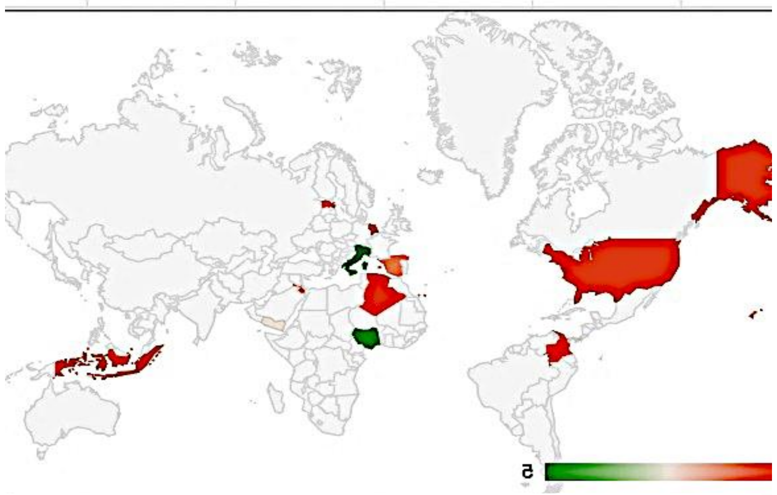
47 participants



I003

- Using a Cyber Range to Understand risk [1,5h]

25 participants

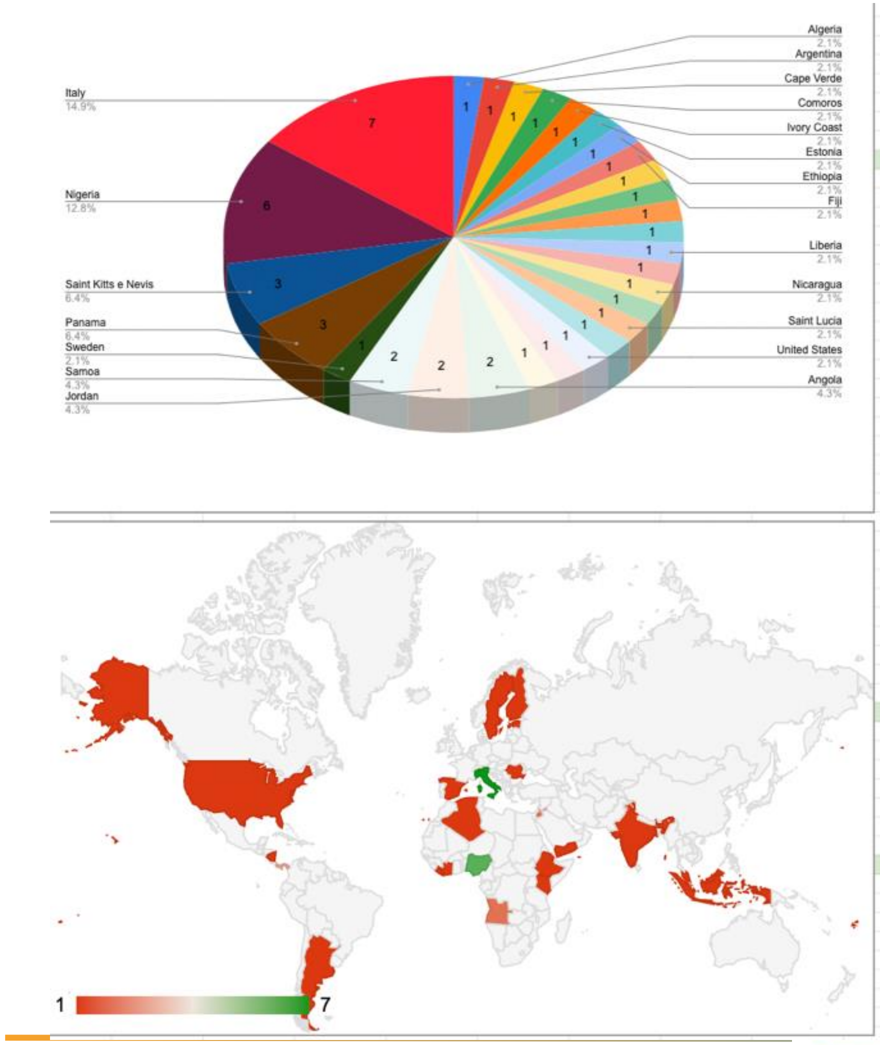


I004

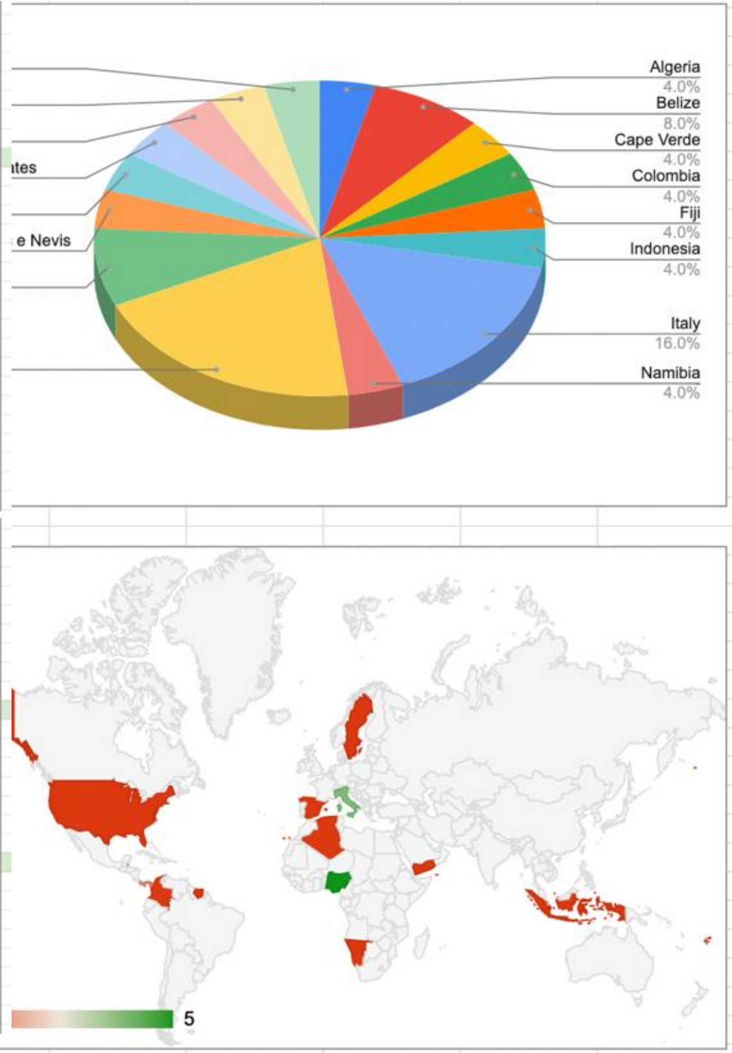
- Lesson learned from Cyber MAR pilots: Cyber- attack scenario on the Valencia port authority’s electrical grid [1h]
- 25 participants

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

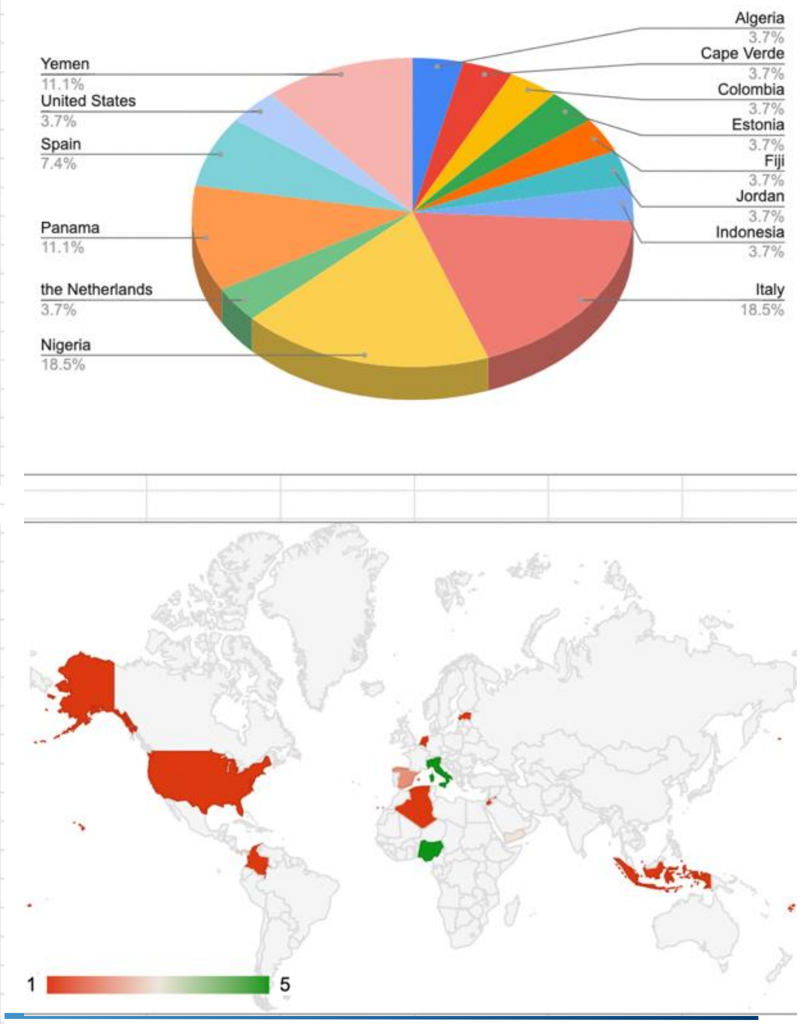
I002



I003

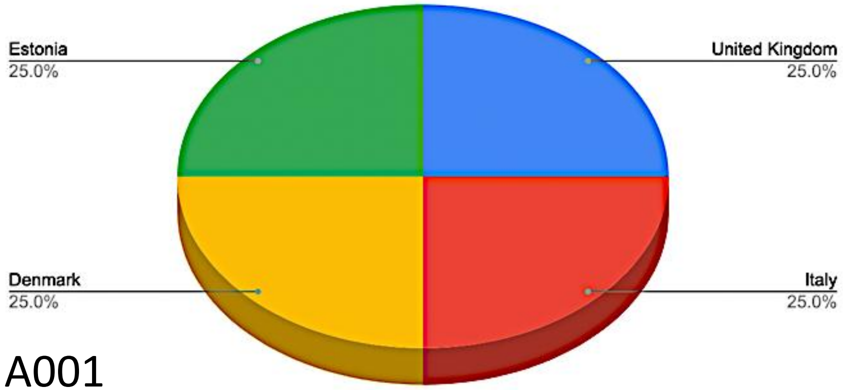


I004

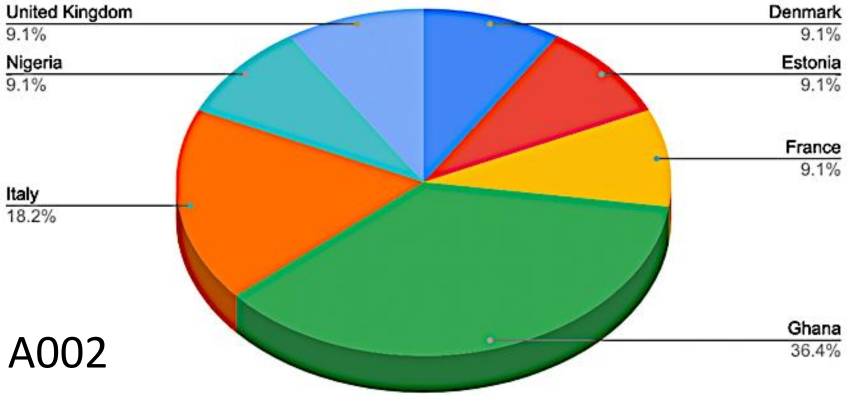


IMPLEMENTED ACTIONS

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



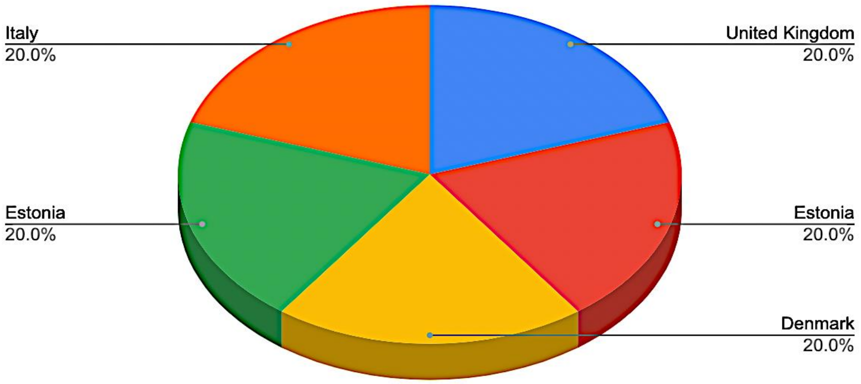
A001



A002

- A001 - HNS Pro user training (4 hours)
- A002 -Introduction to computer and network forensics (2,5 hours)
- A003 –Unlock the capacities of a Cyber Range for Network and Computer Forensics (3 hours)

A003



N° Participants

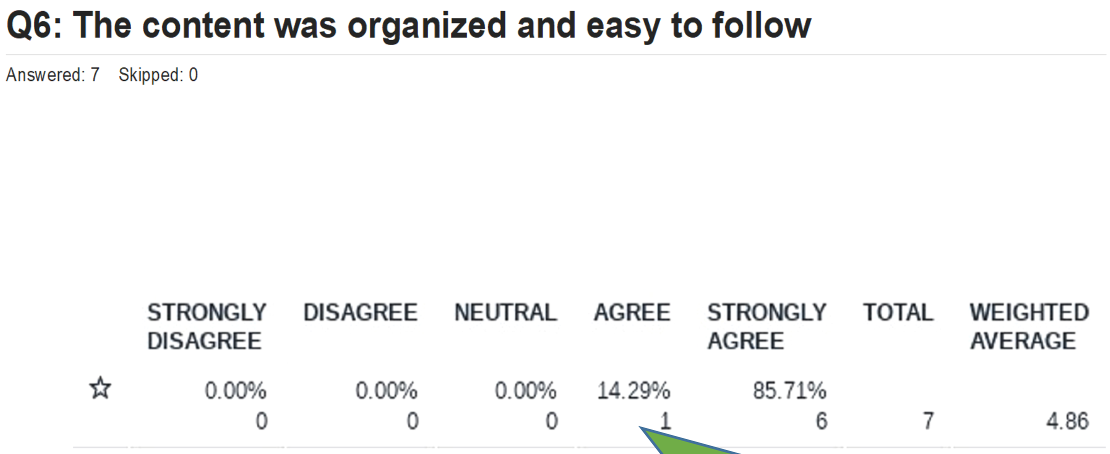
A001 – 04

A002 – 11

A003 – 05

Training effectiveness evaluation form

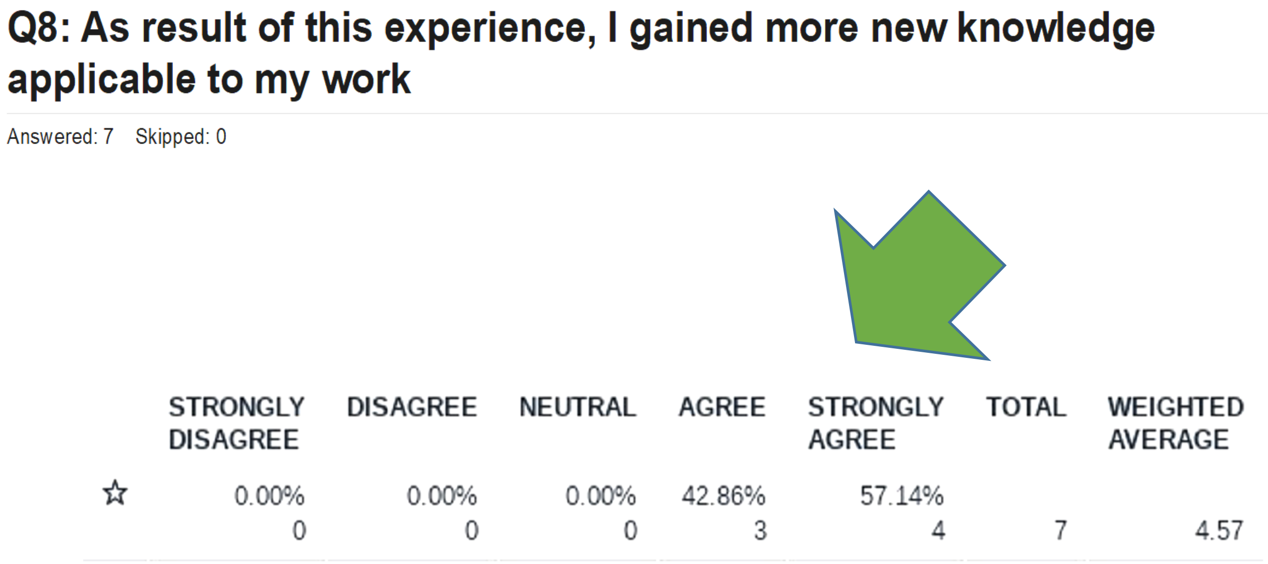
A002



Q6: The content was organized and easy to follow

Answered: 7 Skipped: 0

	STRONGLY DISAGREE	DISAGREE	NEUTRAL	AGREE	STRONGLY AGREE	TOTAL	WEIGHTED AVERAGE
☆	0.00% 0	0.00% 0	0.00% 0	14.29% 1	85.71% 6	7	4.86



Q8: As result of this experience, I gained more new knowledge applicable to my work

Answered: 7 Skipped: 0

	STRONGLY DISAGREE	DISAGREE	NEUTRAL	AGREE	STRONGLY AGREE	TOTAL	WEIGHTED AVERAGE
☆	0.00% 0	0.00% 0	0.00% 0	42.86% 3	57.14% 4	7	4.57

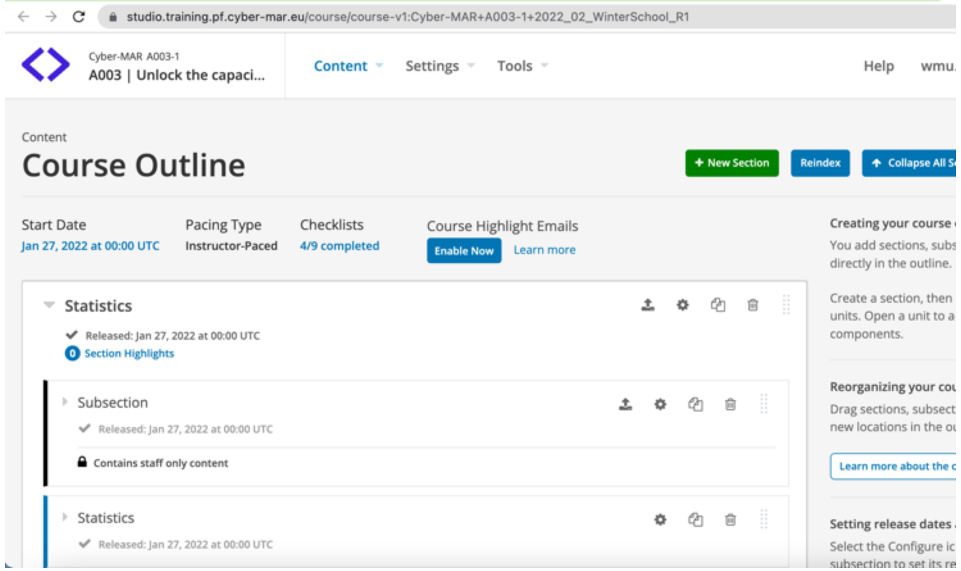
Cyber-MAR LMS platform

Cyber-MAR LMS platfrom has been implemented using openEDX ; integration with MOODLE is on going

DIATEAM

2022 Winter School trainings have been deployed through the LMS

further trainings are added to the LMS platform



studio.training.pf.cyber-mar.eu/course/course-v1:Cyber-MAR+A003-1+2022_02_WinterSchool_R1

Cyber-MAR A003-1
A003 | Unlock the capaci...

Content

Course Outline

Start Date: Jan 27, 2022 at 00:00 UTC
Pacing Type: Instructor-Paced
Checklists: 4/9 completed
Course Highlight Emails: Enable Now · Learn more

Statistics
Released: Jan 27, 2022 at 00:00 UTC
0 Section Highlights

Subsection
Released: Jan 27, 2022 at 00:00 UTC
Contains staff only content

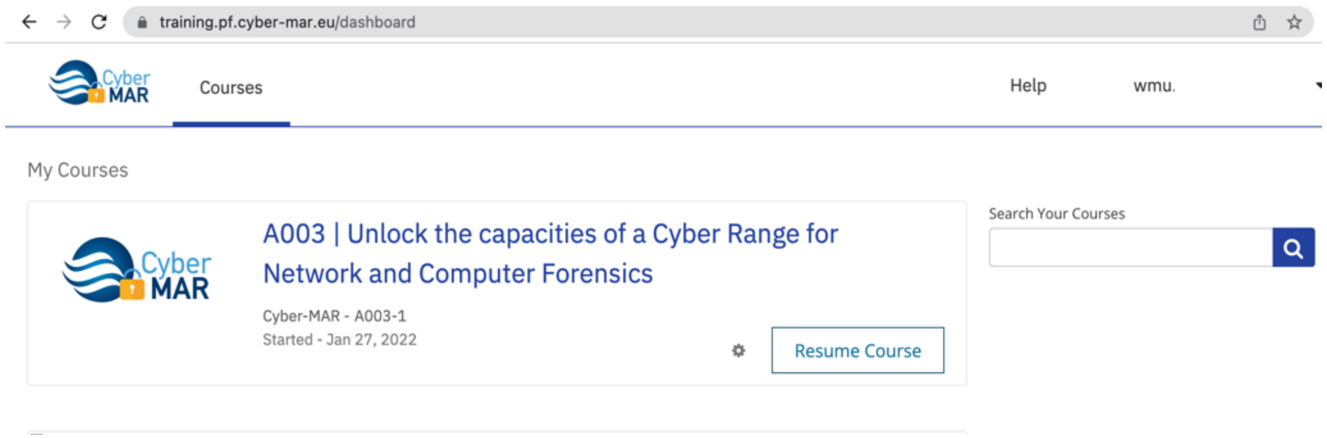
Statistics
Released: Jan 27, 2022 at 00:00 UTC

Creating your course
You add sections, subs directly in the outline.

Create a section, then units. Open a unit to a components.

Reorganizing your cou
Drag sections, subsect new locations in the ou

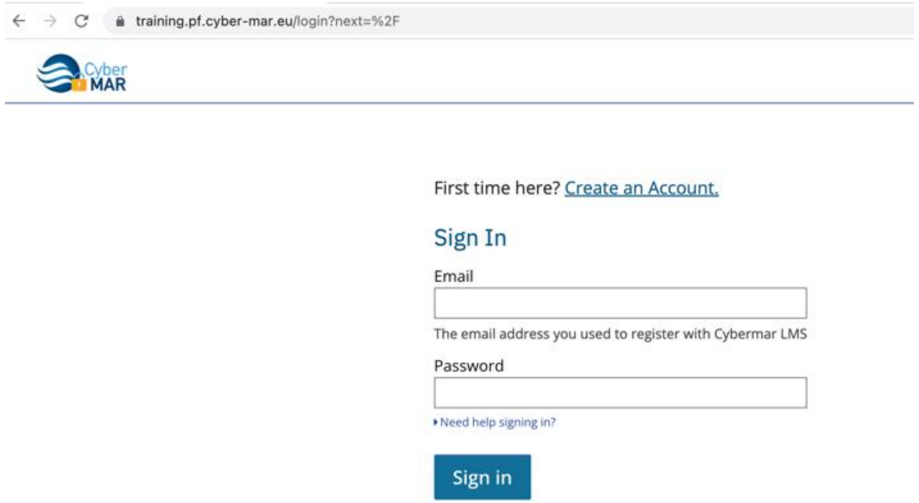
Setting release dates
Select the Configure ic subsection to set its re



training.pf.cyber-mar.eu/dashboard

My Courses

A003 | Unlock the capacities of a Cyber Range for Network and Computer Forensics
Cyber-MAR - A003-1
Started - Jan 27, 2022



training.pf.cyber-mar.eu/login?next=%2F

First time here? Create an Account.

Sign In

Email:
The email address you used to register with Cybermar LMS

Password:

Need help signing in?

IMPLEMENTED ACTIONS
Exploring new Awareness Methods & Qualification

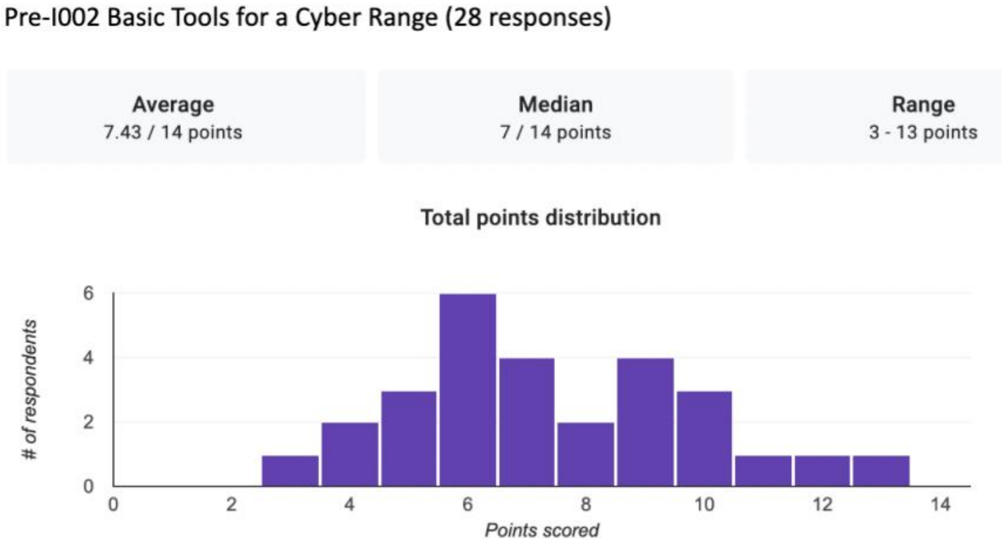
Development of further on novel approaches in awareness methods:

the trainees will be able to understand the threats (past and new) and they take the right steps to prevent them

How are we doing it?

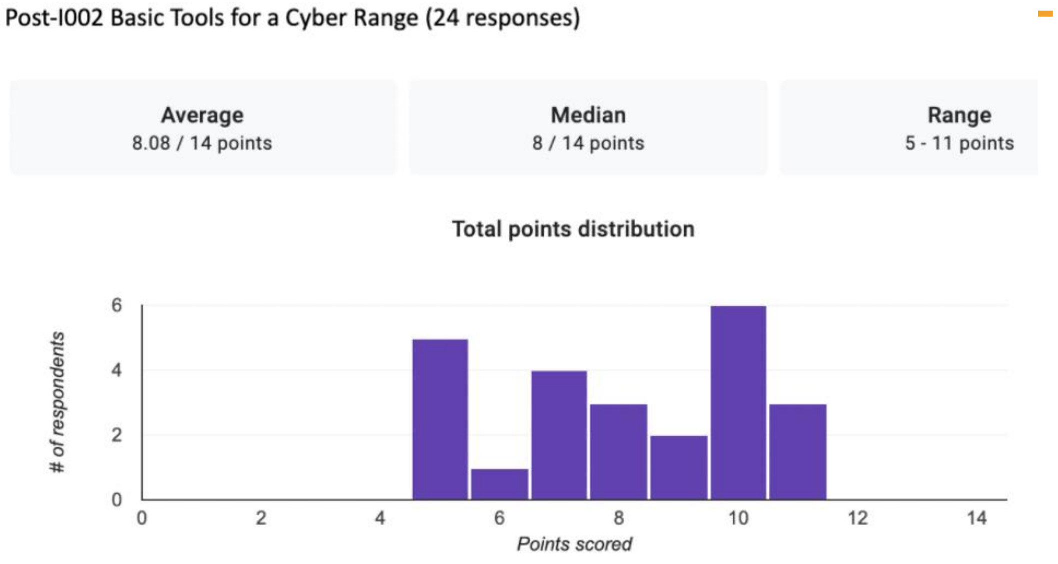
- Having **Cyber-MAR Cyber Range** at the forefront of all relevant activities
    - Cyber-MAR training based on Cyber-MAR cyber range
- Cyber-MAR platform components, which provide a clear vision of the potential impact of a cyber-attack will be presented in order to increase the awareness
- Through an analysis on the current qualification tracks (having as an ultimate goal to identify potential gaps in cybersecurity training)

EVALUATION TEST I002 & I004


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

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

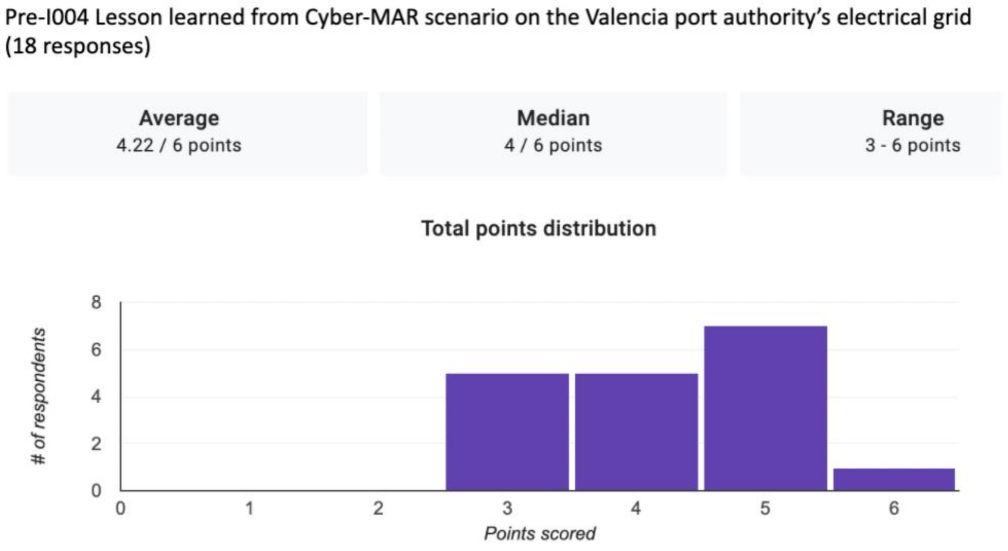
Total points distribution


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

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

Total points distribution

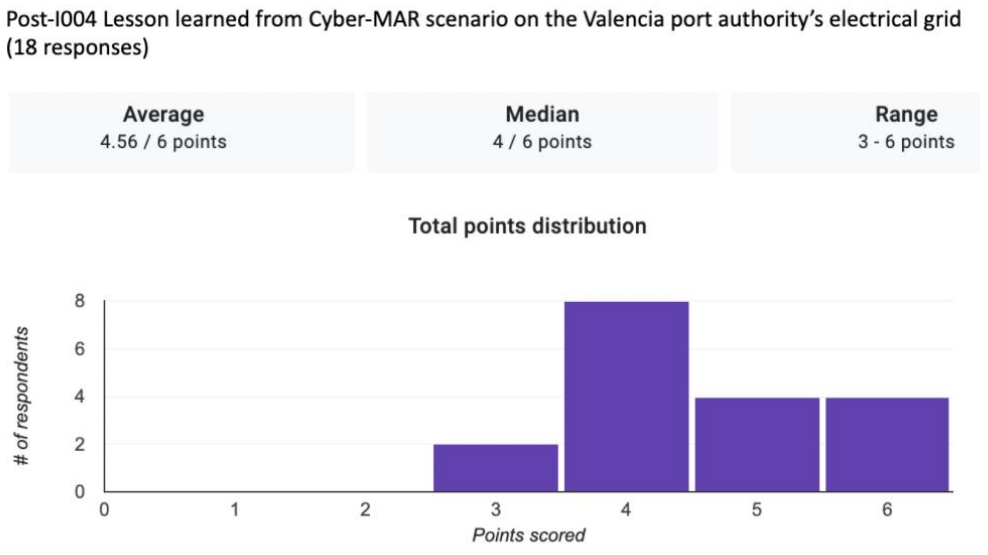
I002


Pre-I004 Lesson learned from Cyber-MAR scenario on the Valencia port authority's electrical grid (18 responses)

Average	Median	Range
4.22 / 6 points	4 / 6 points	3 - 6 points

Total points distribution

I004


Post-I004 Lesson learned from Cyber-MAR scenario on the Valencia port authority's electrical grid (18 responses)

Average	Median	Range
4.56 / 6 points	4 / 6 points	3 - 6 points

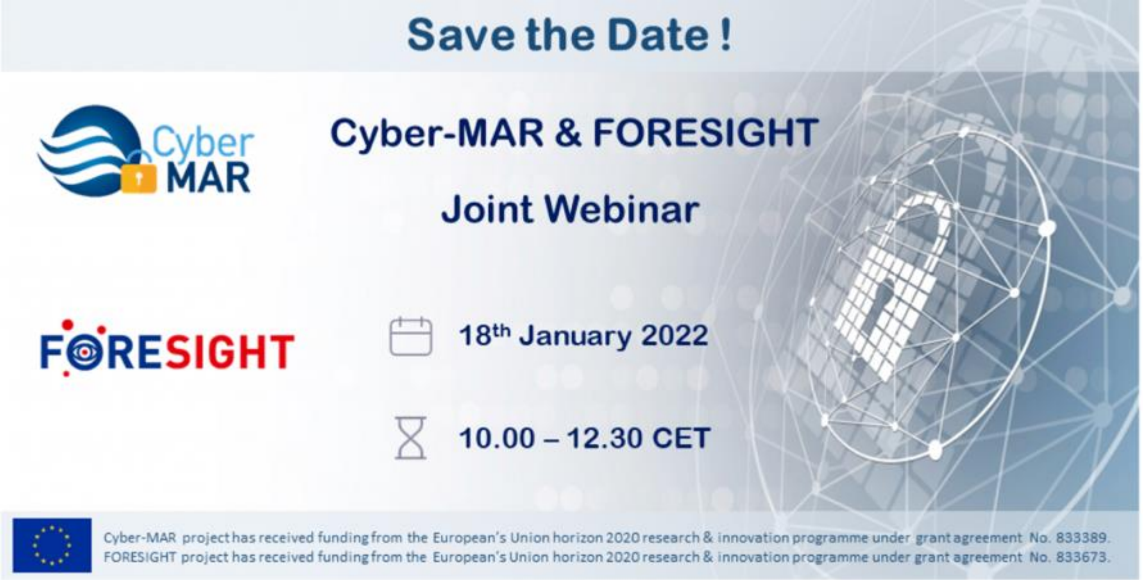
Total points distribution

Training activities / synergies with EU Agencies and other cyber-security EU projects

Mapping on existing Eu Project (linked to Task 7.4 Cyber-MAR Liason with other projects…)

Invitation relevant subjects to the training sessions (virtual or physical)

Invitation relevant subjects to the webinar



Save the Date !

Cyber-MAR & FORESIGHT

Joint Webinar

18th January 2022

10.00 – 12.30 CET

Cyber MAR
FORESIGHT

Cyber-MAR project has received funding from the European's Union horizon 2020 research & innovation programme under grant agreement No. 833389.
FORESIGHT project has received funding from the European's Union horizon 2020 research & innovation programme under grant agreement No. 833673.

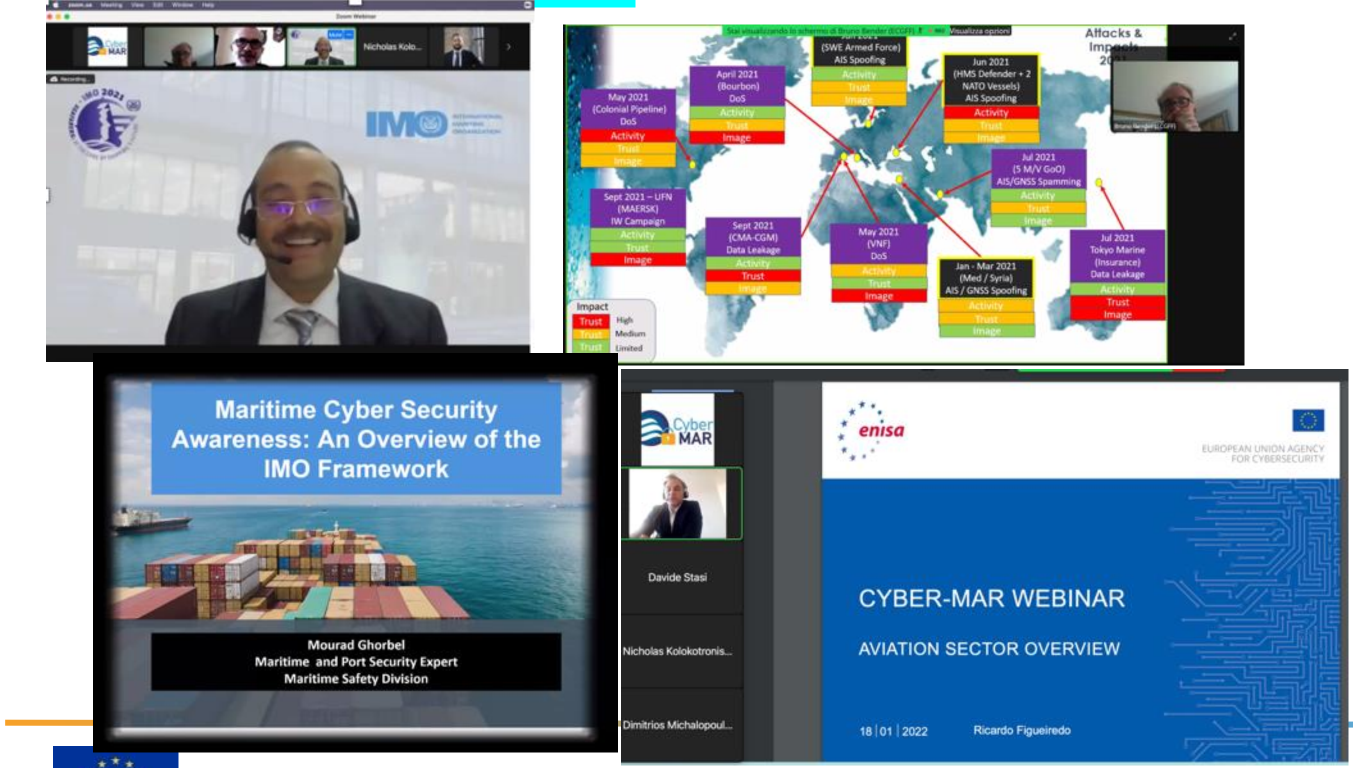
- WINTER SCHOOL with FORESIGHT PROJECT
- WEBINAR with FORESIGHT «*Cyber Security challenges and future perspectives*»

Participants n. 56

WEBINAR “Cyber-Security challenges and future perspectives”

KEY NOTE SPEAKERS

- **Mourad Ghorbel -** Technical Officer for the Maritime Safety Division of the International Maritime Organization **(IMO)**
- **Bruno Bender -** Chairman of the **EU Coastguards Functional Forum Cybersecurity working group** and National cybersecurity coordinator for the Maritime sector in France
- **Ricardo De Sousa - ENISA**



Maritime Cyber Security Awareness: An Overview of the IMO Framework

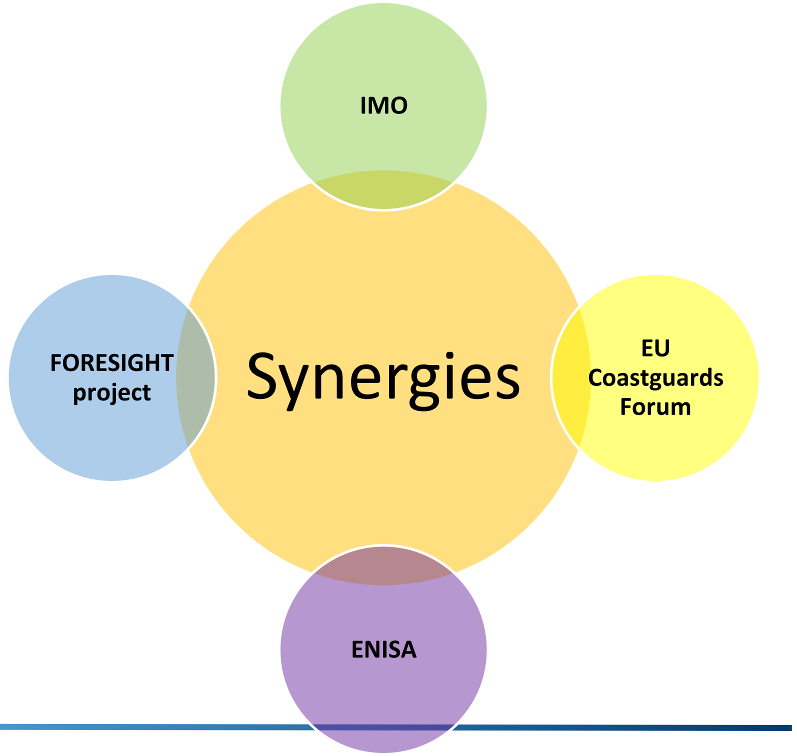
Mourad Ghorbel
Maritime and Port Security Expert
Maritime Safety Division

CYBER-MAR WEBINAR

AVIATION SECTOR OVERVIEW

18 | 01 | 2022 Ricardo Figueiredo

Nicholas Kolo...
IMO
Attacks & Impacts 2021
May 2021 (Colonial Pipeline) DoS
April 2021 (Bourbon) DoS
(SWE Armed Force) AIS Spoofing
Jun 2021 (HMS Defender + 2 NATO Vessels) AIS Spoofing
Jul 2021 (5 M/V GoO) AIS/GNSS Spamming
Sept 2021 – UFN (MAERSK) IW Campaign
Sept 2021 (CMA-CGM) Data Leakage
May 2021 (VNF) DoS
Jan - Mar 2021 (Med / Syria) AIS / GNSS Spoofing
Jul 2021 Tokyo Marine (Insurance) Data Leakage
Activity
Trust
Image
Impact
High
Medium
Limited
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
Cyber MAR
Davide Stasi
Nicholas Kolokotronis...
Dimitrios Michalopoul...



IMO

FORESIGHT project

Synergies

EU Coastguards Forum

ENISA

Ongoing activities: Build up next training

In person training session in Genoa (@IMSSEA facilities)

Entry Level trainings selection

- **May 9, 2022**
  - EL - Attacks issues in deep [UOP]

    Mitigation and remediation [UOP]

    Managing Cybersecurity [WMU]

CUSTOMIZED ON LOCAL STAKEHOLDERS

Next Actions

- Deploy the **LMS** integrated with Cyber-MAR CR

- **TRAINING PLAN TILL END OF 2022**
  - Definition Cyber-MAR training to deliver
  - Preparation syllabus and training material
  - Preparation CTF

- Set up joint activities with sister projects www.Cyber-MAR.eu

Cyber_MAR

Cyber-MAR EU Project

Cyber-MAR

info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION

WORLD MARITIME UNIVERSITY

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