



Cyber-MAR Final and Piraeus Pilot Event

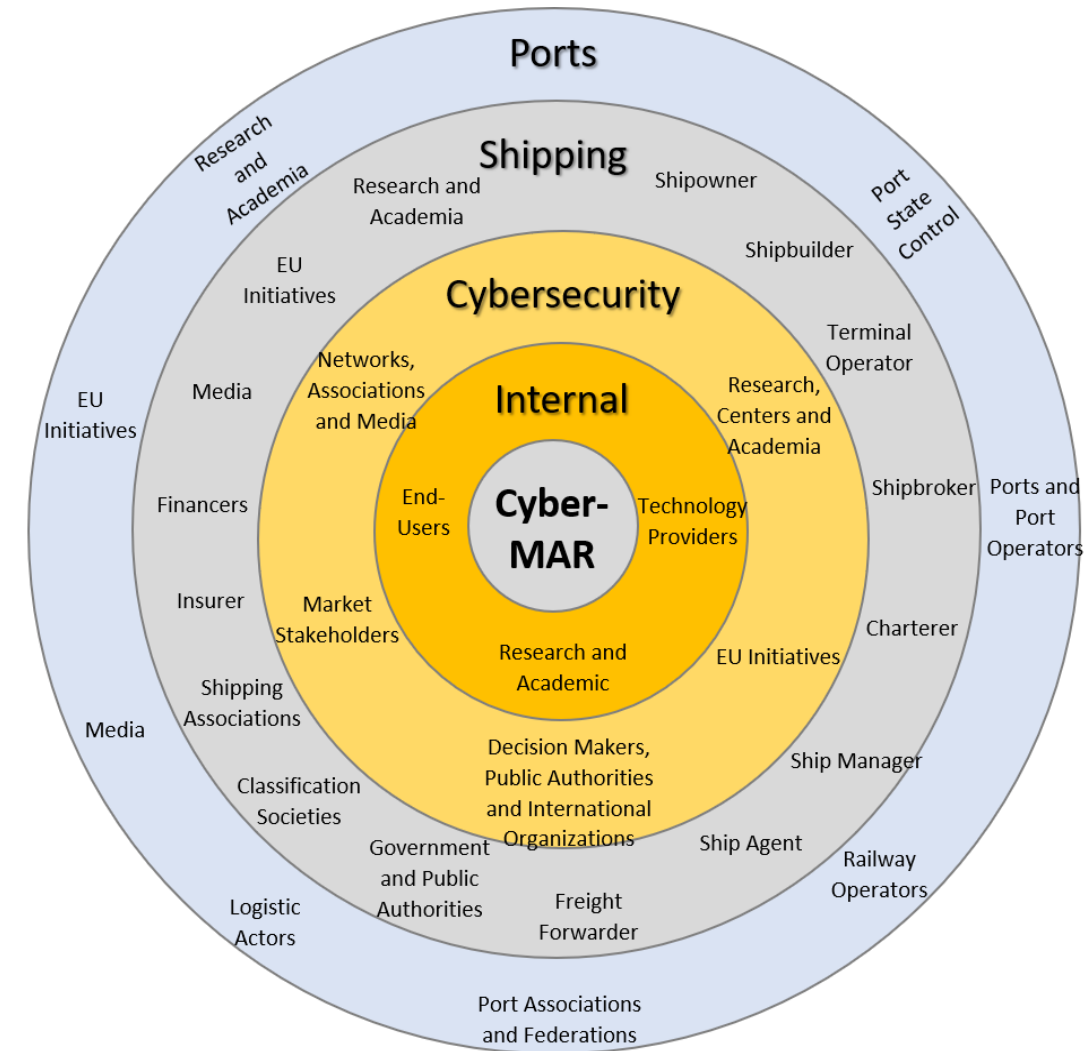
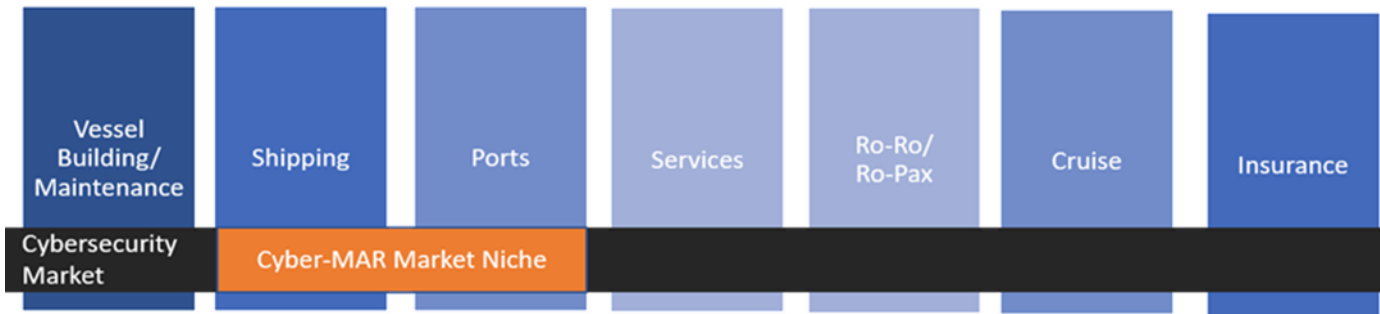
Exploitation of project results

Aljosa Pasic, ATOS

16 December 2022

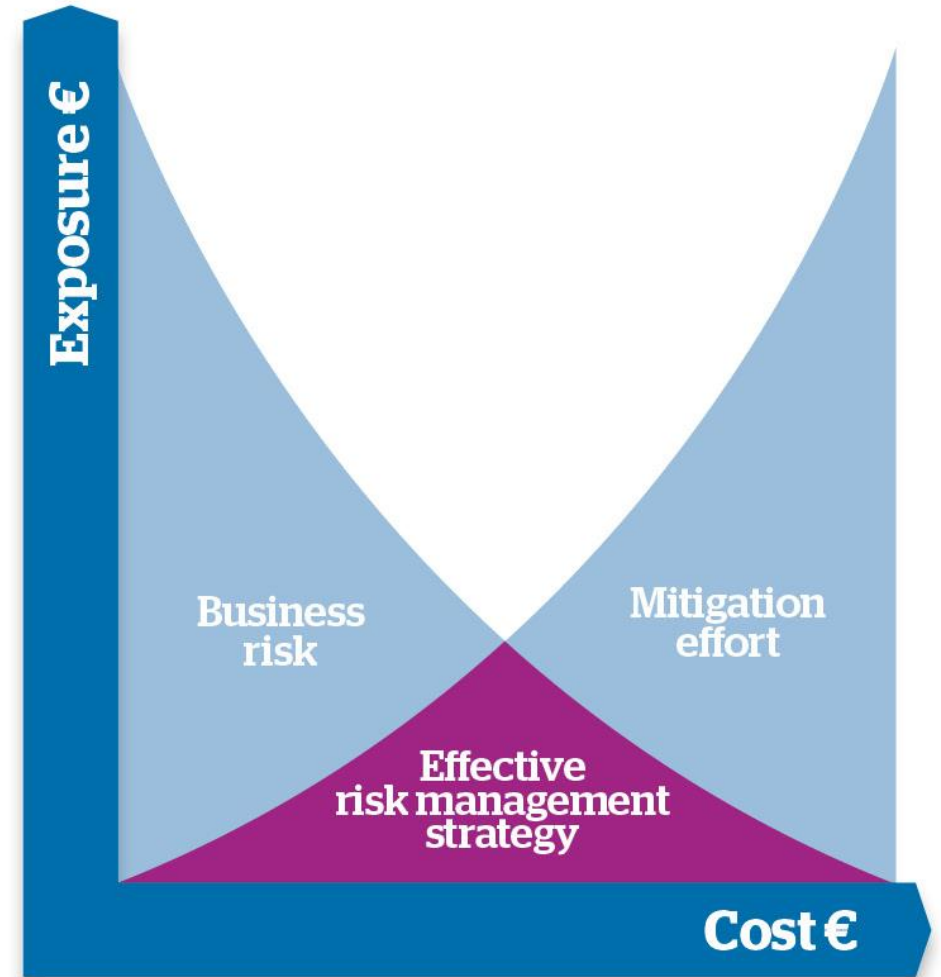
Maritime Sector Ecosystem

- Ecosystem and stakeholders: e.g., ports and shipping decision makers
- Maritime security context and the value chain
- The different levels of cybersecurity maturity
- Speed of cybersecurity technology adoption in the maritime sector
- Legal and regulatory evolution
- Skill shortage and certification schemes



Specific User Perspectives and Challenges

- How much is at risk?
- Do my risks increase as I spend less?
- What is the best preparedness & awareness strategy?
- Do we need more generic cybersecurity training or specific for maritime sector?
- How can we test that every euro spent on security improves security?
- Is it possible to customize detection tools for our specific protocols and technology?

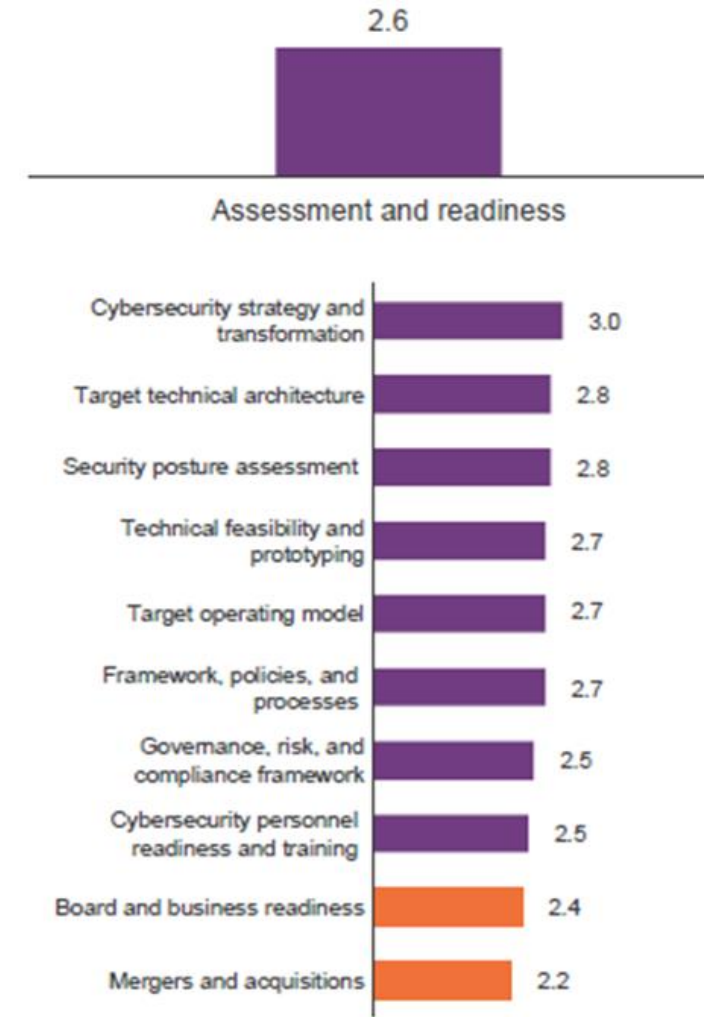


- Intersection of segments:

- Assessment & readiness
- Preparedness
- Training & awareness

- Competitors clustered in 4 categories:

- Large global players
- Maritime sector players that use mix and match with partners of smaller cybersecurity and training providers
- Academic and open source
- CR-platform ecosystems



Maturity of cybersecurity assessment and readiness services (Source:HFS)

Pre-Packaged Cyber-MAR Tools Offering



N	Cyber-MAR Key Exploitable Results (KERs)/ Potential target	SMEs	Research and Academia	Big enterprises and Government
1	VTT Cyber Range			✓
2	UoP Cyber Range		✓	✓
3	DIATEAM Cyber Range	✓	✓	✓
4	Expert S.A.			✓
5	High-Level S.A.			✓
6	VTT IDS Module		✓	✓
7	Ship Simulator		✓	✓
8	SCADA VIRT			✓
9	L-ADS			✓
10	XL-SIEM		✓	✓
11	RecEng			✓
12	LMS platform	✓	✓	✓
13	MaCRA		✓	✓
14	Risk Analysis and Insurance Models			✓

Cyber-MAR Pre-packaged Training Course Offerings



N	Course Level	Cyber-MAR Training Courses	Cyber-MAR Bronze	Cyber-MAR Silver	Cyber-MAR Gold
1	Entry level	Cybersecurity Awareness	✓	✓	✓
2		Managing Cybersecurity	✓	✓	✓
3	Intermediate level	Introduction to the Cyber Range		✓	✓
4		Basic tools for a Cyber Range		✓	✓
5		Using a Cyber Range to understand risk		✓	✓
6	Advanced level	HNS Pro User training			✓
7		Crafting an attack – theory			✓
8		Crafting an attack – practice			✓
9		Lessons learnt from Cyber-MAR pilots: SCADA system in port container terminal			✓
10		Lessons learnt from Cyber-MAR pilots: Vessel navigation & automation system			✓

Exploitable Results (ER), TRL and IPR

N	Cyber-MAR components	Responsible Partner	Initial TRL	Expected TRL
1	VTT Cyber Range	VTT	4	7
2	FMSB/MARSIM (formerly UOP CR and Ship Simulator)	UoP	4	7
3	DIATEAM Cyber Range (formerly named HNS-DIATEAM Platform)	DIATEAM	6	8
4	Expert Situational Awareness	VTT	5	7
5	High-Level Situational Awareness	VTT	5	7
6	VTT IDS Log Mon	VTT	4	7
7	SCADA VIRT	DIATEAM	6	7
8	L-ADS	ATOS	3	7
9	XL-SIEM	ATOS	5	7
10	PREDENG (formerly recommendation Engine)	ICCS	4	6
11	Maritime LMS platform and training	WMU/DIATEAM	5	8
12	MaCRA	UoP	4	6
13	Risk Analysis and Insurance Models (RAIM, formerly named Econometric Model)	AIR	6	7
14	Maritime Cybersecurity Information Sharing Platform (MAR-CISP)	NG	4	6

ER	Components	Ownership (%)	Main Target
1	VTT Cyber Range	VTT (100%)	SMEs, large enterprise, public sector in all sectors
2	FMSB/MARSIM (formerly UOP CR and Ship Simulator)	UoP (100%)	Research and education in maritime sector
3	DIATEAM Cyber Range	DIATEAM (100%)	Large enterprise or public sector in maritime sector
4	Expert SA	VTT (100%)	Research
5	High-Level SA	VTT (100%)	SMEs, large enterprise, public sector in any sector
6	VTT IDS Log Mon Module	VTT (100%)	Research
7	Maritime Cybersecurity Information Sharing Platform (MAR-CISP)	NG (100%)	R&D, maritime stakeholders
8	SCADA VIRT	DIATEAM (100%)	Large enterprise, public sector that uses PLC
9	L-ADS	ATOS (100%)	SMEs, large enterprise in any sector
10	XL-SIEM	ATOS (100%)	SMEs, large enterprise in any sector
11	Prediction Engine (PREDENG)	ICCS (100%)	Research
12	Maritime LMS platform and training (moodle)	WMU (50%) DIATEAM (50%)	Commercial, R&D, Education, Community building

Cyber-MAR Partner	Weight	Background (TRL)	Background (50%)	Foreground (50%)	Total IPR %
DIATEAM	4.5	CR(6), SCADA VIRT(6), LMS(5)	13.64	5.88	19.5
UOP	3	CR (4), MaCRA(4), Ship Simulator (4)	9.09	6.24	15.3
VTT	4	IDS(4), High-Level SA(5), Expert SA(5) CR (4)	12.12	4.77	16.8
ATOS	1.5	XL-SIEM(5), LADS(3)	4.55	4.54	9.0
WMU	0.5	LMS(5)	1.52	2.68	4.1
ICCS	1	PREDENG(4)	3.03	5.39	8.4
AIR	2	EM(6)	6.06	3.63	9.6
VPF	-	-	-	3.76	3.7
PCT	-	-	-	2.65	2.6
SEA	-	-	-	2.42	2.4
NG	-	-	-	5.36	5.3
FAIMM	-	-	-	1.96	1.9
PEARL	-	-	-	0.75	0.7

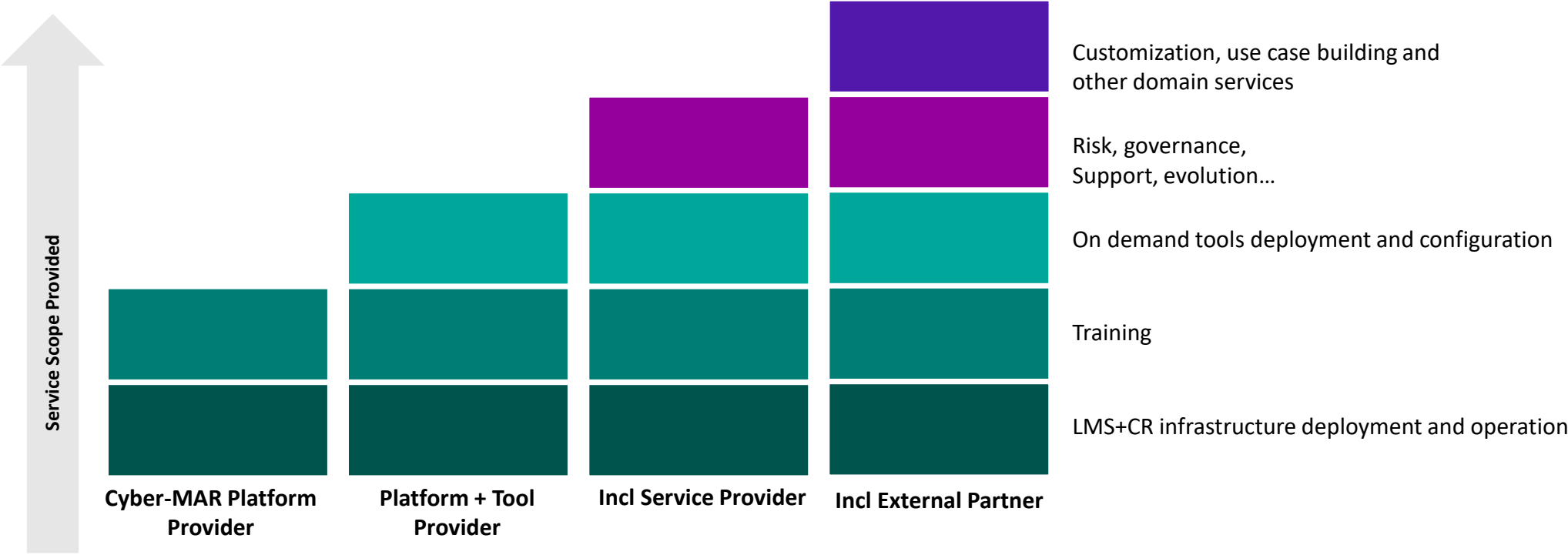


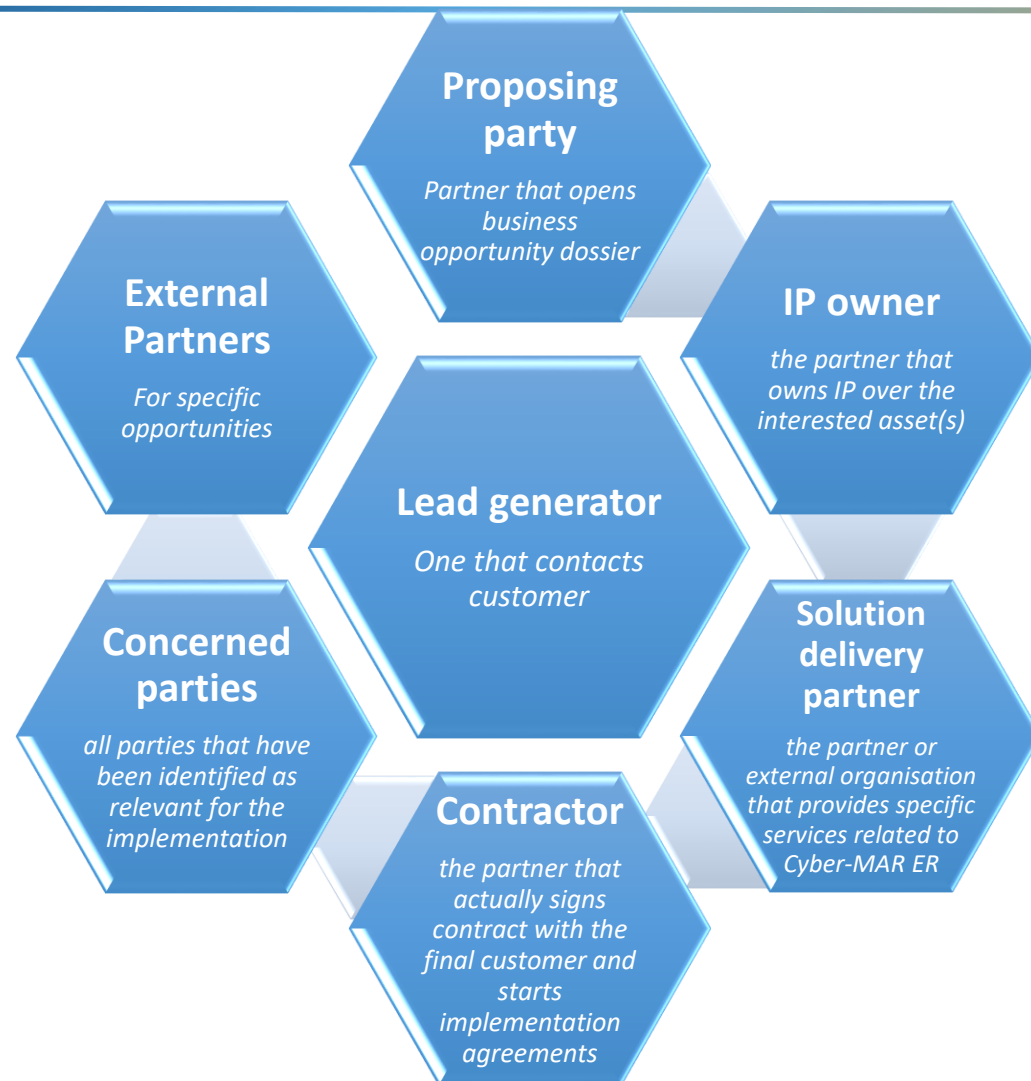
Ready-made Courses, levels and IPR

Course ID	Description	Offering level	Offering Type
E001	Cybersecurity Awareness	Entry Level	Freemium
E002	Managing Cybersecurity	Entry Level	Freemium
I001	Introduction to the Cyber Range	Intermediate	Paid-for
I002	Basic tools for a Cyber Range	Intermediate	Paid-for
I003	Using a Cyber Range to understand risk	Intermediate	Paid-for
A001	HNS Pro User training	Advanced	Paid-for
A002	Crafting an attack – theory	Advanced	Paid-for
A003	Crafting an attack – practice	Advanced	Paid-for
A004	Lessons learnt from Cyber-MAR pilots: SCADA system in port container terminal	Advanced	Paid-for
A005	Lessons learnt from Cyber-MAR pilots: Vessel navigation & automation system	Advanced	Paid-for

Cyber- MAR Partner	Entry-Level Courses (IPR%)	Intermediate Courses (IPR%)	Advanced Courses (IPR%)
DIATEAM	20.31	30.13	39.06
UOP	15.68	10.92	7.35
VTT	2.11	9.85	12.53
ATOS	0.91	8.65	5.07
WMU	36.33	21.16	23.83
ICCS	1.08	1.08	1.08
AIR	0.73	0.73	0.73
VPF	2.11	2.11	2.11
PCT	1.88	1.88	1.88
SEA	1.26	1.26	1.26
NG	1.46	1.46	1.46
FAIMM	15.80	6.87	3.30
PEARL	0.34	0.34	0.34

Cyber-MAR Professional Services

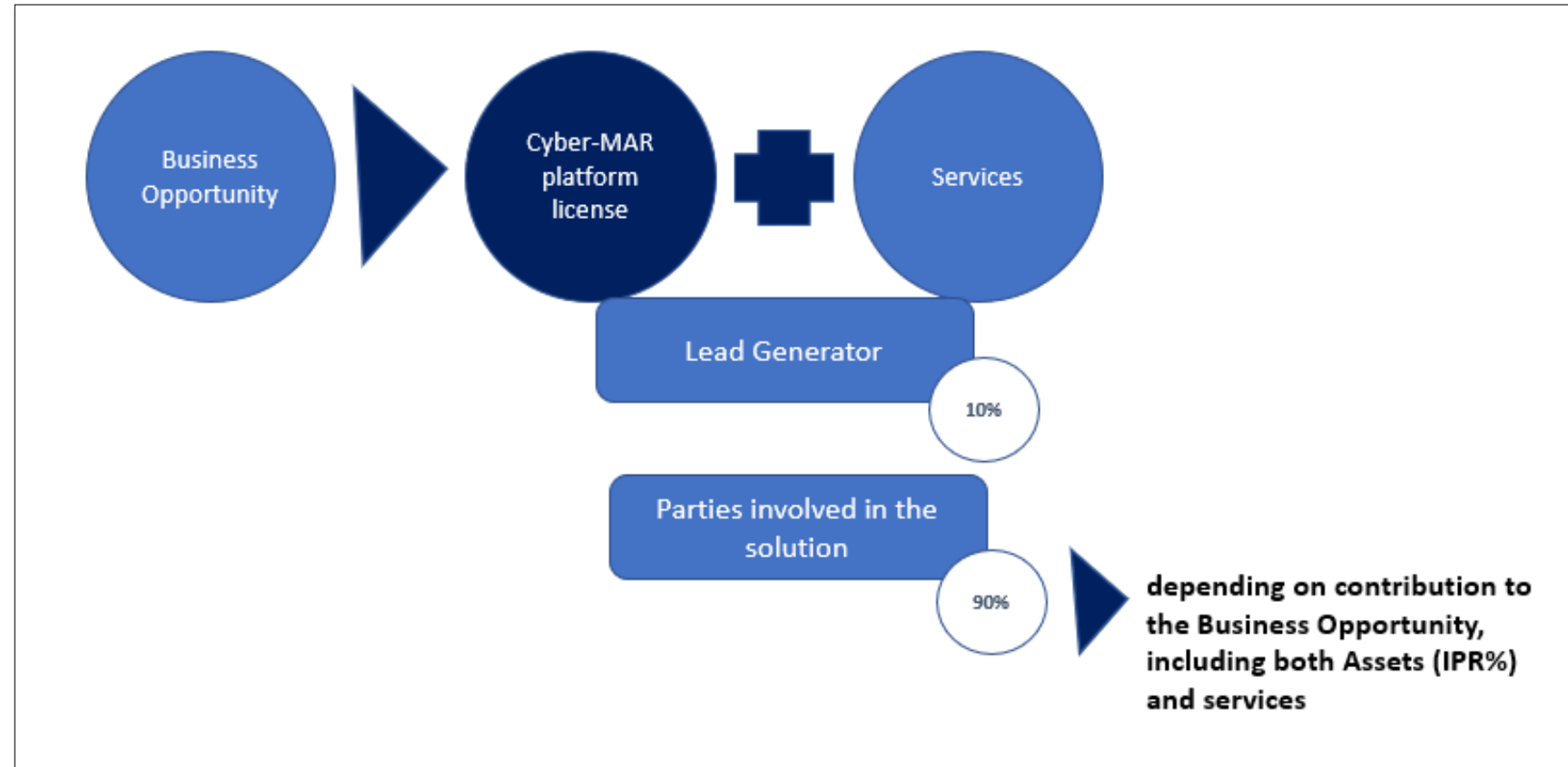




Value Network and Revenue Sharing

Revenue sharing:

- 10% sales
- 90% solution
- A% for IPR owners
- B% for service providers
 - 50% of A to pre-existing IPR
 - 50% of A to new IPR



Cyber-MAR Key Messages (1)

Approach client by:


- Use of references from the project
- Low cost or free service (e.g., initial risk assessment) for the early adopters
- Targeted marketing
- Use of existing partners strengths and channels






Assess cybersecurity maturity, preparedness level, efficiency and feasibility of training by:

- Analyze existing needs, procedures, performance and risks
- Calculate cost to implement offering adapted to business opportunity

A circular diagram divided into four quadrants, each containing a white icon on a dark blue background. The top-left quadrant shows a handshake icon. The top-right quadrant shows a cloud with a checkmark inside. The bottom-left quadrant shows a padlock icon. The bottom-right quadrant shows three stylized human figures. To the right of the circle is a white text box with a dark blue border containing the text "Design offerings of product & service by:" followed by a bulleted list.

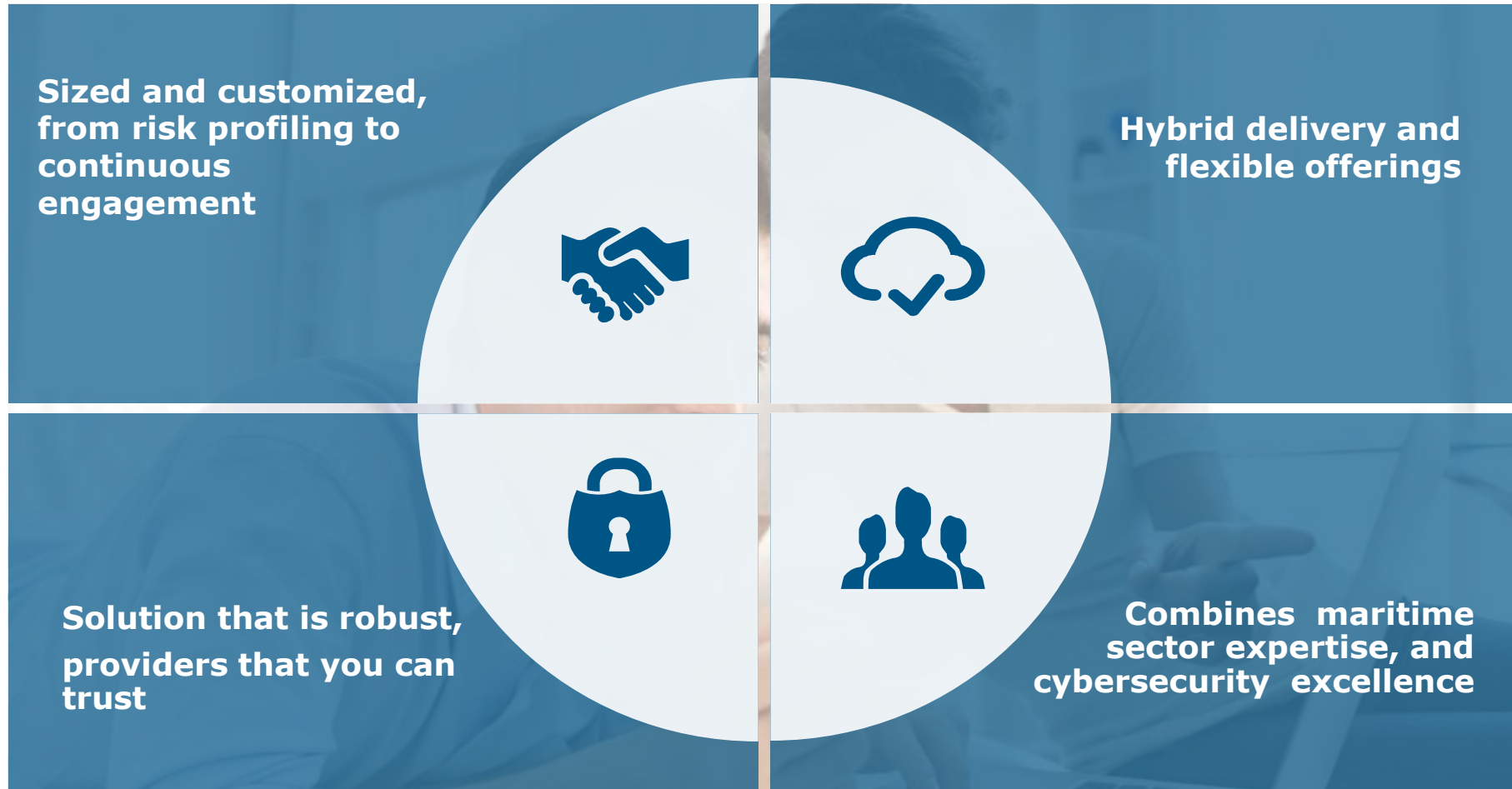
Design offerings of product & service by:

- Adaptation to customers investment strategy
- Collaboration between partners
- Flexibility in implementation arrangements



Engage customer by:

- Continuous support and feedback
- Incentives and change management
- Evolution and maintainance
- Innovation workshops and further assessments



**Sized and customized,
from risk profiling to
continuous
engagement**

**Hybrid delivery and
flexible offerings**

**Solution that is robust,
providers that you can
trust**

**Combines maritime
sector expertise, and
cybersecurity excellence**



www.Cyber-MAR.eu



[Cyber_MAR](#)



[Cyber-MAR EU Project](#)



[Cyber-MAR](#)



info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION

Aljosa Pasic, ATOS

Atos



Aljosa.Pasic@atos.net



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