

Project Title	Civil Cyber Range Platform for a novel approach to cybersecurity threats simulation and professional training
Project Acronym	CYBERWISER.EU
Project Number	786668
Type of instrument	Innovation Action
Topic	DS-07-2017 Cybersecurity PPP: Addressing Advanced Cyber Security Threats and Threat Actors
Starting date of Project	01/09/2018
Duration of the project	30
Website	TBD

D6.1 Communication & Stakeholder plan, first version

Work Package	WP6 Communication, community development, policy & go-to-market
Lead author	Niccolò Zazzeri (Trust-IT)
Contributors	Paolo Lombardi, Cristina Mancarella, Silvana Muscella, Stephanie Parker (Trust-IT), Aniello Bennato, Mario Bizzi (AON), Giorgio Aprile (FFSS), Matteo Merialdo (RHEA), Gencer Erdogan, (SINTEF), Gianluca Dini (UNIP) Anže Žitnik (XLAB), Antonio Álvarez (ATOS)
Peer reviewers	María Teresa García (ATOS), Rossella Miccolis (FFSS), Aida Omerović (SINTEF)
Version	V1.0
Due Date	30/11/2018
Submission Date	21/12/2018

Dissemination Level:

X	PU: Public
	CO: Confidential, only for members of the consortium (including the Commission)
	EU-RES. Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)
	EU-CON. Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)
	EU-SEC. Classified Information: SECRET UE (Commission Decision 2005/444/EC)



The work described in this document has been conducted within the CYBERWISER project. This project has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 786668.

Version History

Revision	Date	Editor	Comments
0.1	13/11/2018	Paolo Lombardi, Stephanie Parker, Niccolò Zazzeri (Trust-IT)	TOC
0.2	14/11/2018	Paolo Lombardi, Niccolò Zazzeri (Trust-IT)	Revised TOC with comments from partners.
0.3	21/11/2018	AON, ATOS, EdP, FFSS, RHEA, SINTEF, UniPi, XLAB,	Feedback on structure of the document and individual contributions.
0.4	05/12/2018	Paolo Lombardi, Cristina Mancarella, Silvana Muscella, Stephanie Parker, Niccolò Zazzeri (Trust-IT)	First complete draft for peer review.
0.5	11/12/2018	María Teresa García (ATOS)	Internal review
0.6	12/12/2018	Rossella Miccolis (FFSS)	Internal review
0.7	13/12/2018	Aida Omerović (SINTEF)	Internal review
0.8	18/12/2018	Paolo Lombardi, Stephanie Parker, Niccolò Zazzeri (Trust-IT)	Internal review comments addressed
1.0	21/12/2018	María Teresa García (ATOS)	Quality Check and final version

List of Contributors

The list of contributors to this deliverable are presented in the following table:

Section	Author(s)
Executive Summary	Trust-IT
1. Introduction	Trust-IT
2. Strategy	Trust-IT
3. Results and dissemination & communication assets	Trust-IT, AON, ATOS, FS SPA, RHEA, SINTEF, XLAB
4. Communication and dissemination plan	Trust-IT
5. Achievements to-date	Trust-IT
6. Conclusions	Trust-IT
References	Trust-IT

Keywords

Communication, Dissemination, Stakeholders, Engagement, Plan, Marketing, Branding.

Disclaimer

This document contains information which is proprietary to the CYBERWISER.eu consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or parts, except with the prior written consent of the CYBERWISER.eu consortium.

Table of Contents

1. INTRODUCTION	6
2. STRATEGY	8
3. PROJECT RESULTS AND ASSETS FOR DISSEMINATION & COMMUNICATION.....	26
4. COMMUNICATION AND DISSEMINATION PLAN	34
5. ACHIEVEMENTS TO-DATE	44
6. CONCLUSIONS	53

List of figures

Figure 1: Main objectives and mission	8
Figure 2: CYBERWISER.eu stakeholders.....	11
Figure 3: The “pyramidal offer”	19
Figure 4: Elements determining an effective communication strategy	21
Figure 5: Event promotion.....	38
Figure 6: First 6-month timeline as presented at the kick-off meeting (Madrid, 3-4 October 2018)	38
Figure 7: post on the social platform Twitter.....	39
Figure 8: post concerning the Open Pilot	39
Figure 9: Press Release published on LinkedIn	40
Figure 10: Typical Monitoring dashboard	42
Figure 11: Roadmap of the communication & stakeholder plan (M4-M18).	43
Figure 12: CYBERWISER.eu branding	44
Figure 13: Standard PPT Template.....	44
Figure 14: Cover and second page of the first version of the CYBERWISER.eu ‘Overview Presentation’	45
Figure 15: CYBERWISER.eu homepage as of November 2018.....	46
Figure 16: CYBERWISER.eu social media presence (sample)	47
Figure 17: Flyer and roll-up banner	48
Figure 18: Press release published on CORDIS	49
Figure 19: CYBERWISER.eu Video	50

List of tables

Table 1. Table of acronyms.....	7
Table 2: Communication, Dissemination & Engagement measures	11
Table 3: Adopters and related benefits.....	13
Table 4: Sample of priority CYBERWISER.eu Multipliers.....	13
Table 5: Stakeholder Group – Students and professionals-in-training	14
Table 6: Stakeholder Group – SMEs and LEs.....	15
Table 7: Stakeholder Group – Public Administration	15

Table 8: Stakeholder Group – HE	15
Table 9: Stakeholder Group – CSIRTs and CERTs.....	16
Table 10: Stakeholder Group – Industry and trade associations	16
Table 11: Stakeholder Group – SDOs, certification organisations	16
Table 12: Stakeholder Group – Policy makers	16
Table 13: Stakeholder Group – Cybersecurity clusters	17
Table 14: Stakeholder Group – Media, opinion leaders and cybersecurity networked groups	17
Table 15: Stakeholder Group – Civil society, NGOs & citizens.....	17
Table 16: CYBERWISER.eu features vs offering level (preliminary)	20
Table 17: Motivational mechanisms	24
Table 18: Project results vs Freemium Level of the offering.	27
Table 19: Project results vs Basic Level of the offering.	27
Table 20: Project results vs Intermediate Level of the offering.	28
Table 21: Project results vs Advanced Level of the offering.	28
Table 22: Project results in Training.....	29
Table 23: FSP#1 on Professional and Academic Training.....	31
Table 24: FSP#2 on Transport Infrastructure	32
Table 25: FSP#3 on Energy Infrastructure	33
Table 26: Additional levers for engagement	36
Table 27: Sample of Media Channels	36
Table 28: Target events (2019)	41
Table 29: Visibility gained at events (as of November 2018).	50

Executive Summary

The present document presents the first of 3 versions of the plan for communication, dissemination and stakeholders engagement activities of the CYBERWISER.eu.

Moving from the project objectives, the strategy for communication and stakeholders engagement (WP6, "Communication, community development, policy & go-to-market") is defined for the period December 2018 – February 2020. In particular, a drill-down on the stakeholder groups and channels utilised is enclosed.

Given the evolving phase of the project, due to the ongoing design and development activities, some of the detailed information around results achieved and communication and dissemination assets related to those is still not available at the time of writing. Therefore, the report is to be considered, for some aspects, a "living document", which will be updated as part of WP6 activities. Be that as it may, a roadmap for communication and engagement activities envisaged for the aforementioned timeframe is provided.

Finally, a summary of the activities conducted in the first 3 months of the project, not covered by the present plan is provided. Some preliminary conclusions complete the document, highlighting the good collaboration registered so far among all project partners to commit to a shared communication and engagement plan.

1. Introduction

1.1 Purpose

The purpose of the present document is to define the strategy and foreseen activities for communication and stakeholder engagement (WP6, "Communication, community development, policy & go-to-market"), for the period December 2018 – February 2020. In particular, a drill-down on the stakeholder groups and channels utilised is enclosed.

The present document presents the first of 3 versions of the plan for communication, dissemination and stakeholders engagement activities of the CYBERWISER.eu. Owing to the early stages in the project workplan, some of the detailed information around results achieved and communication and dissemination assets related to those is still not available at the time of writing, and the report is effectively to be considered, for some aspects, a "living document". The present version of the document it will be updated as part of WP6 activities.

Two more versions of this document are planned for Month 18 (February 2020) and Month 30 (February 2021. Project completion). Other related deliverables: D6.2 "First business model and commercialisation strategy" (Month 12, August 2019).

1.2 Structure of the document

The document is leanly organised in 4 central sections:

- Section 2 defines the strategy at the basis of the present version of the plan;
- The assets available for dissemination and communication, arising from the expected project results, are described in Section 3;
- Section 4 lays out the Communication and Dissemination plan itself for the period M4-M18; The communication and stakeholder engagement activities carried out in the first 3 months of the project and that were not covered by the plan, are reported in Section 5.

1.3 Glossary of Acronyms

Acronym	Description
CyPR	Cybersecurity Professional Register
ECISO	European Cyber Security Organisation
FSP	Full-Scale Pilot
GA	Grant Agreement
HE	Higher Education
IHE	Institution of Higher Education
LEs	Large enterprises
MRLs	Market Readiness Levels
SEB	Stakeholders Expert Board
SEO	Search Engine Optimisation

Acronym	Description
SMART	Specific, Measurable, Achievable, Realistic, Timely and Targeted
SME	Small- and Medium-sized Enterprises
WP	WorkPackage

Table 1. Table of acronyms

2. Strategy

To ensure coordinated, regular communication of CYBERWISER.eu, providing opportunity of visibility to all stakeholders, as well developing an effective go-to-market approach, the following strategic elements have been established, in good agreement with the provisions of the GA.

2.1 Objectives

CYBERWISER.eu delivers a cyber range simulation environment and training platform based on an interdisciplinary approach to cybersecurity capacity-building. By training highly-skilled cybersecurity professionals to respond faster and more effectively to a fast-evolving cyber threat landscape, CYBERWISER.eu fills an important talent gap across the EU. Achieving a core set of indicators in the number of trained students and professionals will show how CYBERWISER.eu reduces fragmentation across the EU. Moreover, CYBERWISER.eu aims to raise awareness with people not directly involved in cybersecurity operations, considering this a fundamental step in protecting ICT-intensive organisations against cyber threats.

The figure below is a concise view of the CYBERWISER.eu path towards innovation and market uptake.

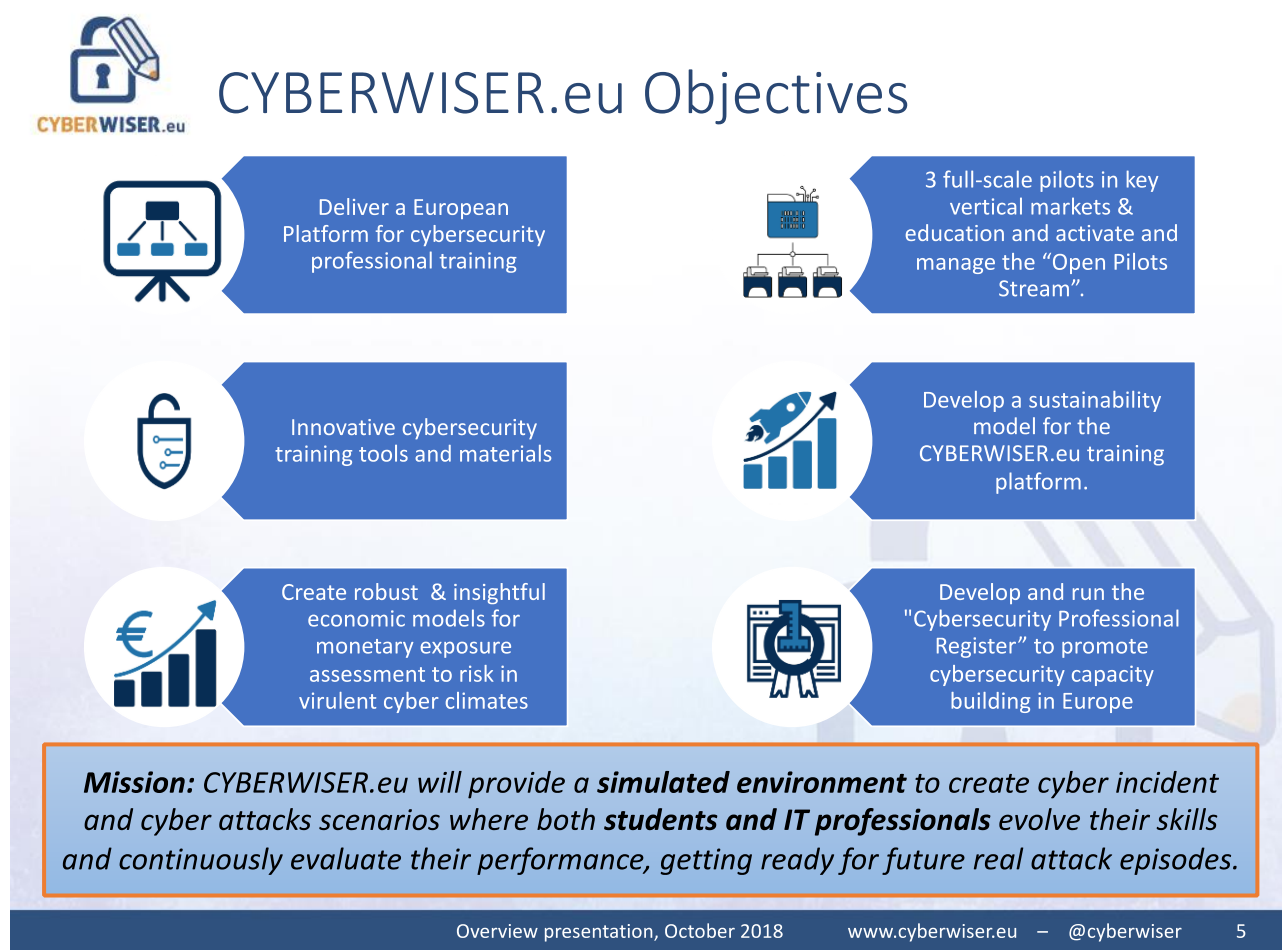


Figure 1: Main objectives and mission

To achieve its exploitation goals, CYBERWISER.eu pursues three complementary paths step by step:

1. A **joint exploitation** path underpinning the sustainability of the CYBERWISER.eu platform by extending uptake through the Open Pilot Stream (open beta) recruited through a large-scale promotional campaign targeting the consortium's extensive networked community. This community comprises private and public-sector stakeholders, spanning risk managers and CISOs to small IT teams and company decision-makers with different skill sets. The strategic goal for CYBERWISER.eu is to establish a viable route to market through the production of a Joint Business and Exploitation Plan.
2. **Exploitation plans of the individual project partners** aligned with the organisation's business and research strategy and aimed at improving business portfolios, institutional research programmes and educational services.
3. **Exploitation of use cases and pilots**, notably 3 full-scale Pilots and pilots coming from the Open Pilot Stream as early demonstrators and users of CYBERWISER.eu. Stakeholder engagement and profiling will be a priority activity for the Open Pilot Stream campaign and identifying other end-users across diverse vertical industries. Key stages in the CYBERWISER.eu go-to-market strategy include: interim and final full-scale pilot validation; market launch based on the final MRL(s) identified and a global expansion phase.

Plans in November 2018; February 2020 and January 2021 set out clearly defined iterative roadmaps of planned communication and stakeholder engagement activities, showing how CYBERWISER.eu is evolving its communication kit with diverse formats and extending its already extensive network. The plans are also key to defining the KPI-driven approach, including some qualitative metrics, by showing how CYBERWISER.eu monitors impacts over time.

CYBERWISER.eu communication strategy supporting the Go-to-Market Strategy

The dissemination and exploitation of results is integrated into the CYBERWISER.eu 30-month Communication Strategy. The strategy is based on the SMART approach (specific, measurable, achievable, realistic, timely and targeted), geared towards the information and training needs of the diverse stakeholders targeted.

Starting line: M1 (September 2018) sees the launch of the CYBERWISER.eu dissemination and exploitation strategy in conjunction with the project launch. This early start ensures the consortium carries out regular activities on its value proposition and stakeholder profiling while extending the current community and increasing awareness and visibility.

Regular desk research on market and technology trends for cyber security will help create up-to-date market analyses and zoom in on exploitation opportunities.

To ensure effective dissemination and exploitation, the CYBERWISER.eu communications plan will combine templates and guidelines for technical partners with a SMART communications kit, including a SEO-based web platform, light-reading content, videos, a clearly defined stakeholder engagement plan and demos showing CYBERWISER.eu in action.

All this will be supported by the CYBERWISER.eu Stakeholder Expert Board (SEB)¹, which will guide CYBERWISER.eu with timely insights into the evolving threat landscape.

¹ While the CYBERWISER.eu Consortium is already skilled for carrying out the Project workplan, will be supported by a Stakeholders Expert Board (SEB), which is going to be composed of at least 15 (and maximum 20) dynamic, high-level opinion leaders at European and global level, with a proven track record. The SEB members are recognised experts in the cybersecurity training domain (including awareness raising efforts), representing different stakeholder groups including the industry, SDOs and Policy and Regulatory views.

From a communication and dissemination perspective we report here below the elements, related measures and metrics that the project will undertake to ensure the effectiveness of its outreach and go-to-market strategy:

Element	Description	KPIs ²
Workshops	3 CYBERWISER.eu Achievements Workshop" plus 1 Final CYBERWISER.eu Showcased Final Event – Oct 2020 in conjunction with the EU Cybersecurity month.	4 co-located workshops
Hackathons	To coincide with the workshops above.	2 Hackathons
Webinars	Webinars will be organized to ensure cost-effective outreach, awareness raising and community member recruitment.	6 Webinars
Synergies #1	Synergies/partnerships established with EU CERTs/CSIRTs/National Cyber Security Centres	>10
Mktg campaigns	Marketing campaigns based on identified MRLs, spanning press releases, social media SMART campaigns, commercial conferences and trade fairs	1 campaign in M1-10 2 campaigns in M11-15 4 campaigns in M16-30 Min. 2 + 4 + 6 events in commercial settings over the same periods
Synergies #2	Synergies established at national, EU or international levels to share new knowledge/promote standardisation.	>5
Synergies with ECSO	Transfer of research results and service offer to ECSO, especially WG4 – SMEs (Atos, Trust-IT)	Presentations at annual meetings and inputs to relevant WGs
Presentations/ Publications	Dissemination of technical results through peer reviewed conferences and papers	Min. 4 scientific conferences
SEO-based and service-oriented web platform	N° of monthly visitors N° of clicks on training platform	1000/month from M6 up to 3000/month by M30 500 in M12 up to 2000 by M30
Web-based Info Desk	Awareness videos; light-reading papers; essential guides; policy insights	Min. 3 videos; quarterly papers; six-monthly guides; six-monthly insights
Promotional and Marketing Material, including banner adverts	For events and web/social media announcements	As required, min. 6-month updates
Newsletters	Featuring project updates and	Monthly from M3.

² As per the CYBERWISER.eu Grant Agreement.

Element	Description	KPIs ²
	insights	
Press Releases	Major project announcements and achievements	Min. 6 over 30 months

Table 2: Communication, Dissemination & Engagement measures

2.2 Stakeholders

Security is engrained in every aspect of our lives. WISER reported extensively on the evolving landscape, noting the lack of awareness about the socio-economic impacts of cyber-attacks especially by SMEs but also across vertical industries with little sense of urgency about the scale of the issues at stake.

The cyber security talent pool is highly fragmented across the EU in a landscape where the impacts of a cyber-attack can be disproportionate to the technical skills of cybercriminals and where few checks are made on hardware and software vulnerabilities, let alone certified.

To fully achieve its impacts, CYBERWISER.eu needs to prove its real-world benefits for end-users and all the other stakeholder groups (see Figure 2 below). Without a solid set of end-users, exploitation impacts will be diminished. CYBERWISER.eu therefore defines a core set of primary end-users within and beyond the project, scaling out through the Open Pilot Stream and across a networked community evolving over time.

CYBERWISER.eu has already clearly identified at proposal stage the core set of Adopter Stakeholders to target across vertical sectors (see Table 3). Targeted engagement will thus help build on the extensive business network built during WISER. Community profiling will help to identify market leads and users to exploit also after the project funding cycle.

The figure below offers an overview of the stakeholders targeted by CYBERWISER.eu, divided in End-users and Other stakeholders. The latter include: Industry and Trade Associations; media and opinion leaders; cyber security clusters; relevant civil society groups (e.g. the International Civil Society Centre); policy makers for IT and cyber security, as well as EU and international cyber security think tanks.



Figure 2: CYBERWISER.eu stakeholders

End-users are vital to the success of CYBERWISER.eu exploitation and sustainability. They are also key to contributing to the creation of a cyber security competence community across the EU. The table below shows how CYBERWISER.eu will benefit a wide range of stakeholders from industry (large enterprises, SMEs), universities and research centres and vertical industries participating as Full-scale pilots and through the Open Pilot Scheme. Scaling up the community will be key to realising the full exploitation potential of CYBERWISER.eu across universities, businesses and vertical industries.

Adopter Stakeholder Category	CYBERWISER.eu Benefits and Impacts
Computer Science and telecommunications engineers (e.g. undergraduates, post-graduates, PhD students, post-docs) in institutes of higher education (IHE): this stakeholder group benefits from on-the-ground training designed to increase the ability to deal with high-risk scenarios in a multi-faceted and fast-evolving landscape.	CYBERWISER.eu will provide different entry levels based on current skill levels and needs analysis. Educational certificates to verify learning outcomes and increase impacts of qualifications with a proven track record.
Large Enterprises, Critical Infrastructures and SMEs: All digital businesses are potentially vulnerable as attack targets, whether they are a Fortune 500 company, a family-run business or a utility company. Businesses of all sizes need to adopt a business-driven security strategy and align business and technical goals as attacks generally cause more extensive damage and higher impacts. CYBERWISER.EU encourages large enterprises across different vertical markets to adopt a board-level, holistic approach to cyber security to reinforce cyber range training impacts. CYBERWISER.EU increases interdisciplinary capacities and skills across critical infrastructures.	CYBERWISER.eu builds on its extensive support of this stakeholder category with practical guidance on basic security controls, health checks, risk assessments and audits will help them implement a business-driven security strategy as the convergence of security and risk management. CYBERWISER.EU can help supply-chain SMEs not only in protecting critical business assets but also as a weak link giving access to their larger business partners with more valuable assets. More generally, CYBERWISER.EU will help SMEs build a small but highly specialised cybersecurity team (work group or champions) without needing to hire a CISO wherever this is beyond their financial possibilities.
Expansion to vertical industries: CYBERWISER.eu has already found a core set of stakeholders to target across vertical sectors from its wider networks, including targeted synergies with the most relevant associations (see Table 4).	Increase awareness of cyber-attack impacts across diverse sectors and fostering a systematic approach to cyber security in EU industry. Support the creation of end-to-end common risk management approach across EU industry as vital for achieving the goals of the DSM.
Public Administration (National and Regional): CYBERWISER.EU can help overcome barriers to digitisation by supporting this stakeholder group in understanding cyber risks, fostering best practices and cyber preparedness as central to building trust among citizens.	CYBERWISER.EU offers this group the necessary skills for cyber threat detection and response through a role-based approach within a complementary team while increasing awareness across the entire organisation.
CSIRTs and CERTs: CYBERWISER.eu can help decision makers (directors and heads of security and privacy; directors of national cyber security centres) align national cybersecurity strategies for operational capacity-building through educational and training programmes; strengthen links across different stakeholder groups and improve collaboration.	CYBERWISER.eu can draw attention to best practices in notifying cyber breaches by all organisations oblige to do so under the legal requirements of the GDPR and NIS Directive. The Cartography already developed in the context of the WISER project ³ can be re-structured to highlight competent authorities across EU with practical guides to the legal and

³ <https://www.cyberwiser.eu/cartography>

Adopter Stakeholder Category	CYBERWISER.eu Benefits and Impacts
	technical requirements for GDPR and NIS Directive.

Table 3: Adopters and related benefits

Table 4 below shows a sample of current network connections CYBERWISER.eu will use within and beyond its own community, including strategic synergies with multipliers. CYBERWISER.eu will also establish synergies with peer cyber security projects to boost impacts through joint dissemination activities and stakeholder engagement events. A sample of links to security and industry associations, on which CYBERWISER.eu will draw is provided in the table below.

Priority Multipliers
Cyber security: ECSO; ENISA; EEMA (e-identity and security). National cyber security centres, e.g. Danish Centre for Cyber Security; UK National Cyber Security Centre (NCSC).
LinkedIn groups - Information Security (428K members); Cyber Security Forum Initiative – CSFI 86K. Multipliers and clusters - Cyber security clusters, e.g. Finnish Information Security Cluster, AEI Seguridad. CITIC, @SecTest9 (security testing); @SecurityNews6; @InfoSecurity99; @CyberSecUpdate; @cybersec_cl; @SecurityDialog.
IHE: over 600+ decision makers in universities and research centres. National policy makers, e.g. French Research Ministry of Higher Education.
Transportation: European Rail Union; International Rail Union (EU representatives). The Transport Association (UK), Association for European Transport. @Transport_Assoc , @EuTransportConf , @CENIT_Research .
Energy: eG4U European NGO; FEDARENE aisbl – European Federation of Agencies and Regions for Energy and the Environment; EDSO (smart grid).
Other verticals: CYBERWISER.eu has already engaged with two relevant EU R&I projects to establish a synergy for the joint dissemination of results and stakeholder engagement. Examples include POSEIDON: focus on vertical industries, such as finance and banking; smart cities (e.g. Santander); government (Austria) and the private sector (e.g. SOFTEAM); DEFEND: focus on healthcare and energy.
SMEs: SMEs: Over 130 connections to business and trade associations across EU, e. Digital SME Alliance; ANITEC, ASSINTEL, ISME, CONETIC, CLUSIT; ICT-HU, TechUK, FSB, Federal Association of ICT-SMEs of Germany , Digital Catapult . Over 20 large industry associations and forums .

Table 4: Sample of priority CYBERWISER.eu Multipliers

In the following tables the various Stakeholder Groups are further detailed as far approach and priority multipliers utilised are concerned.

Note: The tables will be completed in the early months of 2019, when the CYBERSECURITY.eu offering will be consolidated, as a consequence of completion of the first phase of design phase (D2.3 "Platform design, initial version" – 6, February 2019).

2.2.1 Cybersecurity HE students and professionals

The stakeholder group is subdivided into 2 subgroups, as indicated in the table.

Stakeholder group	Description and approach	Size of the target group	Priority multipliers (examples)
1a. Cybersecurity HE students	Students (e.g. undergraduates, post-graduates, PhD students, post-docs, professionals in training path) in institutes of higher education (IHE): this stakeholder group benefits from on-the-ground training designed to increase the ability to deal with high-risk scenarios in a multi-faceted and fast-evolving landscape. CYBERWISER.eu will provide different entry levels based on current skill levels and needs analysis.	<i>TBC – work in progress</i>	
1b. Professionals-in-training		<i>TBC – work in progress</i>	

Table 5: Stakeholder Group – Students and professionals-in-training

2.2.2 SMEs, LEs, and critical infrastructures

All digital businesses are potentially vulnerable as attack targets, whether they are a Fortune 500 company, a family-run business or a utility company. Businesses of all sizes need to adopt a business-driven security strategy and align business and technical goals as attacks generally cause more extensive damage and higher impacts. CYBERWISER.eu offers practical guidance on basic security controls, health checks, risk assessments and audits will help them implement a business-driven security strategy as the convergence of security and risk management.

Evidence-based research highlights the potential of reaching out to diverse critical infrastructure stakeholders, e.g. the "white paper on Research and Innovation in Cybersecurity. AEGIS project"⁴. This white paper highlights high priority areas in verticals such as **financial services**, **health** and **maritime** (transport and logistics), where the need to boost cybersecurity education and training is a high priority for Europe, scoring equally with assurance, audit, and certification and security management and governance from an EU perspective.

Stakeholder group	Description and approach	Size of the target group	Priority multipliers (examples)
2a. SMEs	CYBERWISER.EU can help supply-chain SMEs not only in protecting critical business assets but also as a weak link giving access to their larger business partners with more valuable assets. More generally, CYBERWISER.EU will help SMEs build a small but highly specialised cybersecurity team (work group or champions) without needing to hire a CISO wherever this is beyond their financial possibilities.	<i>TBC – work in progress</i>	
2b. LEs	CYBERWISER.EU encourages large enterprises across different vertical markets to adopt a board-	<i>TBC – work in progress</i>	

⁴ October 2018, https://drive.google.com/file/d/1TNPSwVHQYngaaDnZ_itxiu7QzHxk9aP9/view.

Stakeholder group	Description and approach	Size of the target group	Priority multipliers (examples)
	level, holistic approach to cyber security to reinforce cyber range training impacts.		
2c. Critical Infrastructures	CYBERWISER.EU will seek for collaboration with critical infrastructures to adopt a board-level, holistic approach to cyber security to reinforce cyber range training impacts. CYBERWISER.EU increases interdisciplinary capacities and skills across critical infrastructures.	<i>TBC – work in progress</i>	

Table 6: Stakeholder Group – SMEs and LEs

2.2.3 Public administration (National and Regional)

Stakeholder group	Description and approach	Size of the target group	Priority multipliers (examples)
3. Public Administration (National and regional)	CYBERWISER.EU can help overcome barriers to digitisation by supporting this stakeholder group in understanding cyber risks, fostering best practices and cyber preparedness as central to building trust among citizens. CYBERWISER.EU offers this group the necessary skills for cyber threat detection and response through a role-based approach within a complementary team while increasing awareness across the entire organisation.	<i>TBC – work in progress</i>	

Table 7: Stakeholder Group – Public Administration

2.2.4 Universities, research institutions, research infrastructures and other HE organisations

Stakeholder group	Description and approach	Size of the target group	Priority multipliers (examples)
4. Universities, research institutions, research infrastructures and other HE organisations		<i>TBC – work in progress</i>	

Table 8: Stakeholder Group – HE

2.2.5 CSIRTs and CERTs

Stakeholder group	Description and approach	Size of the target group	Priority multipliers (examples)
CSIRTs and CERTs	CYBERWISER.EU can help decision makers (directors and heads of security and privacy; directors of national cyber security centres) align national cybersecurity strategies for operational capacity-building through educational and training programmes; strengthen links across different stakeholder groups and improve collaboration	<i>TBC – work in progress</i>	

Table 9: Stakeholder Group – CSIRTs and CERTs

2.2.6 Industry and trade associations

Stakeholder group	Description and approach	Size of the target group	Priority multipliers (examples)
6. Industry & Trade Associations		<i>TBC – work in progress</i>	

Table 10: Stakeholder Group – Industry and trade associations

2.2.7 SDOs, certification organisations

Stakeholder group	Description and approach	Size of the target group	Priority multipliers (examples)
7. SDOs, certification organisations		<i>TBC – work in progress</i>	

Table 11: Stakeholder Group – SDOs, certification organisations

2.2.8 Policy makers, ECSO, including EU & national agencies

Stakeholder group	Description and approach	Size of the target group	Priority multipliers (examples)
8. Policy makers, ECSO, including EU & national agencies		<i>TBC – work in progress</i>	

Table 12: Stakeholder Group – Policy makers

2.2.9 Cybersecurity clusters

Stakeholder group	Description and approach	Size of the target group	Priority multipliers (examples)
9. Cybersecurity clusters		<i>TBC – work in progress</i>	
		<i>TBC – work in progress</i>	

Table 13: Stakeholder Group – Cybersecurity clusters

2.2.10 Media, opinion leaders and cybersecurity networked groups

Stakeholder group	Description and approach	Size of the target group	Priority multipliers (examples)
10a. Media		<i>TBC – work in progress</i>	
10b. Opinion Leaders		<i>TBC – work in progress</i>	
10c. Cybersecurity networked groups		<i>TBC – work in progress</i>	

Table 14: Stakeholder Group – Media, opinion leaders and cybersecurity networked groups

2.2.11 Civil society, NGOs & citizens

Stakeholder group	Description and approach	Size of the target group	Priority multipliers (examples)
11a. Civil society, NGOs		<i>TBC – work in progress</i>	
11b. Citizens		<i>TBC – work in progress</i>	

Table 15: Stakeholder Group – Civil society, NGOs & citizens

2.2.12 Synergies and Multipliers for CYBERWISER.eu dissemination and exploitation

CYBERWISER.eu builds on a strong network of companies, educational institutions and public-sector organisations as the basis for raising awareness of cyber risks and impacts from the very outset of the project and, subsequently, for promoting and exploiting its offering. To this end, the community will be profiled to pinpoint relevant target stakeholders, with recruitment campaigns filling gaps found, e.g. the organisations and professionals related to the pilots, the open pilot stream and other organisations that can benefit from cyber security capabilities.

Early synergies can help define common stakeholders, including targets for the Open Pilot Stream (which will be part of specific communication and recruitment actions), and the co-organisation of workshops and webinars, starting from M6 (February 2019).

Another important component of the Communications Plan is daily engagement with targeted stakeholders through LinkedIn professional networks and through the Twitter social media channel.

As of today, CYBERWISER.eu has already engaged with two relevant EU R&I projects to establish a synergy for the joint dissemination of results and stakeholder engagement (see also Sec. 5):

- **POSEIDON**⁵: focus on vertical industries, such as finance and banking; smart cities (e.g. Santander); government (Austria) and the private sector (e.g. SOFTEAM).
- **DEFENDER**⁶: focus on healthcare and energy.

2.3 Offering

In the early phases of design, particularly during requirements definition, a preliminary scheme for service offering of CYBERWISER.eu was agreed upon among all Partners during the Project Kick-off meeting in Madrid. The service offering envisaged is represented by the so-called "pyramidal scheme", drafted in the figure below. Basically, the scheme identifies a for-paying service layer and a freemium one. More details on which offering is going to be addressed for are provided in Figure 3. The complete definition and stabilisation of the offering is envisaged for the first semester of 2019.

⁵ https://cordis.europa.eu/project/rcn/214840_en.html

⁶ <https://cordis.europa.eu/project/rcn/210231/factsheet/en>

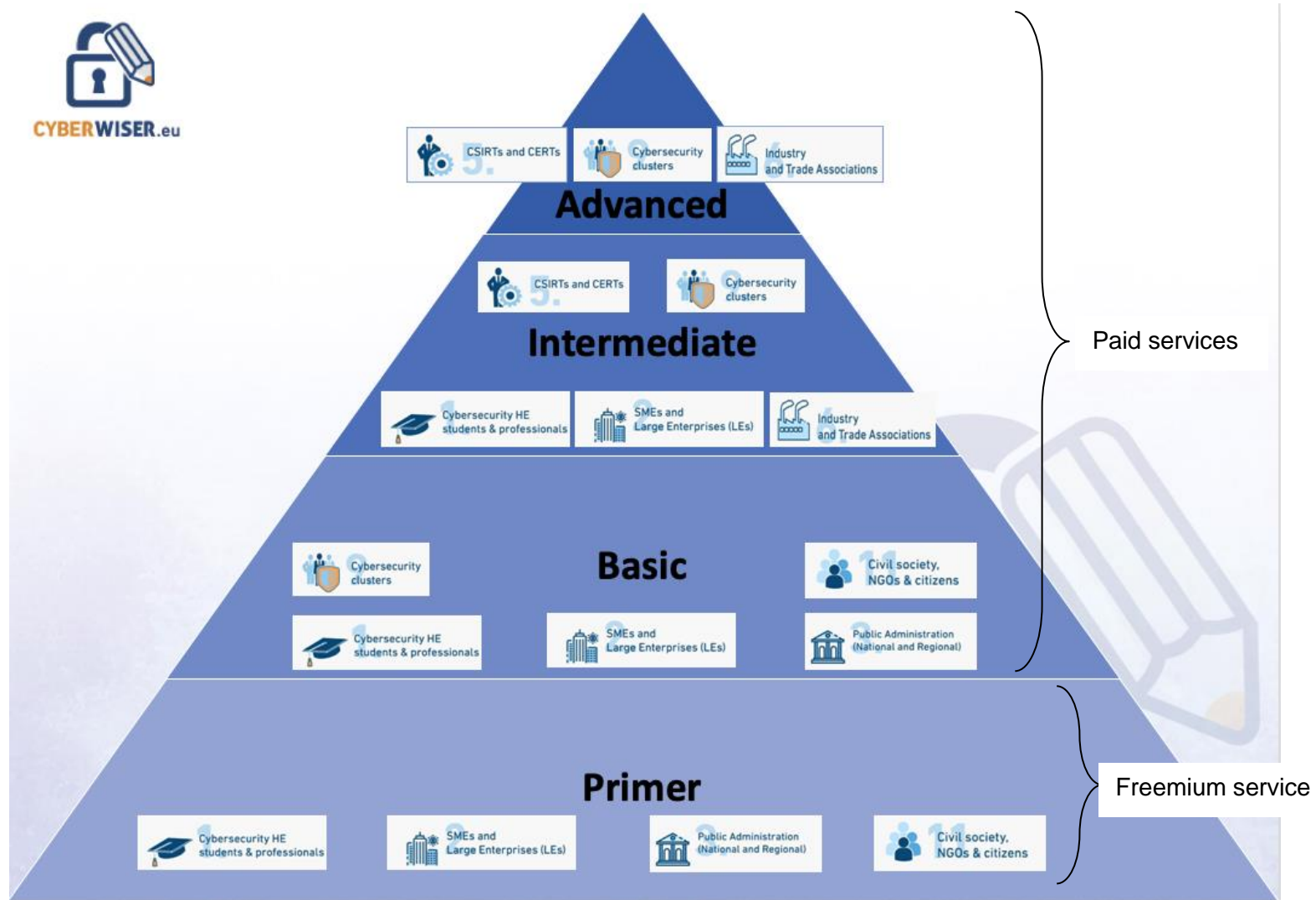


Figure 3: The “pyramidal offer”

In Table 16 below a preliminary exercise of main features available per offering level is reported. The table will be updated according to the results of the technical development activities.

ASSET / PLATFORM VERSION	FREEMIUM	BASIC	INTERMEDIATE	ADVANCED
Web Portal	Available	Available	Available	Available
Cross-Learning facilities	Static courses on cyber risk for non-tech employees Simple cyber competitions in quiz mode Dynamic courses for non-tech people about cyber attacks	Training materials, basic level Guided exercises in static scenarios	Training materials, intermediate level Semi-guided scenarios White team enabled to on-fly scenario modification	Training materials, advanced level Highly flexible scenarios White team enabled to on-fly scenario modification
Training Manager	N/A	Prepared scenarios, no edition, up to 10 elements	Scenario edition up to 50 elements	Scenario edition up to 500 elements
Performance evaluator	N/A	N/A	Evaluation made basing on a limited number of parameters	Extended evaluation capabilities
Digital library	N/A	N/A	Limited representativeness of infrastructure elements	Extended library of network elements
Economic Risk Evaluator	N/A	N/A	Basic suite of economic risk evaluation models and algorithms	Extended suite of economic risk evaluation models and algorithms
Simulated infrastructure manager	N/A	Simple scenarios, low requirements	Small-medium scenarios with medium requirements	Large scenarios with high requirements
Monitoring sensors	N/A	N/A	Automatically deployed in the exercise	Automatically deployed in the exercise
Attack simulator	N/A	Basic suite of available attacks	Intermediate suite of available attacks	Extended suite of available attacks
Countermeasures simulator	N/A	Basic suite of available mitigations	Intermediate suite of available mitigations	Extended suite of available mitigations
Anomaly Detection Reasoner	N/A	N/A	Available to the defender team	Available to the defender team
Vulnerability assessment tools	N/A	Basic version of vulnerability assessment tools	Intermediate version of vulnerability assessment tools	Extended version of vulnerability assessment tools

Table 16: CYBERWISER.eu features vs offering level (preliminary)

It is understood that the details on the levels and their main features will be further shaped up in the course on the following months, as the project developments will unfold, therefore the information above is to be considered as preliminary, although instrumental to develop the next months' communication and dissemination effort of the initiative.

2.4 Channels

CYBERWISER.eu will use various communication channels leveraging on the project partner networks and will produce a set of tailored communication formats targeting different stakeholder groups. The consortium can count on extensive expertise and experience in creating a communication kit with diverse formats and extend the strong network by reaching out to a broad range of stakeholders, media, professional and social channels.

The main channels that will be utilised in CYBERWISER.eu are:

- Website
- Social media
- Events (physical and virtual, e.g. webinars)
- Traditional media
- Other channels

Figure 4 describes the communication channels and the other elements at the basis of an effective communication strategy.

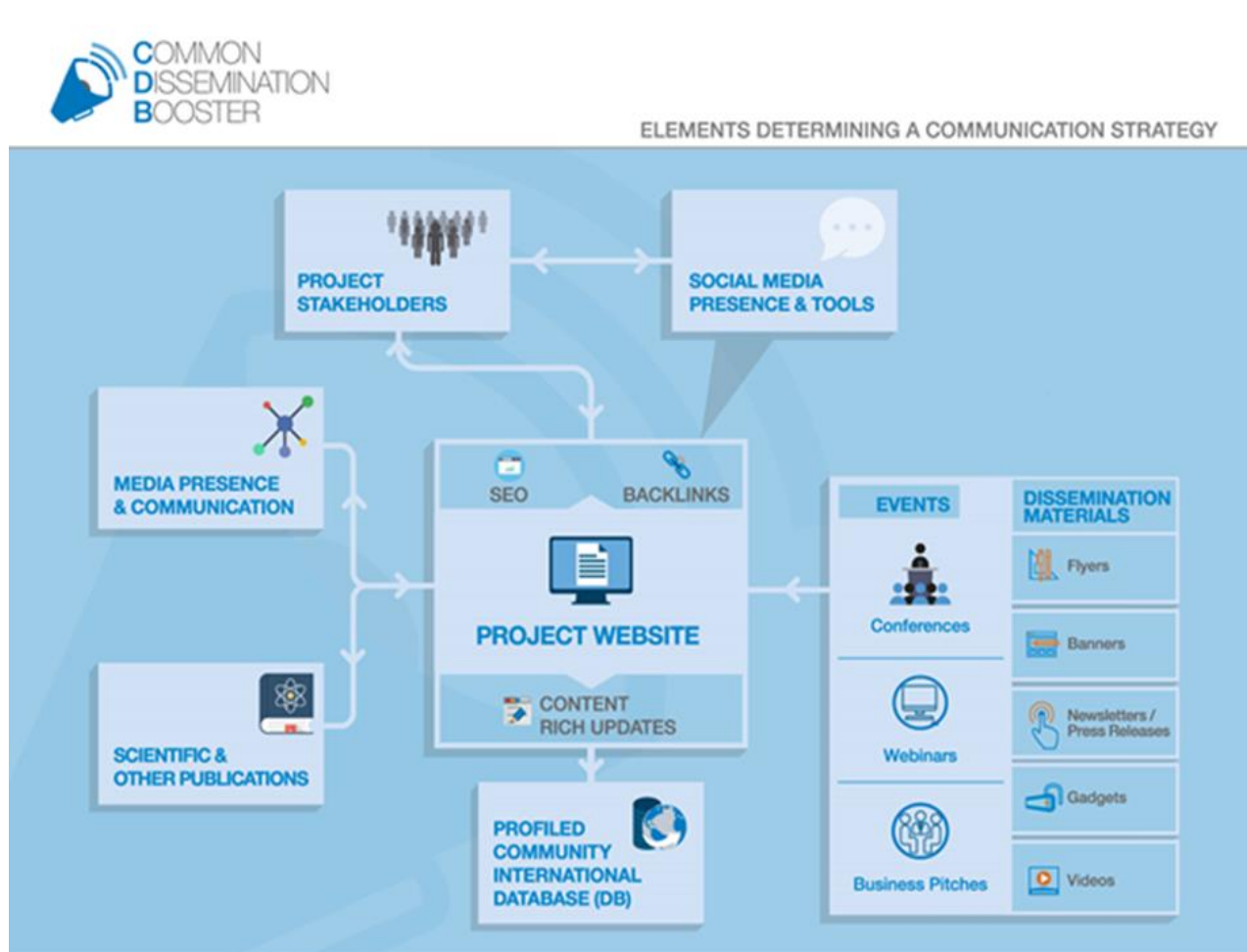


Figure 4: Elements determining an effective communication strategy

The complex lifecycle of the CYBERWISER.eu Innovation Action means putting into motion, at various times and in diverse combinations all the boxes identified in Figure 4⁷. WP6 will ensure all necessary elements are carefully and strategically coordinated so both communication and dissemination can move seamlessly across stakeholder groups and across national borders, including multi-stakeholder engagement, EU and international perspectives.

The following sections give a short description of each channel and how it relates to the CYBERWISER.eu strategy.

2.4.1 Website

The project portal (available at www.cyberwiser.eu since M1) is the central channel of the communication and engagement strategy. The website is GDPR compliant and is updated on a regular basis. It carries forward also all the information assets developed as part of the predecessor initiative, WISER. The website is developed with a Drupal CMS⁸ and is managed by Trust-IT.

Marketing campaigns: leveraging the press & media partner networks as well as the communications experts copywriting skills the project will produce compelling messages, and will be distributing press releases on major announcements and achievements. Operational activities for the Marketing campaigns will include:

- Press Release
- Newsletter
- Promotional Material and Info-graphics
- Video

Operational activities for each Marketing campaign will be further evaluated on a case-by-case basis.

2.4.2 Social media and professional networks

Integration of social media and professional networks like Twitter⁹, LinkedIn¹⁰, Slideshare¹¹, Youtube¹² is a central part of the media platform development. The continuous online presence through prominent social networks will inform, guide and solicit researchers via a growing body of knowledge. An important consideration is that social media accounts require constant updating and monitoring for them to be a real success. All web platform content pieces are designed to allow the user to share content pieces through social media channels.

- Twitter will be mainly used to provide brief real time updates and news and to promote event activities.
- LinkedIn will be mainly used to bring on board new relevant stakeholders, send target messages and to create and follow discussion groups. A key advantage is not only the ability to identify professionals and organisations across sectors and technologies but also the possibility to measure the connection distance across diverse networks, e.g. 1st-degree vs. 2nd degree connections; 2nd-3rd degree and plan recruitment campaigns accordingly.

⁷ www.cdbservices.eu - The Common Dissemination Booster (CDB) a service offered by the European Commission (July 2017-June 2019) that supports all EC-funded, national, and regional projects to maximise their impact & disseminate their projects better.

⁸ <https://www.drupal.org/>

⁹ <https://twitter.com/cyberwiser>.

¹⁰ <https://www.linkedin.com/grps/CyberWISER-8411544/about>.

¹¹ <http://www.slideshare.net/CyberWiser>.

¹² https://www.youtube.com/channel/UC1q_ViOaab1PWgA1uhCaSLQ.

- SlideShare to promote training material and presentations.
- YouTube to upload and store webinars, videos and other audio-visual material.

Social media and professional networks will be combined also with the use of traditional media as relevant to boost visibility and outreach to targeted groups (see Sec. 4.1.4).

2.4.3 Events

CYBERWISER.eu drives engagement with all stakeholders that directly benefit from its offering and with stakeholder that can advocate its role in building the cyber security skills crucial to tackling a fast-paced and increasingly complex threat landscape. Diverse types of events are targeted, spanning CYBERWISER.eu-led and third-party events targeting a range of stakeholders depending on the event strategy and expected outcomes:

1. CYBERWISER.eu events spanning (see also the roadmap reported in Sec. 4):
 - a. 6 webinars.
 - b. 2 hackathons with soft skill pitches and career sessions.
 - c. A final event.
2. 3rd-party-events: Cyber security events also targeting relevant verticals with a dual purpose: 1) raise awareness of CYBERWISER.eu by sharing insights, especially in the early phase of the project and 2) identify leads for new adopters and thus boost the exploitation of results by increasing uptake, especially in phases 2 and 3 of the project (months 10-15; 16-30).
3. Scientific conferences and workshops. In the IA context, such events, often linked to event proceedings or peer-reviewed papers, are a small but important means to confirm results and enhance the reputation of contributing authors in the field. Events are selected based on alignment with event calendars and CYBERWISER.eu proven results/findings. Resulting publications are tracked through WP6 in sync with the project coordinator.

Depending on the level of audience/sector awareness, CYBERWISER.eu will tailor its messages and content of the presentations and panel discussions so they are fit for purpose. Section 4.1.6. provides an example of the stepwise approach CYBERWISER.eu adopts for event promotion and reporting on outcomes and impacts.

2.4.4 Traditional media and other channels

Notwithstanding continual usage of web, social media, and visibility at specialised events, CYBERWISER.eu will also dedicate effort to ensure presence in "traditional media", with the main goal of further expanding outreach, especially to large numbers of European SMEs, Research Centres, Academia, and Citizens.

Among the media that will be leveraged:

- Newspapers and magazines;
- Tech / Specialised publications;
- Newsletters;
- Academic/trade press.

2.5 Motivational mechanisms

To support engagement of the various stakeholders, CYBERWISER.eu strategically pursues a number of pragmatic **motivational mechanisms**. In the following table, such mechanisms are described, highlighting the main stakeholder groups those mechanisms are relevant for.

<i>Motivational mechanisms</i>	<i>Relevant Stakeholders</i>	<i>Description</i>
Mechanism 1 – Open Pilot Scheme	SMEs, Large Enterprises, Universities, Industry and Trade Associations	The Open Pilot Scheme constitutes a fundamental lever to incentivise rapid participation. Interfacing with national agencies and trade associations for policy & decision making will further increase opportunities.
Mechanism 2 – Monetary exposure assessment	Large Enterprises, Public Administration	Demonstrating ultimate savings achievable from usage of the CYBERWISER.EU platform is key to achieving buy-in from selected stakeholders. The monetary dimension of cyber risks that can be simulated in the cyber range environment will further motivate active participation.
Mechanism 3 – Capacity building opportunity	Students & Professionals, SMEs, LEs, and Public Administrations	During project execution, the availability of an initiative aiming to nurture capacity building in a sector gaining so much attention in Europe is going to be a convincing motivational driver to capture the attention and engagement of the targeted, relevant audience.
Mechanism 4 – Reward-driven	Students, Professionals, Public Administrators, SDOs and Certification Organisations	The Cybersecurity Professional Register promoted by CYBERWISER.EU will be a strong driver to raise attention around the initiative and will support the sought-for early adoption of the various elements of the training material and the platform as a whole. Moreover, as part of Task 5.5 "Open Pilots and Awards", other reward-driven initiatives will be carried out.
Mechanism 5 – Access to freely available solutions	ALL	CYBERWISER.EU will provide a unique opportunity for all stakeholders to engage, at various levels, with an EU-wide, open initiative, where user-oriented, pragmatic services and solutions are provided in the field of cybersecurity (also building on the other free services from the WISER project that will be kept available @ www.cyberwiser.eu).
Mechanism 6 – Information-driven	ALL	CYBERWISER.EU will be, for 30 months, a reference, authoritative, independent, information source for Europe's effort in democratising training in cybersecurity . Ultimately, also through its Market Watch activities, increased awareness generated among the stakeholders will support trust and confidence among European Organisations in investing in training and competence development in this field.

Table 17: Motivational mechanisms

In particular, in the first 18 months of the project, while most of the research results will be developed, priority will be given to the following mechanisms (without, however, overlooking the other ones):

- Mechanism 6 – Information-driven;
- Mechanism 3 – Capacity building opportunity;
- Mechanism 5 – Access to freely available solutions (the "Primer" level of the offering);
- Mechanism 1 – Open Pilot Scheme.

2.6 KPI-driven approach

As mentioned, this plan adopts a SMART approach to its continuous communication activities along the 9-month project life-cycle [specific, measurable (KPI-driven), achievable and realistic (based on identified target groups and channels to reach target groups), timely (matched to project opportunities and results) and timed (clear start and end date)].

KPIs that are relevant for communication and engagement are indicated in Sec. 2.1 and in the roadmap (see Figure 11). The roadmap clearly defines a set of 6 macro activities which include more detailed, specific activities that the Consortium will undertake to ensure an effective communication and outreach strategy, spanning across a 15 months period.

3. Project results and Assets for Dissemination & Communication

In following the strategy set out in Section 2, the dissemination, communication and engagement efforts will follow a clear process which can be synthesised as follows:

- A. Identification of a tangible project result ("result");
- B. Definition of its availability date;
- C. Agreement of the dissemination and communication assets on the basis of which to develop the stakeholder engagement activities.

Project results are expected as follow:

- The integrated platform itself;
- The training material produced during the project;
- The publication and dissemination decks produced for the targeted conferences;
- The reward-driven initiatives;
- The results achieved during FSPs.

3.1 Integrated Platform (4 Levels)

At the moment of issuing the present plan, most of the development details are not yet defined. The following tables will be updated as soon as the technical activities of the workplan unfold, producing clear elements (viz. "result names") and therefore leading to dissemination and communication assets to be utilised for communication and stakeholder engagement purposes.

Some ideas that are currently under discussion among the partners include:

- exercises supporting only individual trainees in Basic level and support for teams in higher levels;
- attack and countermeasure simulators could be disabled in the Basic level while maintained in the higher levels;
- emulated infrastructure will be differentiated in terms of requested HW resources (how heavy are your scenarios?) and in terms of complexity of the scenarios;
- different possibilities of the scenarios design could be offered based on the different level of the CYBERWISER.eu offer. For example, in the Basic level the trainer could have small or none possibilities to create a new scenario, but he/she will only be able to select on an existing library of scenarios;
- integration with other systems in an organization (Advanced level only);
- different levels of consulting based on the different level of the CYBERWISER.eu offer;
- training courses/activities/modules separated by each level (and scope) of training, that, upon completion, bring different levels of certificates to the trainees;

These initial discussions will obviously evolve depending on the outcomes of the technical developments and will be further refined and completed in the next iteration of this deliverable. Be that as it may, at this stage and for the benefit of the present Communication & Engagement Plan it is important to have been able to set out the general, analytical methodology that is going to be followed in the months to come.

3.1.2 Freemium level (Primer)

Result Name	Description	Availability date	Partner responsible (TBD)	Dissemination communication asset /
#R1 Informative platform static	Platform includes functionalities to inform non-tech employees regarding cyber risk (static contents).	June 2019	...	<ul style="list-style-type: none"> • Press Release • Demo access • Brochure
#R2 Informative platform dynamic	Platform includes functionalities to inform non-tech employees regarding new kind of cyber-attacks (dynamic contents).	September 2019	...	<ul style="list-style-type: none"> • Press Release • Demo access
#R3 Diffused cyber games and internal competitions	Platform includes functionalities to allow a large number of non-tech employees to answer to simple cyber competitions in controlled scenarios with reward mechanisms.	December 2019	...	<ul style="list-style-type: none"> • Press Release • Demo access • Brochure • Webcast

Table 18: Project results vs Freemium Level of the offering.

3.1.3 Paid level 1 (Basic)

Result ID and Name	Description	Availability date	Partner responsible (TBD)	Dissemination communication asset /
#R1 Integrated platform, Basic level	Platform includes functionalities of scenario generation, etc.	June 2019 (just an example)	RHEA (just an example)	<ul style="list-style-type: none"> • Press Release • Video • Demo access • Brochure • ...

Table 19: Project results vs Basic Level of the offering.

3.1.5 Paid level 2 (Intermediate)

Result ID and Name	Description	Availability date	Partner responsible	Communication Channels

Table 20: Project results vs Intermediate Level of the offering.

3.1.6 Paid level 3 (Advanced)

Result ID and Name	Description	Availability date	Partner responsible	Communication Channels

Table 21: Project results vs Advanced Level of the offering.

3.2 Training Material

There is ample evidence to show that the impacts of a cyber-attack can be disproportionate to the technical skills of cybercriminals. CYBERWISER.eu redresses the balance with a professional training platform with real-world scenarios that can adapt to an evolving and multi-faceted landscape.

The flexibility and ease for adapting the scope and the challenging exercises will make it possible to properly tailor the platform to the specific needs of the users, achieving the pedagogical goals related to the training.

CYBERWISER.EU will make cybersecurity more attractive to more people, enabling trainees to share risks with senior management or board members, with evidence that cyber resilience also comes from cross-organisational engagement, helping define a cyber security incident response plan that also covers business aspects.

Key features include:

- Real-time **student performance assessment, dynamic configuration and adaptation of exercise scope and difficulty**. The academic pilot (Pilot #1) is aimed at proving that the platform meets the challenge.
- Protection of **critical infrastructures** (Pilots #2 and #3) easing the training of highly-skilled cybersecurity experts.
- Easy access to the platform allowing **exercises between teams all over the world**.

Result Name	Preliminary Description	Availability date	Partner responsible	Communication Channels
#R1 Primer Cyber-risk Assessment (Courseware)	This course teaches the trainee the basic concepts related to cyber-risk management, as well as to identify examples of their usage. The trainee will also learn to describe a generic risk	The date of releasing of the Primer level	Content wise: SINTEF	Press release (Cyberwiser Primer), Demo Video, Brochure

Result Name	Preliminary Description	Availability date	Partner responsible	Communication Channels
	management process, explain the purpose of the steps in the process, and relate the basic concepts to the various steps of the process.			
#R2 Basic Cyber-risk Assessment (Courseware)	This course teaches the trainee to associate basic cyber-risk management concepts to a domain-specific risk modelling language and apply the risk modelling language in a generic risk management process. The trainee will do this by analysing basic scenarios (target of analysis) and select and develop basic risk models with respect to the scenarios.	The date of releasing of the Basic level	Content wise: SINTEF	Press release (Cyberwiser Basic), Demo Video, Brochure
#R3 Intermediate Cyber-risk Assessment (Courseware)	This course teaches the trainee to rank identified risks and recommend appropriate risk treatments. The trainee will also be able to describe own risk treatments and associate a cost to the treatment.	The date of releasing of the Intermediate level	Content wise: SINTEF	Press release (Cyberwiser Intermediate), Demo Video, Brochure
#R4 Advanced Cyber-risk Assessment (Courseware)	This course will teach the trainee to analyze real-world scenarios live and investigate the scenarios both from an adversary point of view, as well as a defender point of view. The trainee will be able to select and develop risk models capturing attacks within a real-world scenario, as well as identifying, comparing and selecting appropriate risk treatments in a timely manner within a predefined budget.	The date of releasing of the Advanced level	Content wise: SINTEF	Press release (Cyberwiser Advanced), Demo Video, Brochure, Presentation, Publication

Table 22: Project results in Training.

3.3 Targeted Publications and Conferences

The scientific contribution of CYBERWISER.eu will produce several scientific publications which will be presented in different kind of scientific conference and will be further utilised for dissemination.

A preliminary list of conferences where such contributions can be presented has been agreed upon with the consortium partners:

- Generic scientific conferences:
 - **ISCC 2019**: International Symposium on Computer and Communications. Period and location are not still available;
 - **SMARTCOMP 2019**: 5th IEEE International Conference on Smart Computing. 12-15 Jun 2019, Washington D.C., US;
- Cybersecurity Italian community conference:

- **ITASEC19**: Italian Conference on Cybersecurity. 12-15 February 2019, Pisa, IT;
- ICT Educational conference:
 - **Didamatica**: Conference on ICT Education. Period and location are not still available;
- International cybersecurity educational conferences:
 - **ASE '19**: USENIX Workshop on Advances in Security Education. Period and location are not still available;
 - **WISE 12**: Conference on Information Security Education. Period and location are not still available;
 - **CISSE 23rd Colloquium**: National Colloquium for Information Systems Security Education. 20-12 June 2019, Las Vegas, Nevada, US;
- ICT enterprise cybersecurity conference:
 - **ICT Security Forum 20**: Italian Forum on ICT Security. Period and location are not still available.

The list above will be further expanded and inserted in the document in the upcoming months.

3.4 Awards

With the goal of broadening the pilot user base, the awards will serve as a motivation booster for pilot users. The awarding scheme ranges from badges to more tangible awards, such as the CyPR – Cybersecurity Professional Register.

Three types of badges will be the "Pioneer Badge", the "Best Trainee" award for professionals and the "Best Student" contest for higher education students.

Other reward-driven initiatives will be developed too: a "sandbox" instantiation of the CYBERWISER.EU platform will be set up and maintained to support the early adopters.

- The CYBERWISER.eu **Cybersecurity Professional Register (CyPR)**: A new instrument created by CYBERWISER.EU, to support and promote cybersecurity capacity building in Europe. It will support formally trained cybersecurity professionals. The Register will represent the needs of the public and private sector, with users coming from industry and academia.
- Badges: Pioneer usership badges (Pioneer Badge, Best Trainee, Best Student).
- Other reward-driven initiatives will be developed.
- More initiatives will be considered as the project activities pan out.

CYBERWISER.eu will carry out large-scale promotional campaigns for end-user recruitment and outcomes, with dedicated press releases, newsletters and personalised invites to relevant community members across diverse networks.

3.5 Full Scale Pilots (FSPs)

CYBERWISER.eu runs three (3) **Full-scale Pilots (FSPs)** in key verticals (energy and transportation) and in education, in the specific context of a university master course but generally targeting diverse students of computer science. A key goal is ensuring pilots, through their engaged user panels, test CYBERWISER.eu across diverse attack scenarios and triggers that are as close to real life, simulating the impact of what might happen in the real world, including new scenarios and cyber threats in a way that ensures cost and time effectiveness.

The pilots will validate the real-world value of the multi-purpose platform to skill students and professionals and show how it meets the needs of end-user stakeholders from public (pilot #1) and private organisations

(pilots #2 and #3). With the Open Pilot Stream and the on-boarding of other users, CYBERWISER.eu will help close the cyber security talent gap in Europe.

The three full-scale pilots brought by CYBERWISER.EU will cover the needs of a wide range of end-users, spanning students with a strong interest in building a career in cybersecurity to experienced IT experts who need to ensure they are properly equipped for a multi-faceted threat landscape. CYBERWISER.EU will also meet the specific needs of a broad range of verticals through platform roll-out to the **Open Pilot Stream**. The Open Pilot Stream will also prove the applicability of the platform to public and private institutions, which will be targeted to actively utilise the CYBERWISER.EU platform.

A synthesis of the communication and engagement approach to each of the 3 FSPs is reported in the tables below.

Full-Scale Pilot #1		Professional and academic training: Computer Engineering, Embedded Computing Systems and Telecommunications University of Pisa (UniPi)
Overview		<p>This pilot focuses on user experience and the scalability features of the platform. The diversity of the experiments that a university would require---from elementary ones for BSc, through to more complex ones for MSc and post-graduated users, up to research-oriented for PhD students- will demonstrate the flexibility of the platform. The experiments will thus encompass the entire education chain, providing valuable validation evidence and feedback.</p> <p>Outcomes are expected to fill the gap concerning the high demand of cybersecurity professionals, combining broad technical skills with security expertise and an understanding of business risk – and the difficulties in finding them.</p>
Definition and Engagement User Panel	and with	<p>Activities to support engagement will take care of the fact that, considering that the panel will be comprised of students (undergrads + grads) and master students (mostly professionals), particular care will be taken to engage those target users with the special motivation coming from the innovative element of the training platform they are going to be part of.</p> <p>The resources brought by UniPi, both in terms of computer labs and related IT services, provide an experimental environment for investigating the platform scalability. The computer labs make it possible to accommodate a large number of students: platform user services make it possible to host the platform and, at the same time, monitor a number of performance factors that constitute valid indicators of the platform performance and scalability.</p>
Communication and dissemination of pilot developments		<p>Communicating the value for the entire education chain, spanning many interdisciplinary aspects, with students from Computer Engineering, Embedded Computing Systems and Telecommunications and at diverse stages in their education, namely from BSc through to MSc, up to PhD and a post-graduated programme in Cyber-security.</p> <p>Disseminating results such as enhancing and complementing common teaching approaches by letting students experiment with increasingly complex systems and situations, from base levels of defence (e.g., firewalls and intrusion detection systems), through to more complex networking environments up to realistic attack and defence strategies, validating and demonstrating the high flexibility of the platform, which is of paramount importance in an academic environment. Thus, demonstrating the versatility of the CYBERWISER.EU platform.</p>

Table 23: FSP#1 on Professional and Academic Training

Full-Scale #2	Pilot	Railroad transportation Ferrovie dello Stato (FFSS)
Overview		<p>Proving the potential and added value of the platform in a scenario of business and cyber security experts from the rail transportation vertical.</p> <p>The ambition of Pilot 2 within FFSS is to transform their current SOC into an advanced training and awareness system for Junior Team Members, Risk Management staff and Middle to Top Managers involved with highly dependent IT Businesses and Operations, thus ensuring all-important engagement with management personnel having vital knowledge about business risks.</p> <p>The pilot aims to "close the gap" between cybersecurity experts and decision makers, showing the latter, in an easy to understand environment, what are the values at risk during an attack and how the cybersecurity team can react. By using the CYBERWISER.eu platform, the business experts will be able to understand the costs of a set of countermeasures and estimate cost/benefit scenarios.</p>
Definition and Engagement User Panel	and with	<p>Specific scenarios created in the platform will cover the security requirements of this pilot. The cybersecurity team will use the platform to perform attack and defence scenarios, while business experts will use the platform to understand the threat posed to critical assets in monetary terms (cost of a business interruption, cost of a data breach, and cost of replacing a damaged logical asset).</p> <p>FSP#2 will have basically 2 panels to engage: a highly technical one, which will be treated mostly like the EDP panel (highly skilled FFSS employees to be engaged on a one-to-one bases, with the support of the FFSS pilot management team) and a much more fundamental level one, which will be mostly directed to the "Primer" level of the offering and will actually correspond much closer to an "open panel", and therefore the engagement there will follow a strategy more similar to the one given to the general target audience of CYBERWISER.eu (with a lower specialised profile). This part of the panel is in development and will be defined in the early months of 2019.</p> <p>For the technical part of the panel, FSP#2 will involve 3 to 5 cybersecurity experts, 1 to 3 risk managers and 2 to 5 business users of the digital assets chosen for the cyber game. Ferrovie dello Stato will use its Cyber Security Operation Center (SOC) including a physical room for the simulation and SOC software, hardware, and connectivity infrastructure. The SOC is designed to: (1) protect mission-critical data and assets, (2) prepare and respond to cyber emergencies, help ensure continuity and efficient recovery, and (3) fortify the business infrastructure.</p>
Communication and dissemination of pilot developments		<p>Communicating the socio-economic impacts of cyber-attacks, the importance of cyber risk management and value of CYBERWISER.eu also from a business perspective.</p> <p>Supporting technical partners in disseminating advances in the field, including impacts for this vertical.</p>

Table 24: FSP#2 on Transport Infrastructure

Full-Scale #3	Pilot	Energy generation and distribution: protection of critical infrastructures EDP
Overview		<p>Deploying advanced training modules, increasing the automation of training operations and using gamification to make the training modules more effective.</p> <p>The main purpose of the pilot is to confirm new developments in training scenarios, bringing EDP's knowledge of critical infrastructures and Cyber Range operations, which may then be adopted by other entities in their own environments.</p>
Definition and Engagement User Panel	and with	<p>The panel being mostly internal to EDP (EDP employees), the engagement will be performed in close collaboration with the EDP pilot management team.</p>

Full-Scale #3	Pilot Energy generation and distribution: protection of critical infrastructures EDP
	<p>Three (3) Blue Teams for critical infrastructures: Generation/Distribution/Business Support systems, with knowledge of electrical grid infrastructures and a working model of a thermal power plant (including a water drum, boiler and turbine), a substation and protection gear simulation model, and an EMS (Energy Management System) to ensure remote control over the Generation/Distribution equipment.</p> <p>EDP also has a highly skilled team for supporting the use of security software for monitoring and detecting cyber-attacks, and reacting to security incidents through counter-measures and forensic analysis.</p> <p>The goal of the trainees (Blue team) is to: protect mission-critical data and assets, prepare for and respond to cyber emergencies, ensure business continuity and efficient recovery and enhance the security levels of the business infrastructure. The White Team oversees the trainings, while the Red team performs a set of attacks detected by the blue team. The aim is to understand the threat posed to the energy value chain.</p>
Communication and dissemination of pilot developments	<p>This pilot aims to increase current trainee satisfaction at least 10%. EDP is already checking satisfaction scores through questionnaires at the end of a session and can adopt a similar approach for CYBERWISER.eu.</p> <p>Communicating benefits and impacts through relevant CYBERWISER.eu networks and synergies. Disseminating impacts (e.g. reduced OPEX costs) and user testimonials; supporting technical partners in their dissemination of CYBERWISER.eu results, such as impact evident in two variables, namely reputation and cash. Each decision or evidence found can reduce or add to reputation, which has an influence on the cash flow of the company.</p>

Table 25: FSP#3 on Energy Infrastructure

4. Communication and Dissemination Plan

To support its goals and generate impact, CYBERWISER.eu implements a 30-month communication strategy aimed at supporting the dissemination and exploitation goals and targets of the project, coordinated under WP6 – Communication, Community Development, Policy and Go-to-Market, drawing on extensive practical know-how and experience within the CYBERWISER.eu consortium.

Throughout the 30-month duration of the project, all CYBERWISER.eu partners have effort to contribute to community development and stakeholder engagement on a continuous basis as part of the project's communication plan. Having an effective communication plan is key to paving the way to dissemination and exploitation of results, to which all partners have committed according to availability dates and beyond the project lifecycle.

Assets to support both goals include an already strong networked community developed by WISER. Moreover, CYBERWISER.eu benefits from having an influential **Stakeholder Expert Board (SEB)**, which it can tap into

The various stakeholder groups defined in Sec. 2 will be targeted by means of a number of engagement activities and campaigns aimed at awareness raising and recruiting new adopters, e.g. through the Open Pilot Stream campaign. For each of the stakeholders group, CYBERWISER.eu is carrying out a mapping exercise (in terms of defining which means is the one best suited for the selected group) for recruiting new community members and ensuring interaction through social media and networks, examples include:

- ✓ Press/Media outlets and journalists (specialised; national; local).
- ✓ Events & Trade Fairs (on cyber security; targeting specific sectors and themes), using an already-known channel that has proved effective in the past.
- ✓ Relevant initiatives/projects/strategic alliances in Regional/National/European/International levels.
- ✓ Social Networks (covering cyber security issues; targeting specific stakeholder groups) and including LinkedIn groups.
- ✓ Multipliers (relevant to stakeholder engagement goals).

Partners have an exceptional international network, AON alone have regular liaisons with their multiple EU offices. Trust-IT runs several relevant networks with highly targeted stakeholders, such as security and privacy (e.g. cyberwatching.eu; CLARUSECURE) and 5G (5G-ENSURE; Global5G.org). Such direct links will be a real booster for extending the network and meet the challenging business goals of the project in a fast-paced landscape.

4.1 Plan for boosting CYBERWISER.eu Stakeholder Engagement and Visibility

A number of elements will be leveraged to support engagement, as reported in the following sections.

4.1.1 Starting Point: The CYBERWISER.eu Community

Building on its predecessor WISER, CYBERWISER.eu has already started to expand existing community thanks to:

- Partner efforts;
- Web platform registration;
- Social networks;
- Participation in events.

- Organisation of events;
- Synergies and strategic collaborations.

At the time of writing, CYBERWISER.eu has a community network of **1,833 members** (Overall Twitter and LinkedIn professional network: 1,515 – Registered users: 308) spanning across very different profiles such as:

- IT Specialist/IT Architect.
- Researcher/Scientists.
- Advisor/Consultant.
- Chief Security Officer (CSO)/Chief Information Security Officer (CISO).
- CEO/Managing Director/Chief Executive.
- Programme Manager/Project Manager.
- Chief Technology Officer (CTO)/IT Director.
- Professor.
- Journalist/Editor/Copywriter.
- Policy development manager/Policy Consultant.

A continuous effort of community monitoring is performed by Trust-IT and circulated every month (or higher frequency) to all Consortium Partners.

4.1.2 Stakeholder Expert Board (SEB)

Stakeholder engagement within CYBERWISER.eu is also supported by its Stakeholder Expert Board (SEB).

One of the main advantages of having the SEB is access to expert insights that can be tailored to different targeted stakeholders, helping CYBERWISER.eu to create enticing content with its own unique value add. The SEB will also be influential in steering the content strategy in the right direction. The SEB can also provide strategic advice on the project's exploitation of results and drive towards sustaining its most market valuable assets.

4.1.3 Samples of additional levers for reaching end-users and other stakeholders

Additional Engagement Levers

ICT and Cyber Security Groups LinkedIn groups - Information Security (428K members); Cyber Security Forum Initiative – CSFI 86K. Multipliers and clusters - Cyber security clusters, e.g. Finnish Information Security Cluster, AEI Seguridad. CITIC, @SecTest9 (security testing); @SecurityNews6; @InfoSecurity99; @CyberSecUpdate; @cybersec_cl; @SecurityDialog

SMEs: Over 130 connections to business and trade associations across EU, e. Digital SME Alliance; ANITEC, ASSINTEL, ISME, CONETIC, CLUSIT; ICT-HU, TechUK, FSB, Federal Association of ICT-SMEs of Germany, Digital Catapult. Over 20 large industry associations and forums.

Global Telecommunications industry: vendors and operators (350+); Industry 4.0, IIoT, & SMEs and Vertical Industries (300+);

Health (SME supply side, healthcare facilities) Professional LinkedIn groups, e.g. Innovations In Health, Health 2.0, Digital Health, Medica. Media: Health IT Central, HealthTech Wire, Insights. @digitalhealth2 (industry-leading website for NHS & digital health news). Events: World of Health IT (WoHIT), 21-22 November 2017.

Additional Engagement Levers

Manufacturing Factories of the Future (manufacturing companies). Synergies with FoF projects: ICT Innovation for Manufacturing SMEs (I4MS); BEinCPPS, Fortissimo 2, HORSE, I4MS-Growth, ReconCell, XS2I4MS. Media: [@TheEngineerUK](#) (aerospace, automotive, chemical, electrical, electronics).
Transportation (airports, ports, train companies, haulage companies) The Transport Association (UK), Association for European Transport. [@Transport_Assoc](#), [@EuTransportConf](#), [@CENIT_Research](#)
Events: European Transport Conferences

Table 26: Additional levers for engagement

4.1.4 Media and professional levers

Stakeholders, especially potential customers, will be reached through the most relevant media channels, drawing on extensive media relations and journalistic skills within the consortium, including the examples in Table 27 below.

Media and professional levers

IT and Security Media: Computer Weekly, Tech Target & Search Security; Business Cloud News; Cloud Computing Intelligence Magazine; Cloud Pro weekly newsletter; Computer World (security section); Global Security Mag; TechWeekEurope UK; Security Info Watch; Security Week; Threat Post; The Register; IT Briefcase; CIO; Cyber Defense Magazine; SC Magazine; Info Security; CSO Online; Financial Director; Risk Management Professional; Strategic Risk; The Actuary.

Table 27: Sample of Media Channels

4.1.5 Content-driven approach







The communication and dissemination plan will concentrate its efforts around copywriting and it will be the **CONTENT** that will make the difference, which needs to engage, stimulate and interest so much so that readers cannot get enough of the event's outputs that aim to have pragmatic, uptake by a group of end-users – this is the tangible outcome that classifies if an activity has been successful or not. Figure 5 below provides a recent, real example of precisely this.

Coupled with the CYBERWISER.eu web presence, the continuous activity of populating a profiled, international **community database**, will be pursued. The DB will be made up of the stakeholders of the initiative (the first priority of users), then the secondary stakeholders, where the funding agencies or regulatory or policy members could sit and then relevant other stakeholders, who all make up part of a: "massaged, profile-oriented, and aggregated community database".

One asset that CYBERWISER.eu can leverage is the WISER cartography and its revamp. The overriding goal is to turn the cartography into a niche product with increasing attention to its offering in an updated cyber security context.

4.1.6 Step by step promotion of events through its outreach channels

Typical examples are given below of **event promotion** carried out for similar projects. Emphasis is given to the "human factor" hence images of the presenter. In the specific case of CYBERWISER.eu, a set of images of the pilots with a live feed of interesting outputs will be featured. The idea will be to perceive the complete lifecycle and promotion of an event, from pre-, during-, and post-event activities.

<h3>Pre-Event</h3> <p>ATMOSPHERE @AtmosphereEUBR</p> <p>Tomorrow, #ATMOSPHERE, through its European Coordinator @iblanque will be presenting in the #DI4R2018. If you'll be at the @DI4R_eu then join our Computing Services Session where we will be the first to present among several projects atmosphere-eubrazil.eu/digital-infras ...</p>  <p>DIGITAL INFRASTRUCTURES RESEARCH 2018 ATMOSPHERE European Coordinator Ignacio Blauque presents ATMOSPHERE Computing Services Session Part I Wednesday, 10 October, 10:30AM</p> <p>1:50 AM - 9 Oct 2018</p> <p>1 Retweet 6 Likes</p>	<h3>Live Coverage</h3> <p>ATMOSPHERE @AtmosphereEUBR</p> <p>Ongoing, the #DI4R2018 presentation of @iblanque where he presents ATMOSPHERE at the Computing Services Session. Here's what we will produce: a hybrid federated VM and container platform, trustworthiness frameworks and a pilot use case on medical imaging processing</p>  <p>12:49 PM - 10 Oct 2018</p> <p>1 Retweet 4 Likes</p>	<h3>Live Coverage</h3> <p>ATMOSPHERE @AtmosphereEUBR</p> <p>The problem that ATMOSPHERE addresses: #SensitiveData, #TrustworthyCloud #Privacy, #CloudSecurity, #DI4R2018</p> <p>ATMOSPHERE The problem</p> <p>I'm building a classifier that can segment and monitor for a high computing demand. One drawback, I want to run service securely and with a Quality of Service.</p>  <p>12:53 PM - 10 Oct 2018</p> <p>1 Retweet 4 Likes</p>
<h3>Conclusion</h3> <p>ATMOSPHERE @AtmosphereEUBR</p> <p>Thanks for those who attended the #DI4R2018 Session on #ComputingServices and saw the presentation of @iblanque on ATMOSPHERE. If you want to get in touch, reach out here or through our details below!</p>  <p>Don't miss a beat! REGISTER FOR THE NEWSLETTER www.atmosphere-eubrazil.eu/user/register Contact: ignacio.blauque@ec.europa.eu Francisco Rodriguez - francisco.rodriguez@ec.europa.eu</p> <p>1:25 PM - 10 Oct 2018</p> <p>1 Retweet 3 Likes</p>	<h3>Immediate Follow-up</h3> <p>ATMOSPHERE @AtmosphereEUBR</p> <p>#DI4R2018 friends: We've just posted the slides to ATMOSPHERE's presentation by @iblanque during the #ComputingServices Session. Take a look: atmosphere-eubrazil.eu/atmosphere-dig ...</p>  <p>3:36 PM - 10 Oct 2018</p> <p>4 Likes</p>	<h3>Speaker Interview</h3> <p>ATMOSPHERE @AtmosphereEUBR</p> <p>European Coordinator @iblanque presented during #DI4R2018 & reported that since project is now halfway through, it's now looking for synergies, collaborations and adopters of its #cloud #trustworthiness project results. See the presentation here: atmosphere-eubrazil.eu/digital-infras ... #H2020</p>  <p>Ignacio Blauque ATMOSPHERE European Coordinator</p> <p>3:44 PM - 10 Oct 2018</p> <p>3 Retweets 3 Likes</p>
<h3>LinkedIn Announcement</h3>		

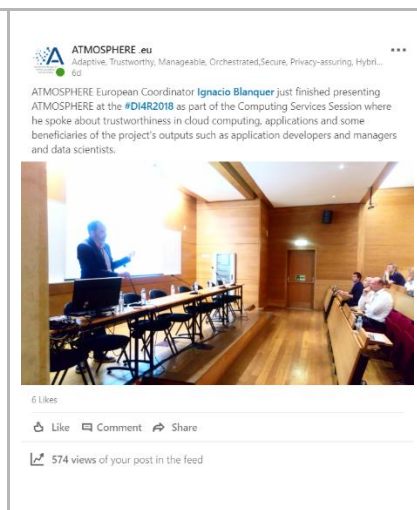


Figure 5: Event promotion

An effective communication & dissemination strategy follows a rigorous weekly and monthly timeline which is closely monitored. An example of a monthly timeline that has been created for the project Kick Off Meeting is reported below. The timeline below has been further developed in the Roadmap described in Sec. 4.5.

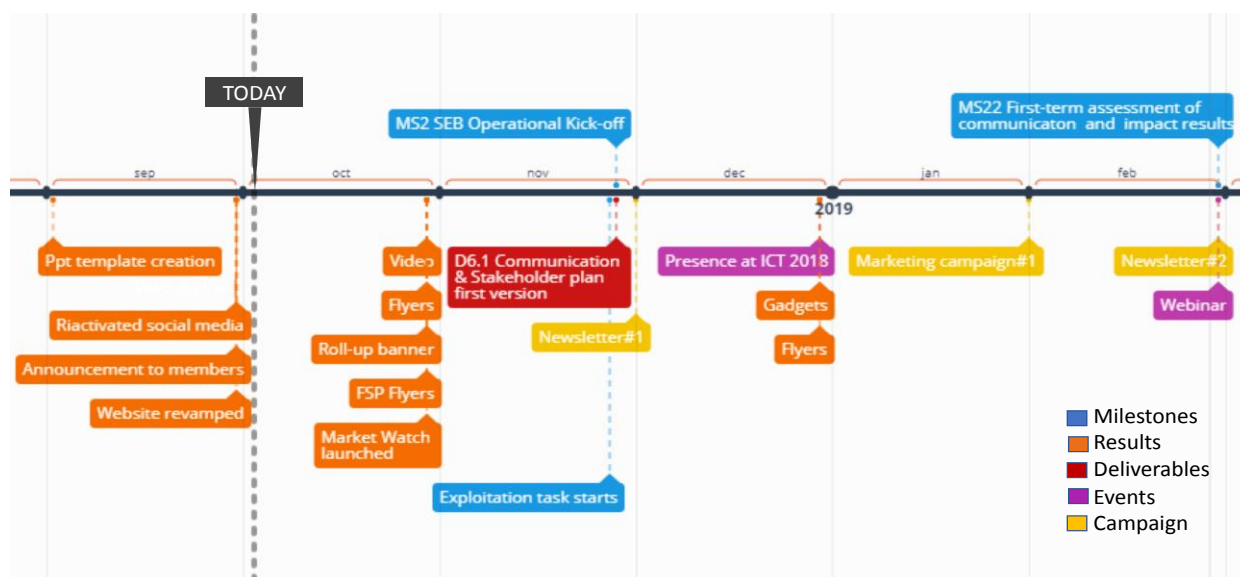


Figure 6: First 6-month timeline as presented at the kick-off meeting (Madrid, 3-4 October 2018)

4.2 Examples of messaging and value proposition

In line with current trends, CYBERWISER.eu's social media activities are focused on actionable, goal-oriented, highly-visual, content-rich posts that combine insightful, yet concise text content, hashtags, engaging images and videos.

For example, the short post below focuses on the positive impact of CYBERWISER.eu in the creation of new career opportunities and reduction of cyber risks, the image helps to visualise and gain a better idea of its benefits for the main end-user group and other stakeholders.



Figure 7: post on the social platform Twitter

Some of the targeted messages aim to disseminating results on upcoming opportunities, such as in the Open Pilot Stream, offering at the same time an overview on the current state and the possibility to join the platform by becoming an early adopter. The messages in the example below are enhanced by the difference of colours in the image that immediately catches the reader's attention.

CYBERWISER.eu @cyberwiser · 31 ott

Great to see interest in our Open Pilot Stream already coming in from #EU companies. If you would like to become an early adopter of the CYBERWISER.eu #cyberrange platform just fill in the form: ow.ly/6JRg30mrDv5

Figure 8: post concerning the Open Pilot

The activities on the various social media channels will also be supported by press releases, such as the one recently published in the News section of the website. While the simple posts with text and visual are meant to have an immediate impact in terms of creating interest, press releases deliver great results also for targeting the specialised journalists and other multipliers.

The fact of publishing the press release on social platforms such as LinkedIn, populated by a lot of SMEs and potential stakeholders, is a great advantage as it allows interested readers to find out more by even just having a short look at the article.

An effective press release campaign offers the chance to underline the attributes of CYBERWISER.eu to anyone who gains interest by reading about it in the shorter posts, and it also involves important SEO benefits, thereby increasing traffic to the website.

CYBERWISER .eu posted this



Figure 9: Press Release published on LinkedIn

4.3 Visibility at events

For events planning, as outlined already under Section 3.3 Targeted Publications and Conferences, the consortium will understand, through a shared online events document available to all partners, what events represent the best opportunity for the project. The "events file" of CYBERWISER.eu will include at least:

- Who is going to attend, where & when;
- What is going to be presented (Overview of presentation/topic);
- Type of audience/stakeholder & approximate number (to support in reporting activities);
- What Graphical material & details for shipping is needed.

- **Event promotion**

In the promotion of events, we include several social media activities:

5+ Months prior to an event

- Even as the event is being conceptualised, we already put up a "Save the date" post
- Formulating an official hashtag for future posts
- Custom social media banners promoting the event
- Setting up a pinned tweet usually with the announcement news about the event

3 Months leading up to the event

- Official event announcement (following a general agenda structure and venue)
- Setting up tracking links for event links to be promoted on social media
- General event video
- Promotional posts
- Event updates: registration opening, early bird rates, extensions, agenda updates, logistics.

As part of the communications plan Trust-IT takes care to: timely **publish the event** on the website; **publish the presentation slides**; set up a dedicated **Social Media campaign**; this allows additional visibility for partners and the project.

Event Name	Date	Location	URL
1st Transport Cyber Security Conference	23/01/2019	Lisbon, Portugal	https://www.enisa.europa.eu/events/first-transport-cyber-security-conference/first-transport-cyber-security-conference
Secops Europe	23-24/01/2019	Budapest, Hungary	https://secops-europe.com/
TEISS 2019	12-13/02/2019	London, UK	https://teiss.eu/
The Future of Cyber Security Europe	19/03/2019	London, UK	https://cybereurope.events
ITALIASSEC	14-15/05/2019	Rome, Italy	https://cyberseries.io/italiassec/
Cyber Incident 2019	3/06/2019	Oxford, UK	https://www.c-mric.com/ci2019
Cyber Security Summit Belgium	12/06/2019	Brussels, Belgium	https://cyber-security.heliview.be/
SECURITY 2019	16-28/07/2019	Prague, Czech Rep.	http://www.secrypt.icete.org/
ARES Conference	26-29/08/2019	Canterbury, UK	https://www.ares-conference.eu/conference-2019/
ISGT Europe	29-02/10/2019	Bucharest, Romania	http://sites.ieee.org/isgt-europe-2019/
Cybersecurity for Critical Assets Europe	01-02/10/2019	London, UK	https://www.cs4ca.com/europe/
Cybersecurity week	2-5/10/2019	The Hague, Netherlands	https://www.cybersecurityweek.nl/
Cybersecurity Europe	9-10/10/2019	London, UK	https://www.cybersecurity-europe.com/
DSS ITSEC 2019	TBA	Riga, Latvia	https://www.dssitsec.eu
13 ENISE	TBA	Léon, Spain	https://www.incibe.es/enise
Cybercamp 2019	TBA	Malaga, Spain	https://cybercamp.es

Table 28: Target events (2019)

4.4 Monitoring

The WP6 Leader will set-up a **Monitoring Service** to measure the impact achieved by the communication activities carried out to support CYBERWISER.eu. Through partner-consortia-in house data science expertise combined with our communications competencies, the partners shall monitor KPIs that allow us to gauge the effectiveness of our campaigns and make necessary adjustments where necessary. A sample dashboard that will be set-up for CYBERWISER.eu is reported in the figure below.

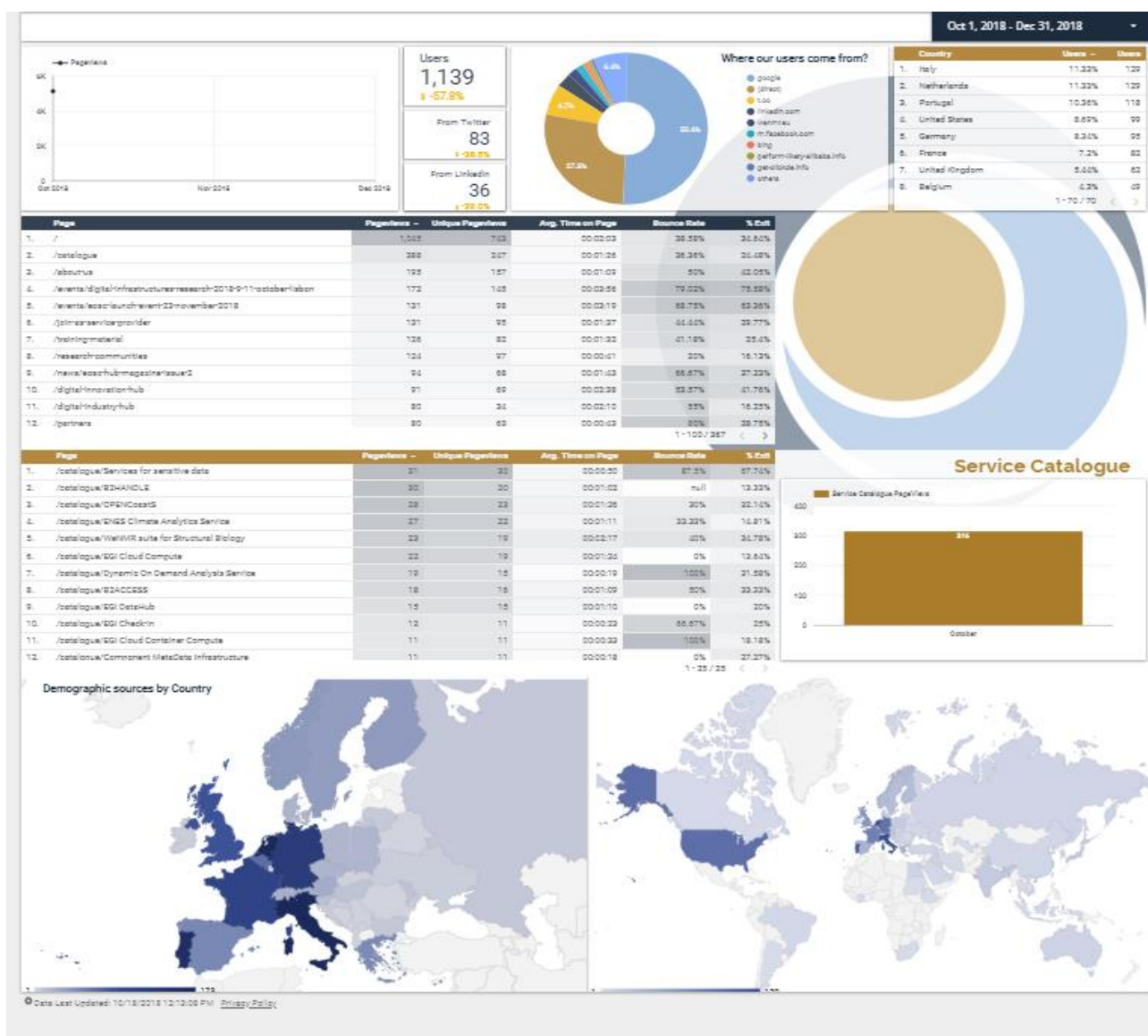


Figure 10: Typical Monitoring dashboard

4.5 M3-M18 Roadmap

Any communication and dissemination plan should follow a regular roadmap with identified actions that may be tracked, monitored against the main KPIs of WP6, the following table provides a first draft roadmap from month1 to month 18.

Macroactivity	Specific activity	Current status	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18	End-of-project value
			Dec-18	Jan-19	Feb-19	Mar-19	Apr-19	May-19	Jun-19	Jul-19	Aug-19	Sep-19	Oct-19	Nov-19	Dec-19	Jan-20	Feb-20	
1. Multimedia material production and distribution	Marketing Campaign	0				X			X			X			X			7
	Press Release	1	X						X			X			X			May vary (Min. 6)
	Newsletter	0	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	26
	Promotional Material and Infographics	2	Continuative action - May vary based on number of events attended															May vary based on specific events attended (Min. 6)
	Video	1						X										3
	Distribution to traditional media	0	Continuative action															Continuative action
2. Social media presence & Community	Tweets	40	Continuative action															TBD
	LinkedIn Post/Article	10	Continuative action															TBD
	Twitter Followers	23	Continuative action															3000 by M30 (LinkedIn included)
	LinkedIn Connections	10	Continuative action															3000 by M30 (Twitter included)
	Overall Community	1825	Continuative action															5000 by M30
3. Events	3rd Party events	0	Continuative action - See Events Timeline for more details															50
	Webinar	0	X-?	X			X				X				X			6
	Hackaton	0											X					2
	Co-located Workshops	0										X						4
4. Synergies	EU CERTs/CSIRTs/National Cyber Security Centres	0					X				X			X				10
	National, EU or international level	1					X				X			X				5
	ECSC	0					X				X			X				TBD
5. Dissemination of technical results through peer reviewed conferences and papers	Presentations	0	Continuative action															Min. 4 scientific conferences
	Publications	0	Continuative action															Min. 4 scientific conferences
6. Website	N° of monthly visitors	1035	1035															3000/month
	N° of clicks on training platform	0																200 by M30

Figure 11: Roadmap of the communication & stakeholder plan (M4-M18).

5. Achievements to-date

CYBERWISER.eu has carried out continuous communications from the very outset, setting up the media platform (www.cyberwiser.eu) and social networks, creating collaterals and creating media campaigns on the project launch. This section provides some details on those activities carried out in the first 3 months of the project.

5.1 Branding

A complete brand image for CYBERWISER.eu has been consolidated in the first weeks of project activities (the logo was developed at proposal writing time and the url cyberwiser.eu was already active, as it has been carried-over from the WISER initiative (2015-2017)).

Concerning the logo, various formats have been created for use in different contexts (social media, website, printed material).

The project branding (see below for extended logo & pay-off and simple logo) is aimed at ensuring a distinctive look and feel across a broad set of communication tools spanning posters, fliers, pop-up banners, the web platform graphics, etc., to facilitate the communication of CYBERWISER.eu target messages to the various stakeholder groups.



Figure 12: CYBERWISER.eu branding

The mission of the project has been consolidated to the following one:

*CYBERWISER.eu will provide a **simulated environment** to create cyber incident and cyber attacks scenarios where both **students and IT professionals** evolve their skills and continuously evaluate their performance, getting ready for future real attack episodes.*

As part of the branding effort, a standard PPT Template has also been developed, to be used by partners when attending events or circulating CYBERWISER.eu-related presentations.

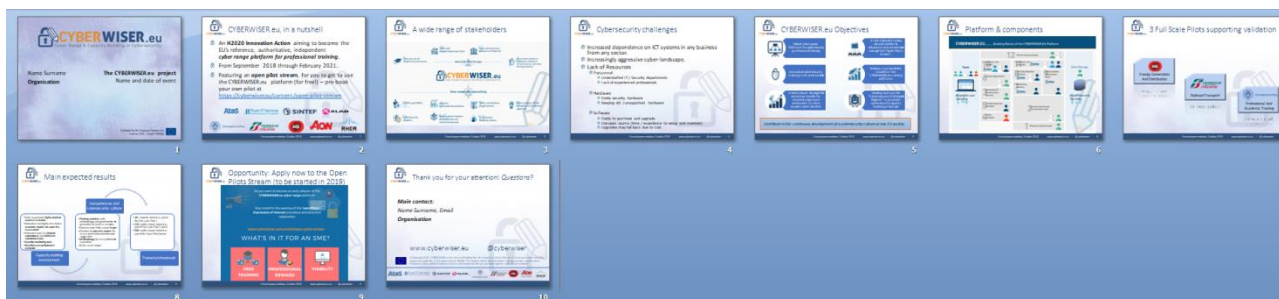


Figure 13: Standard PPT Template

Likewise, the standard deliverable template has been consolidated: It is the one utilised for the present document and it will be utilised for all future deliverables of CYBERWISER.eu.

A first official presentation of the project has been developed by the WorkPackage Leader and uploaded in the project repository, for all Partners to utilise at will.



Figure 14: Cover and second page of the first version of the CYBERWISER.eu ‘Overview Presentation’

5.2 Website (operational since Month 1)

The CYBERWISER.eu url, www.cyberwiser.eu, will be the unique access point for all the tools and services that will be developed during the project. This policy has expressly agree-upon from project onset and it will be maintained throughout project duration. As the initiative will progress, with more results, pilots, and services

being developed, the web platform will ensure access to users already registered on the Platform, possibly through a single-sign-on solution.

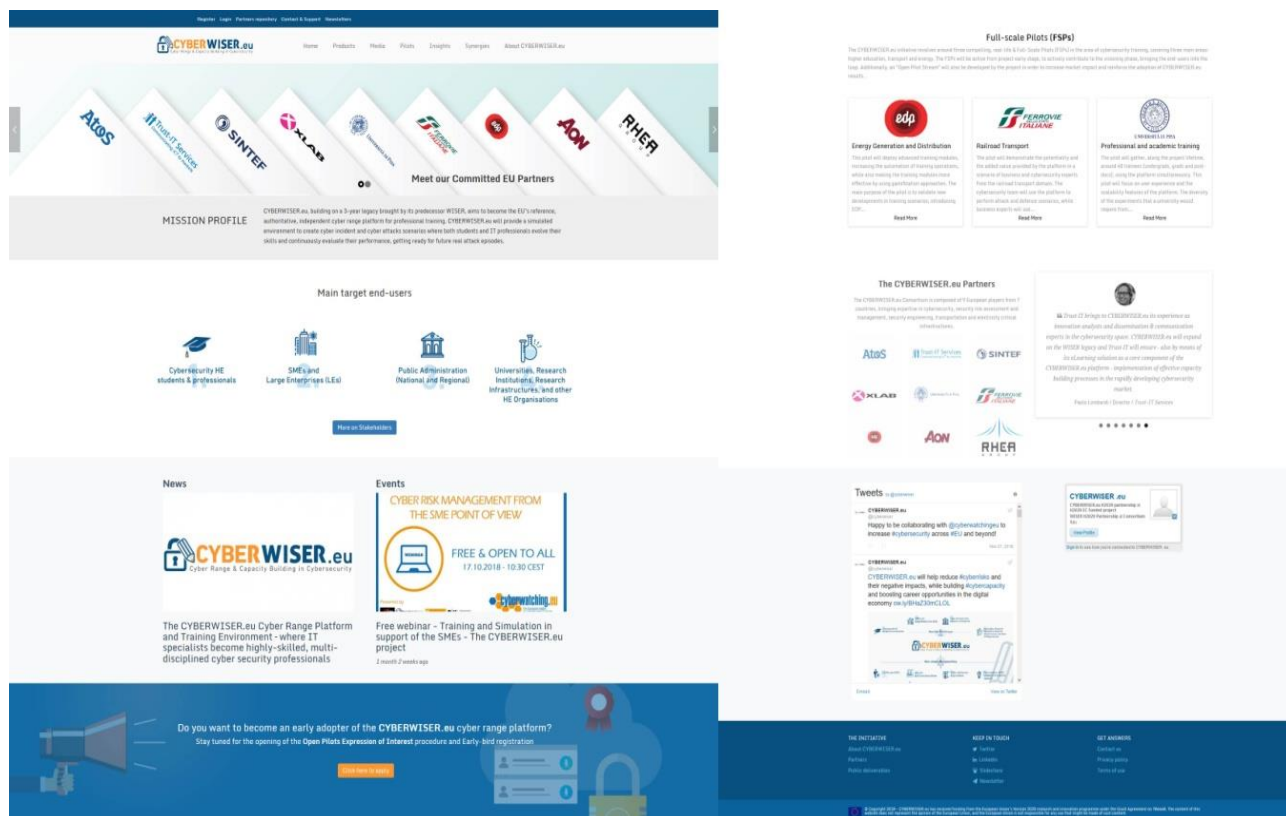


Figure 15: CYBERWISER.eu homepage as of November 2018

The website will be an interactive meeting point and a key element, during the lifecycle of the project, and beyond, to raise awareness around cybersecurity and to gather interest and develop opportunities for different potential customers in this field.

Official launch Date: 20 September 2018.

Average number of sessions per month: 748.

M1 (Sep 2018): 864

M2 (Oct 2018): 27 (low number is due to a Google Analytics issue now fixed)

M3 (Nov 2018): 1.353

5.3 Social Media (active since Month 1)

Building upon its predecessor WISER, CYBERWISER.eu has selected different social networks to communicate its outputs and results and enlarge its community.

An animated social media platform (@cyberwiser) for brief real-time updates and news and to promote event activities; insightful contributions on professional networks (@CYBERWISER.eu). SlideShare is used to disseminate training material and presentations; YouTube to upload and store webinars, videos and other audio-visual material.

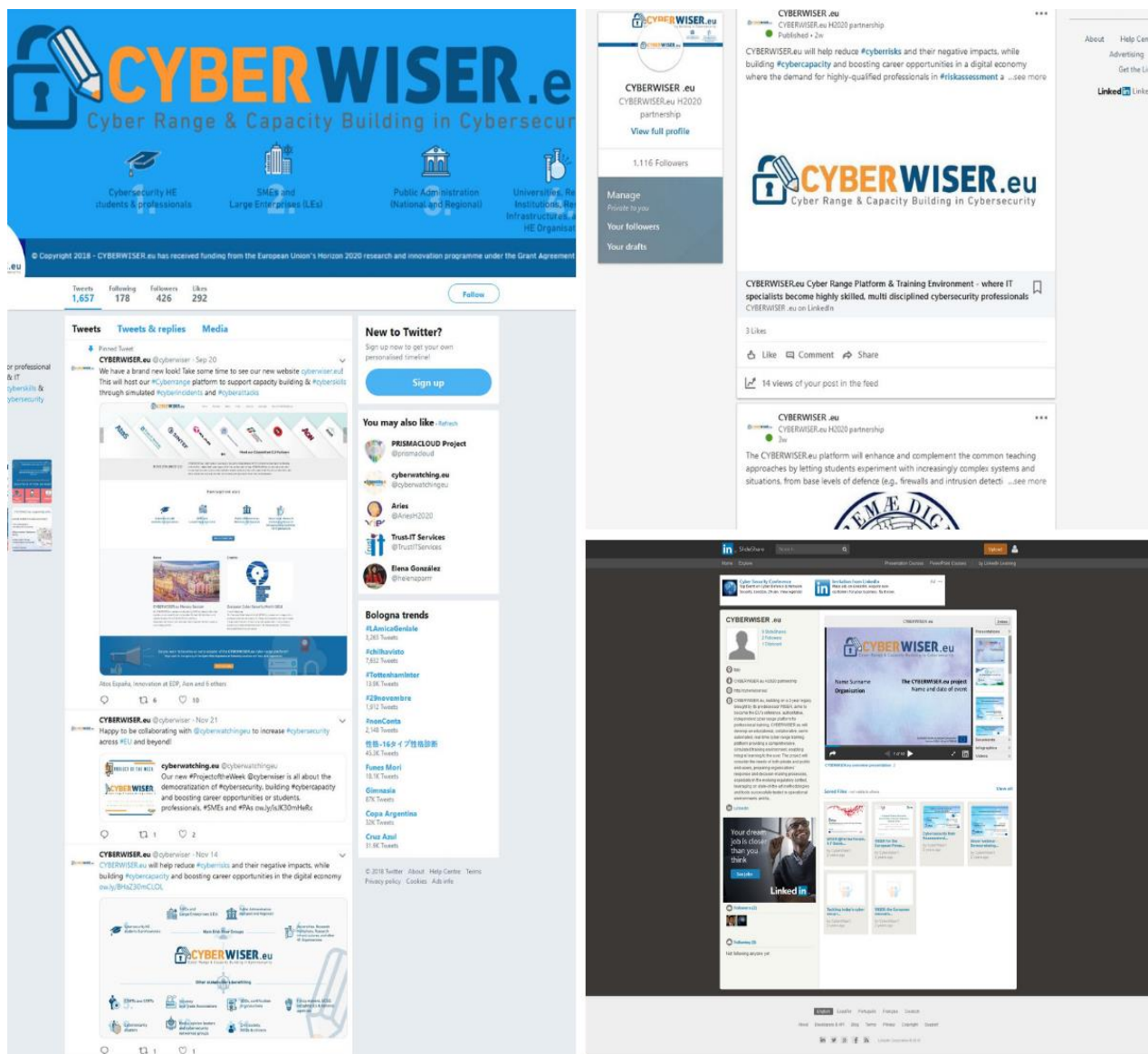


Figure 16: CYBERWISER.eu social media presence (sample)

Main achievements from M1 (September 2018) as of M3 November 2018

Total Twitter Followers:	431
Tweets sent:	40
Total LinkedIn Connections:	1.089
LinkedIn posts/articles:	10
Slideshare presentations uploaded:	1
Youtube videos uploaded:	1

5.4 Collaterals (as of end of Month 3)

A roll-up banner and a flyer (see the figure below) were designed and published in M2 and used to provide a general overview of the project at different events.



Figure 17: Flyer and roll-up banner

A Press Release on the launch of the project has been produced in M2 to be distributed to specific Press & Media Channels and slightly tweaked to be disseminated through social media.

[About CORDIS](#) | [Contact](#) | [Advanced Search](#) | [Legal Notice](#) | [English \(en\)](#)


 European Commission

CORDIS

Community Research and Development Information Service

European Commission > CORDIS > News and Events > CYBERWISER.eu Cyber Range Platform & Training Environment – where IT specialists become highly skilled, multidisciplinary cybersecurity professionals

Search

[Sign in](#)



NEWS & EVENTS
PROJECTS & RESULTS
RESEARCH*EU MAGAZINES

CYBERWISER.eu Cyber Range Platform & Training Environment – where IT specialists become highly skilled, multidisciplinary cybersecurity professionals

Contributed by: **Trust-IT Services**

CYBERWISER.eu will help reduce cyber risks and their negative impacts, while building cyber capacity and boosting career opportunities in a digital economy where the demand for highly qualified professionals in risk assessment and cyberattack response is continuously growing in the light of the existing cyber threat landscape.

The world is more digitally connected than ever. Technology is changing and improving our lives. But we face new challenges. Cybercrime is a major obstacle in our path to a networked society with huge costs to the economy and society.

Studies on cyber risk costs point to increasing impacts to all kinds of organisations, especially where gains for hackers are high, not just in terms of financial gains but also intellectual property and sensitive data. Kaspersky has shown that the monetary impact of cyber breaches can increase by as much as a factor of five when left undetected for seven days, compared to the cost of being detected instantly.

CYBERWISER.eu will help reduce cyber risks and their negative impacts, while building cyber capacity and boosting career opportunities in a digital economy where the demand for highly qualified professionals in risk assessment and cyberattack response is continuously growing in the light of the existing cyber threat landscape.

CYBERWISER.eu will develop an educational, collaborative, real-time civil cyber range platform where cybersecurity competitions will take place. This will become the EU's reference for an authoritative, independent cybersecurity platform for professional training. Users can play the role of attackers and/or defenders in different scalable and configurable scenarios with a set of virtual resources representing a simulated company IT infrastructure.



Figure 18: Press release published on CORDIS

5.5 Publications and participation to events

Table 29 below provides a preliminary list of CYBERWISER.eu visibility at different market targets and stakeholder events.

Event Name / Attending Partner	Date	Location	Attendees	CYBERWISER.eu presence
1. cyberwatching.eu Annual Event (Trust-IT)	08/10/2018	Krakow (Poland)	30	General presentation of the project after the WISER legacy
2. Working Group "Cybersecurity" of the AIPCR/PIARC Italian Technical Committee on "Automatic and Connected Driving" (UNIFI)	05/10/2018	Marghera (Italy)	10	Brief presentation of the project with particular focus on Open Pilots and related Expression of Interest.

Event Name / Attending Partner	Date	Location	Attendees	CYBERWISER.eu presence
3. Cybersecurity Day 2018 organized by CNR (National Research Council) (UNIFI)	12/10/2018	Pisa (Italy)	100	Brief presentation of the project with particular focus on Full Scale Pilot "Professional and Academic Training".
4. WEBINAR - Cyber risk management from the SME point of view (RHEA)	17/10/2018	Online	50	Early presentation of the concept of cyber range platform to perform custom training for professionals in a simulated environment

Table 29: Visibility gained at events (as of November 2018).

5.6 Other communication & dissemination activities

5.6.1 Video

During the first Kick Off Meeting of the project, a promotional video for the project was produced and published through the CYBERWISER.eu YouTube channel and the website.

The video is made of brief speeches from partners of the Consortium introducing the project, the added value that it is going to bring in the context of cybersecurity capacity building, and the role of the FSPs as well as the Open Pilot.



Figure 19: CYBERWISER.eu Video

Despite its length of nearly 5 minutes, the video is intentionally structured in different independent bits that can be extracted to be fully promoted through all social media channels, which usually have different time limits for the video promotion.

5.6.2 Synergies

CYBERWISER.eu will contact a number of European Initiatives, operating in the field of ICT innovation and in other fields, that might present complementary approaches and objectives with the aim of establishing synergies and strategic collaborations.

At the time of writing this deliverable the project has duly consolidated the strategic liaison with cyberwatching.eu¹³ - The European watch on cybersecurity privacy. Thanks to this collaboration a number of activities have been put in place to spread the word about CYBERWISER.eu, namely:

- CYBERWISER.eu is now present in the cyberwatching.eu Observatory¹⁴ with a [dedicated overview page and backlinks](#).
- CYBERWISER.eu is now present in the cyberwatching.eu Service Offer Catalogue¹⁵ with a [detailed presentation of its Full Scale Pilots and the Open Pilot Stream](#).
- CYBERWISER.eu participated as a speaker at the cyberwatching.eu Annual Event¹⁶ in Krakow
- CYBERWISER.eu participated as a speaker at the WEBINAR - Cyber risk management from the SME¹⁷ point of view organized by cyberwatching.eu

At the time of writing this deliverable other 2 important synergies with PoSeID-on¹⁸ and DEFEND¹⁹ have been established and will be further exploited in the coming months.

Further synergies to be exploited during the lifetime of the present communication plan will be evaluated on a case-by-case basis and possibly included in the document.

5.7 The CYBERWISER.eu Community

Building upon its predecessor WISER, CYBERWISER.eu has further expanded the existing community thanks to:

- Partner efforts;
- Web platform registration;
- Social networks;
- Participation to events;
- Organisation of events;
- Synergies and strategic collaborations.

13 <https://www.cyberwatching.eu>

14 <https://www.cyberwatching.eu/observatory>

15 <https://www.cyberwatching.eu/services/catalogue-of-services>

16 <https://www.cyberwatching.eu/news-events/events/cyberwatchingeu-annual-event-krakow-athens>

17 <https://www.cyberwatching.eu/cyber-risk-management-sme-point-view>

18 <https://www.poseidon-h2020.eu/>

19 <https://www.defendproject.eu/>

At the time of writing, CYBERWISER.eu has a community network of **1,833 members** (Overall Twitter and LinkedIn professional network: 1.515 – Registered users: 308) spanning across very different profiles such as:

- IT Specialist/IT Architect.
- Researcher/Scientists.
- Advisor/Consultant.
- Chief Security Officer (CSO)/Chief Information Security Officer (CISO).
- Other.
- CEO/Managing Director/Chief Executive.
- Programme Manager/Project Manager.
- Chief Technology Officer (CTO)/IT Director.
- Professor.
- Journalist/Editor/Copywriter.
- Policy development manager/Policy Consultant.

A continuous effort of community monitoring is performed by Trust-IT and circulated every month (or higher frequency) to all Consortium Partners.

6. Conclusions

The present document is the first of 3 versions. The main conclusions are:

- The “Communication & Stakeholder Plan” is tightly linked to the project results and therefore is to be considered as a **living document**: It will be up to the “Communication, community development, policy & go-to-market” work package to timely update it whenever necessary, well before the second version of it, expected in Month18 (February 2020).
- WP6 activities in the **first 3 months** of the project have been conducted with good coordination and produced tangible results, including completion of project branding, launch of the new website, visibility at 4 events, and production of a number of collaterals.
- A first **roadmap for the period M4-M18** has been developed and it will be followed as part of WP6. The roadmap will be updated in the upcoming months as part of WP6 activities.
- All Consortium Partners have shown **good alignment and high commitment** in development and implementation of the present plan.

References

- [1] Grant Agreement-786668-CYBERWISER_EU