Deliverable

Communication & Stakeholders Engagement plan

December 2017

Disclaimer

The work described in this document has been conducted within the project cyberwatching.eu. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no. 740129. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

cyberwatching.eu consortium

Trust-IT Services
Communicating ICT to markets

Oxford e-Research Centre

UNIVERSITY OF OXFORD

ICT LEGAL CONSULTING
Balboni Bolognini & Partners

European Digital SME Alliance

CONCEPTIVITY
360° SECURITY

AON

aeiciberseguridad
Agrupación Empresarial Innovadora CIBERSEGURIDAD y Tecnologías Avanzadas

Abstract:

This document sets out the initial communication and stakeholder engagement plan covering months 1-18 for cyberwatching.eu. It maps cyberwatching.eu assets to each stakeholder group targeted, highlighting tangible benefits and explaining how cyberwatching.eu will engage with each one, through events, multipliers, social media and professional networking. Impacts are measured through pre-defined KPIs.

Keywords *Cyberwatchng.eu communication strategy, stakeholder engagement, KPI, EU Cyberwatching.eu Observatory, SME, Cyberwatching assets and stakeholders, standardization organisations*

The work described in this document has been conducted within the project cyberwatching.eu. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 740129. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

Executive Summary

The overriding objective of cyberwatching.eu is to lower barriers to innovative cyber security and privacy (CS&P) products and services such as those coming from projects funded by the EC, EU member states and associated countries.

The assets of cyberwatching.eu are designed to address these barriers:

- An EU Cyberwatching.eu Observatory offering a comprehensive and organic view of R&I initiatives, services and products emerging across the EU and Associated Countries.
- A mark complex and multi-faceted landscape of cyber risks while increasing understanding of EU compliance obligations.
- Cyberwatching.eu SME end-user club: bringing small businesses together in one place facilitates the adoption of a cyber-security strategy in companies with few resources, learning from best practices adopted by others.

In addition, cyberwatching.eu will deliver a set of insightful reports and white papers helping policy makers and other stakeholders to understand the cyber security ecosystem, spanning R&I results, policy, regulation, standards and best practices.

This Communication and Stakeholder Engagement Plan is the first document setting out specific actions and measures that will ensure community building and practical assets key to sustaining a multi-service marketplace beyond the project's funding lifecycle.

The Plan outlines cyberwatching.eu stakeholder groups and targeted engagement activities with a roadmap for the first 18 months of cyberwatching.eu, as foundational for future actions in two further documents (D4.3 in M18 and D4.9 in M48). The Plan shows how activities will be monitored through pre-defined KPIs. It also provides a concise report on current achievements, upcoming synergies and knowledge sharing, as well as engagement roadmaps for each stakeholder group targeted.

Terminology

CSIRTs	Computer Security Incident Reponse Teams
CS&P	Cybersecurity and privacy
EC	European Commission
ECSO	European Cyber Security Organisation
ENISA	European Network and Information Security Agency
ETSI	European Telecommunications Standards Institute
EU	European Union
EU-JP	Europe-Japan
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
KPI	Key Performance Indicator
NIST	National Institute of Standards and Technology
OASIS	The Organization for the Advancement of Structured Information Standards
SDO	Standards Development Organisation
SME	Small Medium Enterprise
SRIA	Strategic Research and Innovation Agenda
SSO	Standard Setting Organisation
ITU	International Telecommunication Union

Table of Contents

LIST OF FIGURES

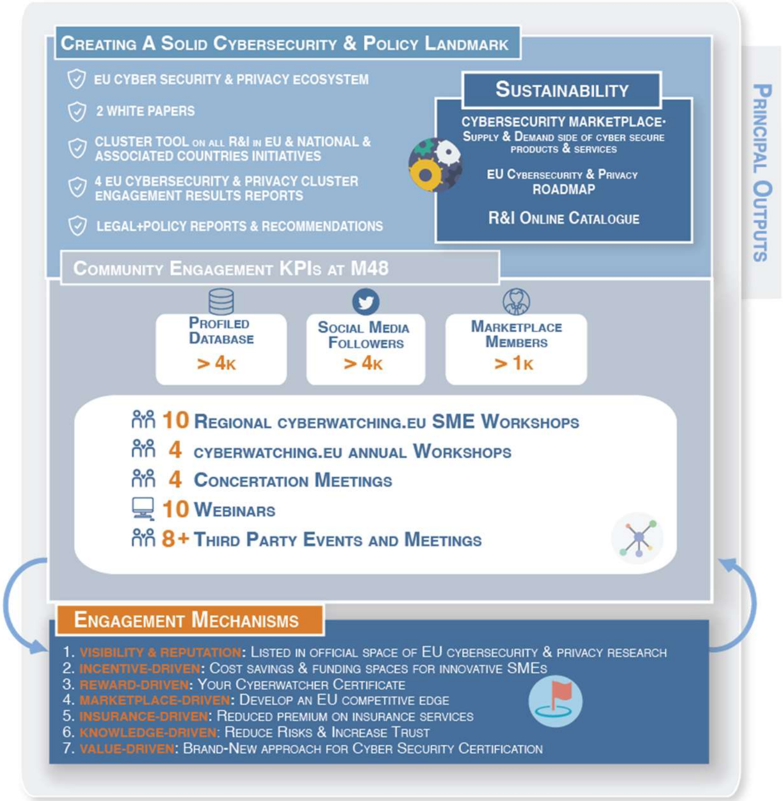
LIST OF TABLES

1 Introduction & scope of the document

In the age of online business and e-government services, the impact of a data breach can be huge and long lasting. Risks span business interruption, data loss, IPR theft, brand damage, loss of customers and reduced ability to win new business. All businesses are at risk cyberattack, whether they are a Fortune 500 company, a family-run business, a utility company or a tech start-up. However, most SMEs significantly underestimate the risks they face and there are many reports revealing vulnerabilities affecting large companies. Similar impacts can be found for public sector organisations, notably healthcare facilities and services.

Because awareness of risks amongst EU organisations is low, the uptake of cyber security and privacy (CS&P) products and services is inadequate for responding to cyberattacks and building resilience.

The overarching objective of cyberwatching.eu is to reduce barriers to CS&P across the EU. To this end, cyberwatching.eu will roll out a compelling set of practical outputs and assets benefitting a variety of stakeholders, from SMEs to R&I teams, public sector organisations and policy makers.



Creating A Solid Cybersecurity & Policy Landmark

- EU CYBER SECURITY & PRIVACY ECOSYSTEM
- 2 WHITE PAPERS
- CLUSTER TOOL on all R&I in EU & NATIONAL & ASSOCIATED COUNTRIES INITIATIVES
- 4 EU CYBERSECURITY & PRIVACY CLUSTER ENGAGEMENT RESULTS REPORTS
- LEGAL+POLICY REPORTS & RECOMMENDATIONS

Sustainability

CYBERSECURITY MARKETPLACE· Supply & Demand side of cyber secure products & services

EU Cybersecurity & Privacy ROADMAP

R&I Online Catalogue

Principal Outputs

Community Engagement KPIs at M48

Profiled Database > 4k

Social Media Followers > 4k

Marketplace Members > 1k

10 Regional cyberwatching.eu SME Workshops

4 cyberwatching.eu annual Workshops

4 Concertation Meetings

10 Webinars

8+ Third Party Events and Meetings

Engagement Mechanisms

1. Visibility & Reputation: Listed in official space of EU cybersecurity & privacy research
2. Incentive-driven: Cost savings & funding spaces for innovative SMEs
3. Reward-driven: Your Cyberwatcher Certificate
4. Marketplace-driven: Develop an EU competitive edge
5. Insurance-driven: Reduced premium on insurance services
6. Knowledge-driven: Reduce Risks & Increase Trust
7. Value-driven: Brand-New approach for Cyber Security Certification

Figure 1 cyberwatching.eu outputs

The cyberwatching.eu communication strategy is a pragmatic, KPI-driven effort to ensure assets are appropriately promoted and taken up by the various stakeholders targeted. Communications is defined as a continuous flow of information from the very outset of the project, engaging stakeholders around cyber security and privacy, and ensuring they make them their top business priority in a fast evolving and multi-faceted landscape.

The communication plan is designed as a coordinated, joint effort by all cyberwatching.eu partners. Every partner will contribute to the actions foreseen in the communication plan, in proportion to the effort allocated to them in WP4.

Specific details on every partner commitment on single actions and activities will be required during the regular WP4 conference calls.

2 Cyberwatching.eu Communication Strategy

2.1 Cyberwatching.eu communication objectives

The overarching objective of the cyberwatching.eu communication strategy is to build an extensive community of end-users as key for the sustainability of the European Observatory after the 48-month project execution.

The cyberwatching.eu Communication and Stakeholder Engagement Plan sets out specific measures for a European cyber security and privacy (CS&P) Observatory that creates a strong cyber security culture as the basis for a competitive EU ecosystem.

The main objectives are to:

- Design, deliver and sustain an EU observatory (www.cyberwatching.eu) tailored to different stakeholder needs with fast and easy access to a wealth of CS&P practical guides and insights into multiple formats, such as SEO-based texts, videos, webinars, leading to the activation of the **Marketplace** and its **Catalogue of Services**.
- Ensure a strong focus on **SMEs** as the lifeblood of the EU economy, launching and animating an **End-User Club** and by increasing awareness that cyber risks are a business risk and not simply a technical issue.
- Pursue **multi-stakeholder engagement** and dialogue at EU and global level in a way that ensures full representation of the ecosystem and encourages a collective understanding of all major aspects of CS&P.
- Provide **educational and informative services** on the EU legal and regulatory framework with practical guides tailored to diverse levels of knowledge and expertise.
- Foster the implementation of **best practices** based on a collective understanding among all key stakeholders, encourage and monitor the uptake of relevant ICT standards, spanning standards on risk management, cyber security and privacy.

All the stakeholders targeted by cyberwatching.eu will benefit from the assets delivered by cyberwatching.eu, as EU R&I initiatives find effective channels for their results, businesses access new CS&P products and services, organisations of all types learn about the importance of responsibility in cyberspace and legal compliance. Policy makers will benefit from new insights shaping future research directions and synergies with the European Cyber Security Organisation (ECSO) and its working groups, including WG1 - Standardisation, certification, labelling and supply chain management; WG2 - Market deployment, investments and international collaboration; WG4: Support to SMEs coordination with countries (in particular East and Central EU) and regions; WG6: Strategic Research and Innovation Agenda (SRIA), as well as co-operation on taxonomy.

The communication and engagement plan is led by WP4 which has a key and central role in the project in terms of communicating and disseminating results to target stakeholders.

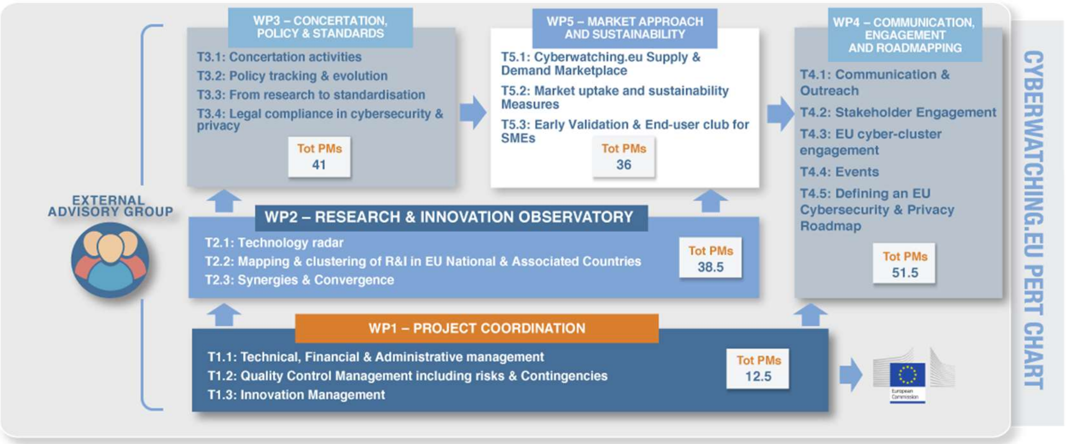

WP3 – CONCERTATION, POLICY & STANDARDS
T3.1: Concertation activities
T3.2: Policy tracking & evolution
T3.3: From research to standardisation
T3.4: Legal compliance in cybersecurity & privacy
Tot PMs 41
WP5 – MARKET APPROACH AND SUSTAINABILITY
T5.1: Cyberwatching.eu Supply & Demand Marketplace
T5.2: Market uptake and sustainability Measures
T5.3: Early Validation & End-user club for SMEs
Tot PMs 36
WP4 – COMMUNICATION, ENGAGEMENT AND ROADMAPPING
T4.1: Communication & Outreach
T4.2: Stakeholder Engagement
T4.3: EU cyber-cluster engagement
T4.4: Events
T4.5: Defining an EU Cybersecurity & Privacy Roadmap
Tot PMs 51.5
EXTERNAL ADVISORY GROUP
WP2 – RESEARCH & INNOVATION OBSERVATORY
T2.1: Technology radar
T2.2: Mapping & clustering of R&I in EU National & Associated Countries
T2.3: Synergies & Convergence
Tot PMs 38.5
WP1 – PROJECT COORDINATION
T1.1: Technical, Financial & Administrative management
T1.2: Quality Control Management including risks & Contingencies
T1.3: Innovation Management
Tot PMs 12.5
European Commission
CYBERWATCHING.EU PERT CHART

Figure 2 WP4 playing a central role in cyberwatching.eu

Input for WP4 activities will come from all other WPs:

- WP2 – Research and Innovation Observatory:
  - Cybersecurity and Privacy Technology radar (T2.1)
  - Mapping & clustering of R&I in EU National & Associated Countries (T2.2)
  - Synergies & Convergence (T2.3)
- WP3 – Concertation, Policy & Standards
  - Concertation activities (T3.1)
  - Policy tracking & evolution (T3.2)
  - Results and recommendations from standards and certification (T3.3)
  - Legal compliance (T3.4)
- WP5 – Market approach and sustainability
  - Cyberwatching.eu supply and demand marketplace (T5.1)
  - Early validation and end-users club (T5.3)

2.2 Multiple Channels and Formats for cyberwatching.eu stakeholders

To implement the communication and stakeholder plan, cyberwatching.eu will use a variety of channels and formats tailored to its different stakeholders based on the levels of awareness and expertise. Such channels and formats include the cyberwatching.eu website, social media channels, newsletters, videos, press releases, webinars, and collaterals such as brochures, flyers, pop-up banners and factsheets on CS&P:

- A dynamic, content-rich and SEO-driven **cyberwatching.eu website** hosting informative guides, outputs and assets as the project evolves over time. The website (www.cyberwatching.eu) will serve as the information focal point and delivery channel for the project results. The platform will be a gateway for the services offered by Cyberwatching.eu (Observatory, Catalogue of Services, Marketplace, SMEs End Users Club) and will also integrate social media channels.
- An animated social media platform (cyberwatching.eu **Twitter**) for brief real-time updates and news and to promote event activities; insightful contributions on professional networks (cyberwatching.eu **LinkedIn and relevant groups**). SlideShare is used to disseminate training material and presentations; **YouTube** to upload and store webinars, videos and other audio-visual material.
  - **Blogs, news and opinion pieces** Published through social media, websites and media channels to communicate objectives and disseminate results to different stakeholders.
- **Newsletters**: targeting content to specific stakeholders.
- **Videos**: Informative and marketing videos produced by professional in-house team.
- **Press releases**: to be distributed to specific Press & Media Channels.
- **Branded graphics and printed material:** Clear branding in all online content and printed material. Fliers, pop-up banners and booklets communicate objectives and disseminate results. Partner-specific material can be produced for each partner to

promote the initiative within their institutes and at specific partner events as well as through their networks and channels, also in line with their organisational mission.

cyberwatching.eu and 3rd-party events

- **Webinars** dedicated webinars targeted to specific stakeholders.
- **Concertation and Cluster Meetings** co-located with annual cyberwatching.eu workshops.
- **Annual workshops** with multi-stakeholder coverage.
- **National/regional SME workshops** co-located with relevant (3rd-party) events.
- **3rd-party events** to also cover training aspects targeting technologies and topics such as network and information security, cloud computing, industry and policy conferences.
- **Policy events** with priority given to ECSO annual conferences and meetings.

Campaigns on events, project outputs and assets will be based on the **SMART** approach: specific (e.g. topic and stakeholders), measurable (e.g. based on pre-defined KPIs), achievable and realistic (e.g. evidence based and knowledge of topic/stakeholders), timed (e.g. clearly defined start and finish) and timely (e.g. based on knowledge of the landscape and specific information needs).

2.3 A KPI-driven Approach

The impact of the activities described in this plan will be measured through a core set of key performance indicators (KPIs) wherever they are quantifiable.

A continuous activity of monitoring will be carried on by TRUST IT Services and shared with all partners weekly.

The table below shows the project targets as defined in the Grant Agreement.

Communication Measures	KPIs
Web platform (EU Observatory & Marketplace with Catalogue of Services)	Design, development and operation of a dynamic and responsive web platform as a single access point on CS&P → Impact of web platform (e.g. unique visitors, sessions, downloads etc.) **KPIs:** 10,000 visitors/month by M12; 30,000 by M24; 50,000 by M36 and 80,000 by M48
Promotional and Marketing Material	Brochures, fliers, posters, roll-up banners, slide decks - tailored to different audiences **KPIs:** Min. 8 fliers-brochures/year (regularly updated); Min. 1 roll-up banner/event; Min. 2 general and 4 tailored slide decks/year.
Videos	Informative and marketing videos produced by professional in-house team. **KPIs:** Final suite of 4 videos by M48.
Newsletters	**KPIs:** Min. 10/year, including tailored newsletters to specific stakeholders on each major cyberwatching.eu output
Press releases and media content	**KPIs:** Min. 2 PRs/Media content (e.g. opinion piece or podcast) per year with 3 major campaigns planned for the launch of the marketplace and related services.

Table 1 Communication Measures & KPIs

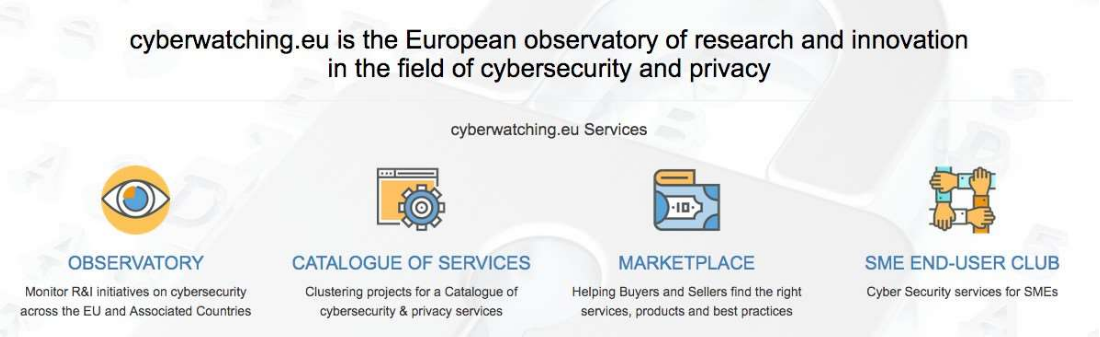
The table below shows the project targets for event-related activities, as defined in the Grant Agreement.

Event Formats	KPIs
Webinars	**KPIs:** 10 webinars (average attendance of at least 40 registered members per webinar).
International events	**KPIs:** 4 international events (Workshops + concertation meetings) in EU with at least 150 engaged attendees.
Deep-dive workshops	**KPIs:** 4 Cybersecurity and privacy Technology deep-dive workshops involving CS&P project clusters.
Concertation meetings	**KPIs:** 4 Concertation meetings for coordination of R&I projects in Europe and Associated States with involvement of a significant number of cybersecurity stakeholders.
National/regional workshops	**KPIs:** 10 national/regional workshops will address an SME audience and will be organised in collaboration with local SME associations.
Third-party events	**KPIs:** participation to at least 8 third-party events / meetings.

Table 2 Event formats & KPIs

3 Cyberwatching.eu Assets and Stakeholders

3.1 Cyberwatching.eu assets and outputs



cyberwatching.eu is the European observatory of research and innovation in the field of cybersecurity and privacy

cyberwatching.eu Services

OBSERVATORY
Monitor R&I initiatives on cybersecurity across the EU and Associated Countries

CATALOGUE OF SERVICES
Clustering projects for a Catalogue of cybersecurity & privacy services

MARKETPLACE
Helping Buyers and Sellers find the right services, products and best practices

SME END-USER CLUB
Cyber Security services for SMEs

Figure 3 Cyberwatching.eu assets and outputs

Cyberwatching.eu is the European CS&P observatory comprising a comprehensive and organic view of R&I initiatives, services and products emerging across the EU and Associated Countries. The value of cyberwatching.eu lies in offering not only a systematic view of results to avoid dispersion and duplication but an effective forum for marketing them and increasing uptake. It provides a synoptic view of all on-going and recently concluded projects advancing cyber security and privacy for the benefit of the many. A key feature is highlighting specific needs, processes and practices across diverse technology and sector-specific domains: from embedded systems to cloud and the Internet of Things to healthcare, financial services and high-tech engineering, to name but a few. In addition, the Observatory showcases European values that are embedded into new R&I, such as the protection of personal data and the implementation of standards, helping to build confidence and trust in consumers and businesses and public sector organisations.

The Cyberwatching.eu observatory (www.cyberwatching.eu) will showcase key project outputs:

R&I clustering and an R&I service offer catalogue

Three main strands lie at the base of the mapping and clustering activities of WP2. This is reflected in the website:

- Foundational technical methods and risk management for trustworthy systems in cyber security and privacy.
- Applications and user-oriented services to support cyber security and privacy.
- Policy, governance, ethics, trust, usability and human aspects of cyber security and privacy.

This clustering process also has the benefit of streamlining R&I in one convenient place, focusing discussions based on common interests and shaping future directions by clearly showing what is already being developed.

The website will provide the online focal point for these activities hosting the following:

- Service offer catalogue of R&I projects: The service offer catalogue is made up of one-page service offers provided by projects. Projects complete a simple one-page template which focusses on end-user needs and impact of project results. The service offers can be filtered on cyber security elements (see taxonomy in WP2) and vertical markets.
- Point of reference for service offer online submission.
- Information on clustering methodology and cyberwatching.eu cybersecurity taxonomy.
- Point of reference for submission of clustering scoring: projects will submit their cluster scores directly on an online webform hosted on the website. Information gathered will be added cyberwatching.eu cluster tool, as well as to the service offer catalogue.
- Cluster workshop information and results

Concertation meetings

Cyberwatching.eu will organise 4 annual Concertation meetings (T3.1) which will be described in more detail in D3.1. Cluster workshops mentioned above will be co-located at these events. The cyberwatching.eu website will be the online focal point for these events with dedicated sections focussing on promoting both pre-event and post-event information. Sections will be published including:

- Event overview & why attend
- Agenda & event presentations
- Registration
- Service offer submission
- Logistical information

cyberwatching.eu marketplace: the added value of the marketplace comes from lowering the entry barrier to an EU-driven cyber security and privacy culture by meeting new end-user needs stemming from a complex and multi-faceted landscape of cyber risks while fulfilling stricter EU legislation requirements on data protection and privacy. User-friendly discovery to innovative solutions means interested organisations from the public and private sector can easily match offers to their specific needs.

From a supply side, the marketplace will feature CS&P services with an MRL from in particular 3-6. The benefits for the providers are outlined below. Providers can be R&I projects and European start-ups and SMEs.

1. MRL 3 Validation of services to marketplace end-users
2. MRL 4 Small-scale stakeholder campaign targeting selected marketplace end-users
3. MRL 5 Large-scale stakeholder campaign with marketplace end-users one of other targets
4. MRL 6 Proof of traction. Potential source of paying customers

A detailed summary of the marketplace will be provided in D5.1.

The Marketplace also provides considerable benefits and opportunities for its users (in particular, SMEs):

1. to purchase products/services with prices that are cheaper than those offered in the market;
2. to validate/test some of the products for free (its continuous usage is normally not charged either) and contribute to their development – research projects, offering to validate their products, might even adjust their products based on user's feedback!
3. to contact the supply side directly

Cyberwatching.eu SME end-user club: bringing small businesses together in one place facilitates the adoption of a cyber-security strategy in companies with few resources, learning from best practices adopted by others. The club guides SMEs through the Catalogue of Services, offering a unique, win-win opportunity to become early adopters of new products and services, providing feedback on usability and effectiveness in addressing cyber risks. The club is also an opportunity to share business requirements and therefore ensure that products and services are designed around real user needs.

End-users should not just be limited to SMEs but also other end-users such as large enterprises and public administrations.

Main incentives to join the end-user club

- Access to Marketplace services
- Invitation to cyberwatching.eu SME workshops and other events. This includes networking opportunities with cyberwatching.eu stakeholders and importantly the opportunity to actively contribute to events through presentations and panel discussions.
- Dedicated webpage on organisation and requirements as an end-user
- Opportunity to become a marketplace champion and be the focus of a cyberwatching.eu use case analysis (T5.3)
- Access to CS&P guides published by cyberwatching.eu (e.g. legal guide etc)
- Increased visibility for the company: marketplace champions or other active participants can be mentioned in our European and/or national level media campaigns, in social networks of cyberwatching.eu, etc
- End-users will get cyberwatching.eu users' badge that will also boost their communication activities

Legal tips

With the GDPR launch in mid-2018 legal compliance is a key area of interest for stakeholders. A section dedicated to legal tips has been created and is regularly updated in particular by ICTL as part of T3.4. In addition D3.4 & 3.7 Cybersecurity Legal and Policy aspects will be a key project output and source of content for this section. They will also feed into specific content tailored for the SME end-user club.

A self-assessment tool will also be created where SMEs can check their general compliance with GDPR: SMEs will get a short questionnaire; upon its completion they will see their level of compliance and get some tips on likely improvements.

Cyber insurance pilot service

Specific recommendations on the importance of risk management and service will be available to end-user club members.

End users will get special offers for the cyber insurance if they decide to purchase one.

Cyber security policy and roadmap

As part of T3.1, cyberwatching.eu will contribute to policy dialogue with key recommendations on EC policy. The website section updates on policy-related issues and project results on this. In addition, the Cybersecurity & Privacy Roadmap (M22; M45 will see a 3-5 year roadmap identifying also the socio-economic impact of cybersecurity and current gaps and future priorities in the Cybersecurity and privacy landscape that should be addressed for an effective Digital Single Market. The roadmap will make recommendations stemming from the R&I Catalogue of Services and will encourage projects to plan early their route to market. In addition, the roadmap will set out guidelines for the industry and the public sector to comply with standards which support global interoperability and seamless trustworthy standardisation.

Standards and certification.

As part of T3.3, Cyberwatching.eu will map current standards adoption by projects in order to identify existing gaps and to make a series of recommendations regarding this in particular to encourage greater security by design best practices. In addition, the website will provide information on existing CS&P standards and certification.

3.2 Stakeholder groups

cyberwatching.eu assets are designed around the specific needs of diverse stakeholder groups targeted by the project. For example, **stakeholders for www.cyberwatching.eu span:**

- **R&I teams and projects** with sufficiently mature results (based on market and technology readiness levels) can easily find potential customers for their new products and services.
- **SMEs and large companies** as potential users of services, including the dedicated cyberwatching.eu **end-user club**.
- **Financial services and insurance industry**: foster the implementation of best practices through the cyberwatching.eu cyber insurance pilot service as the cyber insurance market evolves in response to new risks and requirements for compliance filter through the market.
- **National and regional administrations**: educating IT and decision makers on the importance of creating a cyber security and privacy culture within their organisations to increase awareness and concrete actions towards risk-based cyber security, resilience and compliance.
- **Standardisation organisations (SDOs):** Catalogue of CS&P standards and certifications within the website offers an opportunity to increase visibility of best practices, showcasing best practices in the field, encouraging implementation as well as contributions from standards specialists in EU R&I initiatives, which is an important policy goal for the realisation of the Digital Single Market.

Overall, cyberwatching.eu facilitates **policy and regulators** monitor the EU cyber security and privacy landscape, project lifecycles and the impact of funding.

Multipliers, Media and Synergies

- **Cyber security clusters**: offering potential channels for raising awareness about advances in the field, as well as new supply and demand offers through cyberwatching.eu.
- **Synergies**: cyberwatching.eu will identify like-minded projects at national and EU level with which it can share knowledge and conduct joint promotional and awareness campaigns on topics of common interest.
- **IT and information security media channels**: cyberwatching.eu targets these channels to help extend its key messages and promotes its main assets.

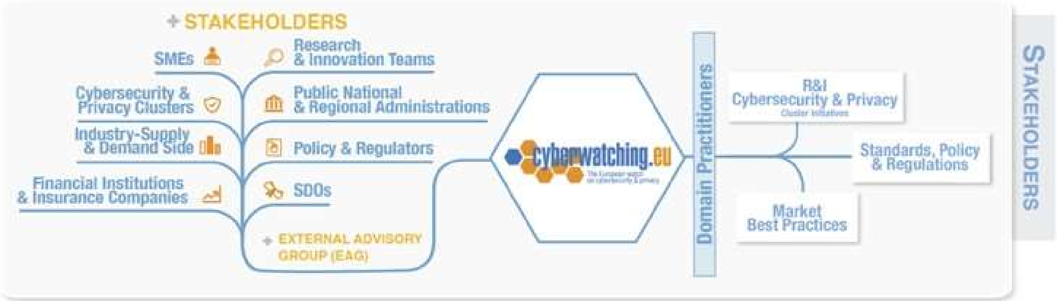

+ STAKEHOLDERS
SMEs
Research & Innovation Teams
Cybersecurity & Privacy Clusters
Public National & Regional Administrations
Industry-Supply & Demand Side
Policy & Regulators
Financial Institutions & Insurance Companies
SDOs
+ EXTERNAL ADVISORY GROUP (EAG)
cyberwatching.eu
Domain Practitioners
R&I Cybersecurity & Privacy
Cluster Initiatives
Standards, Policy & Regulations
Market Best Practices
STAKEHOLDERS

Figure 4 cyberwatching.eu stakeholders

3.3 R&I teams and projects

Research and Innovation Teams are developing software and solutions to help tackle the current and evolving threat landscape with

Their main challenges are:

- The lack of available and easily findable channels for exploiting project results for potential uptake, thereby supporting exploitation and sustainability goals.
- Easily findable channels that can be used as showcases of new R&I advances in cyber security and privacy.
- Guidance in presenting results that are understandable to target audiences other than technical constituencies.
- Awareness of other on-going initiatives on similar cyber security and privacy challenges, helping to position their R&I, while also shaping future R&I directions.

Major benefits of cyberwatching.eu:

- cyberwatching.eu offers a fresh, novel approach to R&I impact through joining the marketplace and catalogue of services for commercialising results to appropriate stakeholders, whether they be SMEs, large companies, public sector organisations, national research and education networks or other cyber security and privacy initiatives taking forward research results and open source software.
- cyberwatching.eu makes R&I results findable and usable by end-users by taking R&I results, services and solutions closer to users and businesses, including early validation and market uptake.
- cyberwatching.eu provides concertation and clustering activities across cyber security and privacy topics, with opportunities to raise awareness and share knowledge, monitor project lifecycles and showcase EU excellence. cyberwatching.eu provides opportunities to also shape future research directions without duplication of effort and facilitates the creation of new knowledge synergies across the EU.
- Synergy with SEREN3 providing a link to NCPs for EU mapping.

3.3.1 Channels & Formats

www.cyberwatching.eu	The catalogue of services and marketplace provides the opportunity for projects to publish and showcase results. Cyberwatching.eu partners will also promote events and news coming from projects thus providing an extra channel of visibility to them.
Social Media Channels: Twitter	cyberwatching.eu will carry out dedicated communication activities through its social media channels to increase projects visibility through a multiplier effect. cyberwatching.eu will promote R&I project results, outputs, news and events through both its social media channels. Core messages will also be conveyed through high-impact images created as part of the project's communication strategy.
Professional Networks: LinkedIn	Regular engagement and contributions to relevant discussions and groups to share best practices. Promote opportunities to R&I professionals and encourage virtual networking with major stakeholders.
Newsletters	Informative newsletters will be delivered to R&I representatives with the aim of promoting cyberwatching.eu activities of interest for R&I target and updates on the cyberwatching.eu services that are relevant for R&I.
Videos	Specific videos targeting R&I and promoting the benefits of joining cyberwatching.eu. Interviews and testimonials from projects will also be collected.

Collaterals	Specific graphic material including fliers targeting R&I and promoting the benefits of joining cyberwatching.eu and its services. A printed version of the service offer catalogue will be created and distributed at the annual Concertation meetings.
Concertation Meetings	cyberwatching.eu will organise 4 annual Concertation meetings to showcase EU excellence and leadership through success stories, facilitate synergy-ignition among R&I Teams, support collaboration and cross-fertilisation with clustering along market sectors and software developments, encouraging re-use of R&D results.
Technology Deep Dive Workshops	Specifically intended for R&I teams funded under Unit H1, these workshops are part of the cyberwatching.eu clustering activities that designed to enable this stakeholder group to measure impact and RoI, create knowledge synergies and identify future funding opportunities. The project clustering tool will also help this group and other initiatives funded by EU member states and associated countries to identify knowledge synergies and identify new funding opportunities that build on and potentially re-use existing R&I results.
Webinars	Of the 10 cyberwatching.eu webinars planned, 3 will cover topics related to R&I clustering. The webinars are an opportunity to showcase innovative R&I, demonstrate the value of cyberwatching.eu clustering tools and support and help shape future strategic research and innovation agendas, for example, in synergy with the European Cyber Security Organisation (ECSO).

Table 3 R&I teams and projects dissemination channels & formats

The timeline gives an overview of communication and dissemination activities from M1-18.

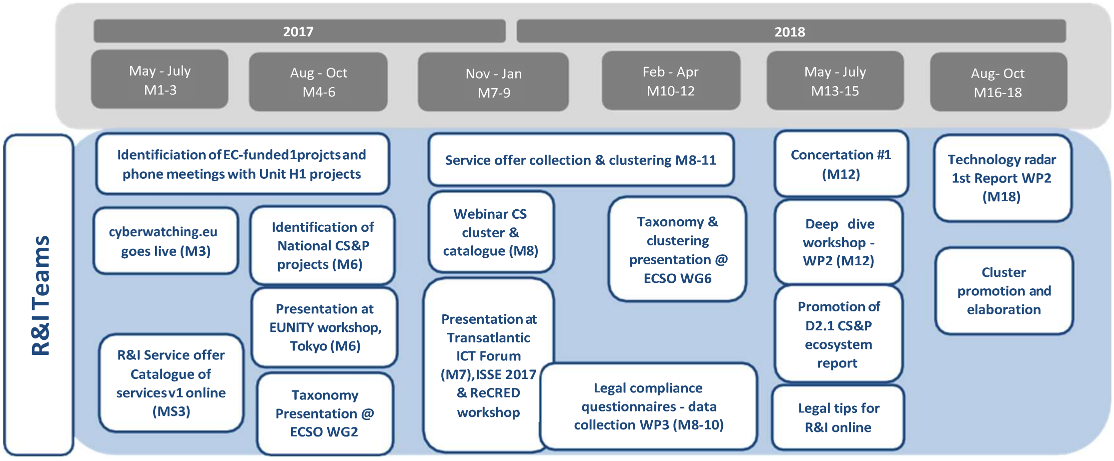

2017
2018
May - July M1-3
Aug - Oct M4-6
Nov - Jan M7-9
Feb - Apr M10-12
May - July M13-15
Aug- Oct M16-18
R&I Teams
Identificiation of EC-funded1projcts and phone meetings with Unit H1 projects
cyberwatching.eu goes live (M3)
Identification of National CS&P projects (M6)
Presentation at EUNITY workshop, Tokyo (M6)
R&I Service offer Catalogue of services v1 online (MS3)
Taxonomy Presentation @ ECSO WG2
Service offer collection & clustering M8-11
Webinar CS cluster & catalogue (M8)
Presentation at Transatlantic ICT Forum (M7),ISSE 2017 & ReCRED workshop
Taxonomy & clustering presentation @ ECSO WG6
Legal compliance questionnaires - data collection WP3 (M8-10)
Concertation #1 (M12)
Deep dive workshop - WP2 (M12)
Promotion of D2.1 CS&P ecosystem report
Legal tips for R&I online
Technology radar 1st Report WP2 (M18)
Cluster promotion and elaboration

Figure 5 R&I teams and projects activity timeline

3.4 SMEs

ICT opens up the world to SMEs and start-ups across Europe, giving them increased opportunities to grow their business but there is also a downside:

Their main challenges are:

- Lack of awareness of the scale of the socio-economic impacts they face, from financial losses through data theft, theft of IPR and fines to loss of reputation, which could be life-threatening for a small business. Awareness of risks is particularly important given the diverse types of risks facing SMEs, not only as data/IP owners, high value companies but also as routes to larger companies with which they partner.

- Lack of resources to deal with cyber threats, usually with only a small IT team, lack of knowledge of potential solutions and greater difficulty in finding and comparing such solutions.
- Lack of information and knowledge on best and most suitable cybersecurity products to purchase/use.
- Gap in availability or affordability to SMEs of standards, compliances and certification schemes;
- Lack of clarity of EU regulations or high-level regulations which are not provided in SME friendly language
- Known and real need for products and services that increase resilience in cyber space at scales larger than current market uptake.

Major benefits of cyberwatching.eu:

- EU-level visibility and networking opportunities through the marketplace social media, and during EU-level events.
- Easy and rapid access to practical information on cyber risks and how to deal with them.
- Direct access to new, affordable and effective CS&P products and solutions that can also give them an edge over competing companies, resulting in increased resilience and enhanced data protection for SMEs as the lifeblood of the European economy.
- Opportunity to be showcased as part of the best practice examples which will showcase the benefit of the marketplace.
- Lower barriers to compliance with complex EU regulations.
- Opportunities to join forces with other SMEs in the End-user Club, learn about best practices on CS&P, access the marketplace as both a supply or demand company, and discover information about future funding.
- A Reward and Certification mechanism by joining the cyberwatching.eu SMEs End-User Club. SMEs entering the club will have discounted access to the market-ready services present in the Marketplace ensuring validation & early adoption of R&I solutions proposed;
- An Insurance-driven mechanism; SMEs that have utilised innovative CS&P measures will receive a reduced premium on insurance services. The insurance companies can benefit from a reduced level of risk and be part of the cyberwatching.eu ecosystem.

cyberwatching.eu strategy: tailoring messages, communication channels and formats in a way that lowers the barriers for small firms. cyberwatching.eu also targets supply-side SMEs in growing niche areas to help them expand market opportunities. A key collaborator for this activity will be ECSO WG4.

3.4.1 Channels & Formats

www.cyberwatching.eu	Tailored content for SMEs including tips on cyber security and risk management. For example, D3.4 Legal guide and practices will be a key deliverable that will be adapted for this audience. The legal tips section already provides key content which targets this audience such as recommendations on how to understand the interplay between the NIS Directive and the GDPR in order to clarify their intricacies, to solve potential conflicts of interpretation
Social Media Channels: Twitter	Tailored messages to raise awareness on benefits of CS&P as a crucial part of the business; offers on the marketplace; insights into cyberspace trends; legal and regulatory information.
Professional Networks: LinkedIn	Recruit and engage with small business professionals. Create and contribute to discussions on cyber security, risk management, privacy and cyber insurance, also asking small

	firms in our network about their top cyber security concerns and practices (and reporting them from f2f interactions). Share takeaway messages from events. LinkedIn Groups like SME Business Growth Forum.
Multiplier Channels	ECSO WG4, Digital SME Alliance, AEI Cibersiguradad, CITIC and partner networks to SMEs, including ICT SME associations across the EU: BASSCOM (BU), IT-FORUM MIDTYLLAND (DK), GPNI (DK), BITMi (DE), CNA (IT), CONECTIC, INCIBE (ES), ClujIT (RO), SwissMedia (CH), UKITA, techUK (UK), STIKK BBS ICT, Vojvodina ICT Cluster (Balkans and Black Sea), http://platforma-msb.org/en/ Associated countries, especially, Ukraine. EU federation of small businesses: BUSINESS EUROPE, AMETIC (ES), AGORIA (BE), Digital Catapult, Innovation UK (UK), Federation of Finnish Technology Industries.
	EIT Digital SMEs through a synergy that has already been established by cyberwatching.eu.
Newsletters	Informative newsletters will be delivered to SME representatives, raising awareness of cyber risks, CS&P best practices, the marketplace and catalogue of services, opportunities to become part of the cyberwatching.eu end-user club.
Videos	Dynamic media for sharing benefits of cyberwatching.eu, interviews at events and testimonials from the SME end-user club members.
Collaterals	Tailored informative brochures; glossaries and guides; business-friendly promotion of relevant cyberwatching.eu assets.
Events	National/regional cyberwatching.eu SME workshops co-located with relevant events across the EU, e.g. trade fairs, major information security events. SMEs benefit from a hands-on approach to CS&P, business-friendly information packs and free access to legal tips to help build a cyber security culture. In addition, SMEs may also be invited to participate at Concertation meetings and also learn about EC policy initiatives and meetings where SMEs are currently under-represented.
Webinars	At least 2 of the 10 cyberwatching.eu will target SMEs, guiding them on best practices for CS&P and guiding them through relevant assets.

Table 4 SMEs dissemination channels and formats

The timeline gives an overview of communication and dissemination activities from M1-18.

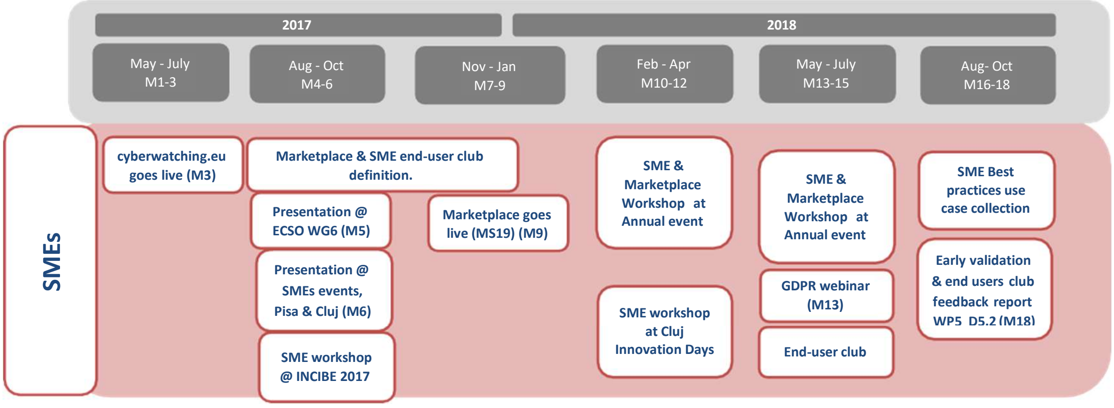

2017
2018
May - July M1-3
Aug - Oct M4-6
Nov - Jan M7-9
Feb - Apr M10-12
May - July M13-15
Aug- Oct M16-18
SMEs
cyberwatching.eu goes live (M3)
Marketplace & SME end-user club definition.
Presentation @ ECSO WG6 (M5)
Presentation @ SMEs events, Pisa & Cluj (M6)
SME workshop @ INCIBE 2017
Marketplace goes live (MS19) (M9)
SME & Marketplace Workshop at Annual event
SME workshop at Cluj Innovation Days
SME & Marketplace Workshop at Annual event
GDPR webinar (M13)
End-user club
SME Best practices use case collection
Early validation & end users club feedback report WP5 D5.2 (M18)

Figure 6 SMEs activity timeline

3.5 Financial Institutions, Insurance Industry and Large companies

This stakeholder group faces several challenges addressed by cyberwatching.eu. Specific needs include:

- Keeping up-to-speed on new CS&P products and services to increase resilience in the complex cyberspace.
- Avoiding increasing costs in the wake of a data breach, as well as damages to reputation, loss of customers, IPR theft, and even negative media coverage.
- Compliance not only with EU legislation, but also regulatory requirements, in cases where data breaches could lead to costly fines.
- Ability to demonstrate best practice implementation to customers as a competitive edge, as well as opportunities to share them with similar companies.
- Keeping up-to-speed with best practices and opportunities in the cyber insurance market.

Major benefits of cyberwatching.eu:

- Quick and easy access to innovative CS&P products and services through the marketplace and catalogue of services as the basis for a sustainable ecosystem.
- Being part of the drive to transform the cyber insurance industry as technologies like IoT, cloud and communication networks advance and converge. cyberwatching.eu can give the insurance industry insightful guidance on IT transformation and best practices.
- A sustainable cyber insurance pilot service as part of the cyberwatching.eu business plan, with opportunities to showcase best practices.
- Guidelines for industry to implement relevant standards and compliance with legislation, helping create a cyber-secure industrial strategy making the EU a leader in cybersecurity & privacy.
- Direct access to the Technology Radar Reports with its state-of-the-art guidelines on CS&P technology, policy, standards and best practices.
- Opportunities to bring their own innovative products and services into cyberwatching.eu and access future funding by bringing closer cybersecurity and privacy supply and demand side in a win-win mechanism.

3.5.1 Channels & Formats

www.cyberwatching.eu	The marketplace and the service offer catalogue entries will be searchable and filterable allowing the top-down search for services related to this group and also based on elements of the taxonomy.

	The website will also include recommendations and raise awareness of risk management and the importance of cyber insurance in particular for SMEs.
Social Media Channels: Twitter	Raising awareness about cyberwatching.eu, sharing insights of interest to this group and promoting outcomes and results from the Technology Radar Report, Marketplace and the Roadmap.
Professional Networks: LinkedIn	Building on current connections covering IT, financial services and insurance companies already in the network. Sharing insights and contributing to discussions, also through relevant LinkedIn groups.
Newsletters	Targeted newsletters will be developed to promote outcomes and results from the Technology Radar Report, Marketplace and the Roadmap.
Videos	Videos promoting the Marketplace and the Roadmap from an Industry perspective will be developed.
Collaterals	Specific graphic material targeting Industry and promoting the benefits of joining cyberwatching.eu and its services.
Events	Participation in the cyberwatching.eu Annual Workshops to gain access to innovative CS&P products and services and contribute to discussions on cyberwatching.eu outputs.
Webinars	1 of the planned cyberwatching.eu webinars targets industry with the expected focus being on GDPR related issues and challenges and the Roadmap.

Table 5 Fintech & large companies dissemination channels & formats

The timeline gives an overview of communication and dissemination activities from M1-18.

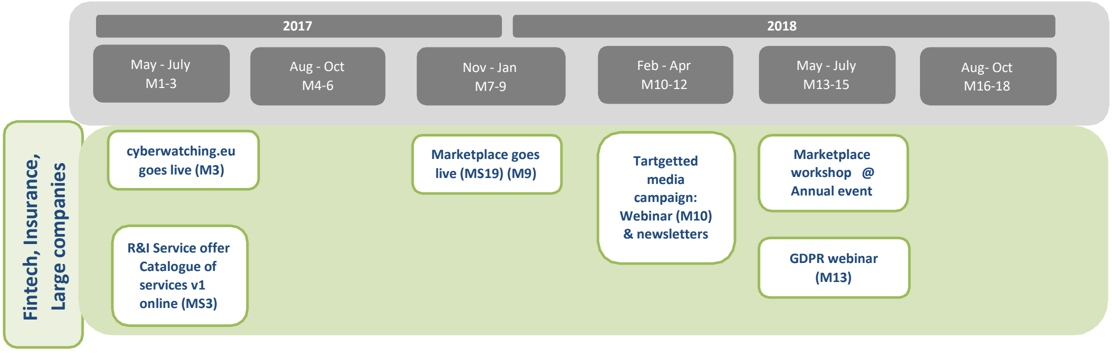

2017
2018
May - July M1-3
Aug - Oct M4-6
Nov - Jan M7-9
Feb - Apr M10-12
May - July M13-15
Aug- Oct M16-18
Fintech, Insurance, Large companies
cyberwatching.eu goes live (M3)
R&I Service offer Catalogue of services v1 online (MS3)
Marketplace goes live (MS19) (M9)
Tartgetted media campaign: Webinar (M10) & newsletters
Marketplace workshop @ Annual event
GDPR webinar (M13)

Figure 7 Fintech & large companies activity timeline

3.6 Cybersecurity & Privacy Cluster Multipliers, Media and Synergies

cyberwatching.eu will leverage diverse types of organisations as multiplier channels to reach major stakeholders and synergies with like-minded initiatives.

- The growing number of cyber security clusters at national and local/regional level across the EU and Associated Countries offer an opportunity to reach the demand side for CS&P. cyberwatching.eu will carry out focused engagement with core members of its collective networks to identify opportunities for promoting the marketplace and other project assets, and to share best practices on key topics.
- IT and information security media channels will be effective in reaching large numbers of representatives from major stakeholder groups, enabling cyberwatching.eu to convey key insights and its assets.

- Synergies with like-minded projects such as EU-Unity (EU-JP) and AEGIS (EU-US), helping to maximise impact by joining forces on communication and stakeholder engagement activities and joint promotion of findings and outputs.

Benefits of cyberwatching.eu

- Providing a unique opportunity of visibility to Cybersecurity & Privacy Clusters, by sustaining their reputation and showcasing their events, projects (national as well as pan-European) and initiatives;
- Avoiding fragmentation by igniting synergies and further opportunities of research and cooperation activities with new partners across Europe;
- Contributing to the creation of a unique European cybersecurity ecosystem by gathering Cybersecurity & Privacy Clusters and all relevant stakeholders in the cyberwatching.eu annual events (see section 4), to foster cooperation with other national and international initiatives (e.g. EC, ENISA, ECSO, National CSIRTs etc.) and maximising outreach to European businesses and citizens.

3.6.1 Channels & Formats

Dedicated website section	Dedicated website section targeting CS&P Clusters will be produced leveraging on the work carried out in D4.2.This includes a catalogue of EU CS&P clusters.
Social Media Channels: Twitter	Targeted messages to clusters, media and project synergies on relevant content.
Professional Networks: LinkedIn	Engagement with relevant LinkedIn groups, drawing the attention also to clusters targeted.
Sample of CS clusters	AT: Cyber Security Austria, CSI; BE: LSEC; CZ: Czeck CyberCrime, NSM Cluster; CY: Cyber Crime Security Forum; DE: TeleTrusT, Bavarian IT Security Cluster; FI: FISC; FR: CNCS, SCS, PÔLE D'EXCELLENCE CYBER, Rennes; HR: FSEC Symposium; IE: CCI; IT: ClusIT, Distretto Cyber Security, Cloud Security Alliance – IT Chapter, Consorzio CINI – Laboratorio Nazionale di Cyber Security; LU: Security Made in LU; NL: NCSC, The Hague Security Delta; PL: FBC; ES: ICT Security and Trust Cluster of the Madrid Network; UK: Cyber Security Forum, Cyber London, Cyber Security Oxford. Baltic Cyber Security Forum (Baltic Area); Nordic IT Security (Scandinavia); International Cybersecurity Forum – FIC (Europe); CSP Forum (Europe); Cyber Security Strategy (Australia).
Sample of IT and Information Security Media Channels	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.
SME media channels	Real Business, Business Insider, StartupNews, Business Matters, Tech City News, Business Zone
Sector specific media channels	The Fintech Times (@theFintechtimes), Fintech Finance, Fintech Forum.
Newsletters	Targeted newsletters will be sent to Clusters identified to ensure timely promotion of Clustering activities and outcomes. Cyberwatching.eu will also leverage the SEREN3 newsletters for this.

Table 6 Clusters dissemination channels and formats

The timeline gives an overview of communication and dissemination activities from M1-18.

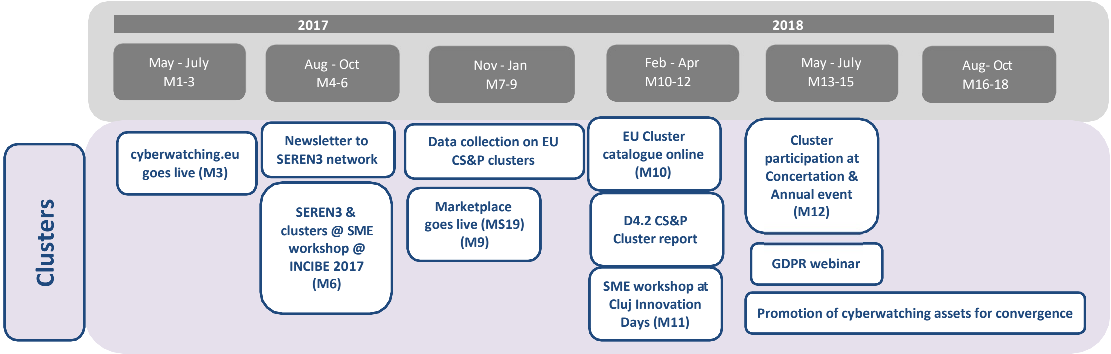

2017
2018
May - July M1-3
Aug - Oct M4-6
Nov - Jan M7-9
Feb - Apr M10-12
May - July M13-15
Aug- Oct M16-18
Clusters
cyberwatching.eu goes live (M3)
Newsletter to SEREN3 network
SEREN3 & clusters @ SME workshop @ INCIBE 2017 (M6)
Data collection on EU CS&P clusters
Marketplace goes live (MS19) (M9)
EU Cluster catalogue online (M10)
D4.2 CS&P Cluster report
SME workshop at Cluj Innovation Days (M11)
Cluster participation at Concertation & Annual event (M12)
GDPR webinar
Promotion of cyberwatching assets for convergence

Figure 8 Clusters activity timeline

3.7 National and Regional Public Administrations

Public administrations face challenges such as:

- Increasing cyber risks with significant socio-economic impact. While high-profile cases of data breaches at public organisations like healthcare facilities and services dominate the headlines, cyber threats are presenting a serious and growing risk to all government organisations at all levels.
- State and local governments need to take action to mitigate cybersecurity risks, and should have a response plan ready in case a breach does occur.
- Need to ensure compliance regarding the protection of personal and sensitive data these organisations hold about citizens, persons etc.

Benefits of cyberwatching.eu:

- Easy access to advanced, new CS&P products, services and solutions thanks to the Marketplace.
- Educating technical and non-technical decision makers on CS&P best practices.
- Guidance on effective CS&P strategy implementation and compliance, including the Cyber Security and Privacy Roadmap, setting out guidelines for industry and the public sector to comply with standards and regulations while highlighting the socio-economic benefits. This will result in coordinated support to the development of a cyber-secure industrial strategy making the EU a leader in cybersecurity & privacy.
- Guidelines presented in Technology Radar Report for industry and the public sector based on the state of the art CS&P technology, policy, standards, and best practices.

3.7.1 Channels and Formats

www.cyberwatching.eu	Cybersecurity best practices and sections such as legal tips will be of interest to this stakeholder group. In addition, services showcased in the service offer catalogue and marketplace may also target this stakeholder group.
Social Media Channels: Twitter	Promoting best practices for a CS&P culture in the public sector; promoting cyberwatching.eu assets and guidelines.
Professional Networks: LinkedIn	Recruit and engage with public sector stakeholders; animate discussions and contribute to relevant LinkedIn groups.
Newsletters	Targeted newsletters will be developed to promote outcomes and results from the Technology Radar Report, Marketplace and the Roadmap.

Collaterals	Specific graphic material targeting National & Regional Public Administrations and promoting the benefits of joining cyberwatching.eu and its services.
Events	Opportunity to attend annual workshop which targets a multi-stakeholder audience and will showcase results from assets such as the marketplace.

Table 7 Public administrations dissemination channels and formats

The timeline gives an overview of communication and dissemination activities from M1-18.

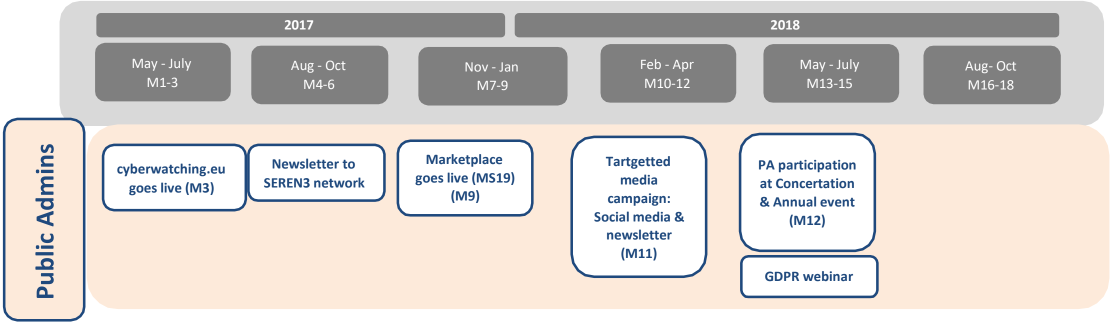

2017
2018
May - July M1-3
Aug - Oct M4-6
Nov - Jan M7-9
Feb - Apr M10-12
May - July M13-15
Aug- Oct M16-18
Public Admins
cyberwatching.eu goes live (M3)
Newsletter to SEREN3 network
Marketplace goes live (MS19) (M9)
Tartgetted media campaign: Social media & newsletter (M11)
PA participation at Concertation & Annual event (M12)
GDPR webinar

Figure 9 Public administrations activity timeline

3.8 Standardisation Organisations

cyberwatching.eu will showcase through its website, social media and professional networks best practices emerging from standardisation organisations (SDOs, SSOs) for cyber risk management, cyber security and privacy.

cyberwatching.eu will ensure all major stakeholders (R&I teams; SMEs, industry and public sector organisations are kept up to speed on the most relevant standards and standardisation efforts, their purpose and why they should be implemented.

Coverage will include not only relevant standards developed in the EU but also internationally, such as new network security standards from organisations such as ISO/IEC; NIST (US National Institute of Standards and Technology), ETSI, ITU, IEEE, OASIS etc.

cyberwatching.eu will thus encourage greater uptake and also increased harmonisation across EU organisations, promoting tangible benefits of standards implementation.

Benefits of cyberwatching.eu:

- Increased awareness of standardisation as a best practice.
- Extended uptake of relevant standards also by R&I teams as a key policy goal for the EU to ensure new products and services are standards compliant.
- Guarantee high visibility of standards best practices through the Catalogue of Standards made available on the website and promoted through dedicated campaigns.
- Timely insights from EAG that are representatives of standardisation organisations, guiding organisations in identifying relevant standards.
- Driving synergies with relevant organisations in the EU, primarily the European Cyber Security Organisation (ECSO) and its WG1 on Standards and Certifications, including multi-stakeholder dialogue and collaboration at cyberwatching.eu or 3rd-party events.
- Contributions to key standardisation EC-funded projects such as StandICT.eu.

Outputs of particular interest include the white paper on cyber security standard gap analysis and the Cyber security & Privacy Roadmap.

3.8.1 Channels & Formats

www.cyberwatching.eu	Dedicated section raising awareness of the benefit of cyber security standards and certification in particular in terms of building trusted services in the Digital Single Market. Reference point for online standards mapping questionnaires targeting EC-funded and national projects. Challenges and outputs from various deliverables will be produced in two phases: an initial draft will be based on activities carried out in WP3, and a final version based on the D3.2 and the SDOs White Paper (M18).
Social Media Channels: Twitter	Promoting best practices emerging from relevant standardisation efforts, meetings and opportunities to contribute. Continuous and extensive social media community development, leveraging the promotion of activities carried out in previous projects.
Professional Networks: LinkedIn	Regular engagement and recruitment of standards specialists. Relevant LinkedIn discussions and groups.
Newsletters	Targeted newsletters will be developed to promote best practices coming from D3.2.

Table 8 Standards organisations dissemination channels & formats

The timeline gives an overview of communication and dissemination activities from M1-18.

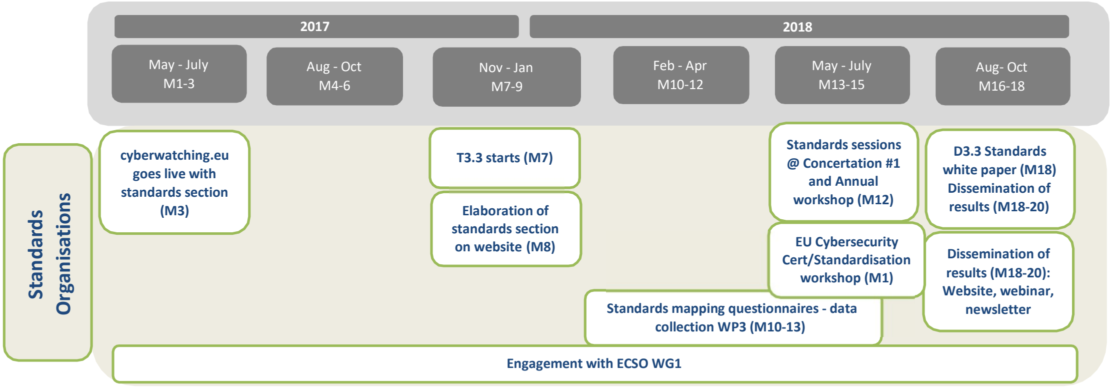

2017
2018
May - July M1-3
Aug - Oct M4-6
Nov - Jan M7-9
Feb - Apr M10-12
May - July M13-15
Aug- Oct M16-18
Standards Organisations
cyberwatching.eu goes live with standards section (M3)
T3.3 starts (M7)
Elaboration of standards section on website (M8)
Standards sessions @ Concertation #1 and Annual workshop (M12)
D3.3 Standards white paper (M18) Dissemination of results (M18-20)
EU Cybersecurity Cert/Standardisation workshop (M1)
Dissemination of results (M18-20): Website, webinar, newsletter
Standards mapping questionnaires - data collection WP3 (M10-13)
Engagement with ECSO WG1

Figure 10 Standards organisations activity timeline

3.9 Policy & Regulators

Policy makers often encounter difficulty in attaining a comprehensive view of CS&P initiatives and their impacts from a socio-economic perspective, as well as understanding how future funding can be channelled for the most effective outcomes. Regulators need an understanding of practices aimed at compliance, as well as reporting data breaches and other issues.

Benefits of cyberwatching.eu

- Contributing to the policy goal of creating a cyber security culture in public and private organisations across the EU and Associated Countries.
- Helping to monitor impact of R&I actions for maximum RoI through the Catalogue of Services and the Clustering activities.
- Shaping future research directions for the DSM. Cyberwatching.eu will ensure key & timely policy insights for monitoring progress of related DSM actions and for shaping future R&I directions.
- Bringing insightful and timely insights through collaboration with ECSO on key CS&P priority topics.

- Providing timely roadmaps on cybersecurity and privacy, regulatory compliance and policy actions, as well as ICT standardisation.

Outputs of particular interest include legal aspects & recommendations and the increased visibility of EU R&I results available to users as innovative CS&P products and services.

3.9.1 Channels and Formats

www.cyberwatching.eu	A dedicated section of the website will focus on Concertation activities and outputs which will help future research directions for the DSM. D3.2 and 3.7 will be key sources of input for these activities.
Social Media Channels: Twitter	Promoting EU cyber security policy framework and recommendations emerging from both the EC and cyberwatching.eu events.
Professional Networks: LinkedIn	Recruit and engage with public sector stakeholders; animate discussions and contribute to relevant LinkedIn groups.
Newsletters	Targeted newsletters will be developed to promote outcomes and results from the Technology Radar Report, Marketplace and the Roadmap.
Collaterals	Specific graphic material targeting policy and regulators; output briefings, including outcomes of synergies with ECSO.
Events	ECSO annual conferences and meetings with timely expert and policy insights reporting on progress towards DSM objectives, actions and measures needed for future R&I directions; as well as direct access to cyberwatching.eu outputs and assets.

Table 9 Policy groups dissemination channels and formats

The timeline gives an overview of communication and dissemination activities from M1-18.

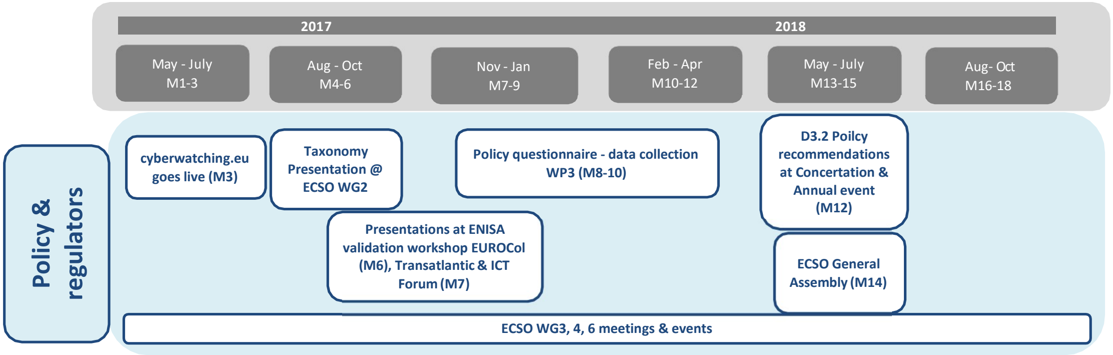

2017
2018
May - July M1-3
Aug - Oct M4-6
Nov - Jan M7-9
Feb - Apr M10-12
May - July M13-15
Aug- Oct M16-18
Policy & regulators
cyberwatching.eu goes live (M3)
Taxonomy Presentation @ ECSO WG2
Policy questionnaire - data collection WP3 (M8-10)
D3.2 Poilcy recommendations at Concertation & Annual event (M12)
Presentations at ENISA validation workshop EUROCol (M6), Transatlantic & ICT Forum (M7)
ECSO General Assembly (M14)
ECSO WG3, 4, 6 meetings & events

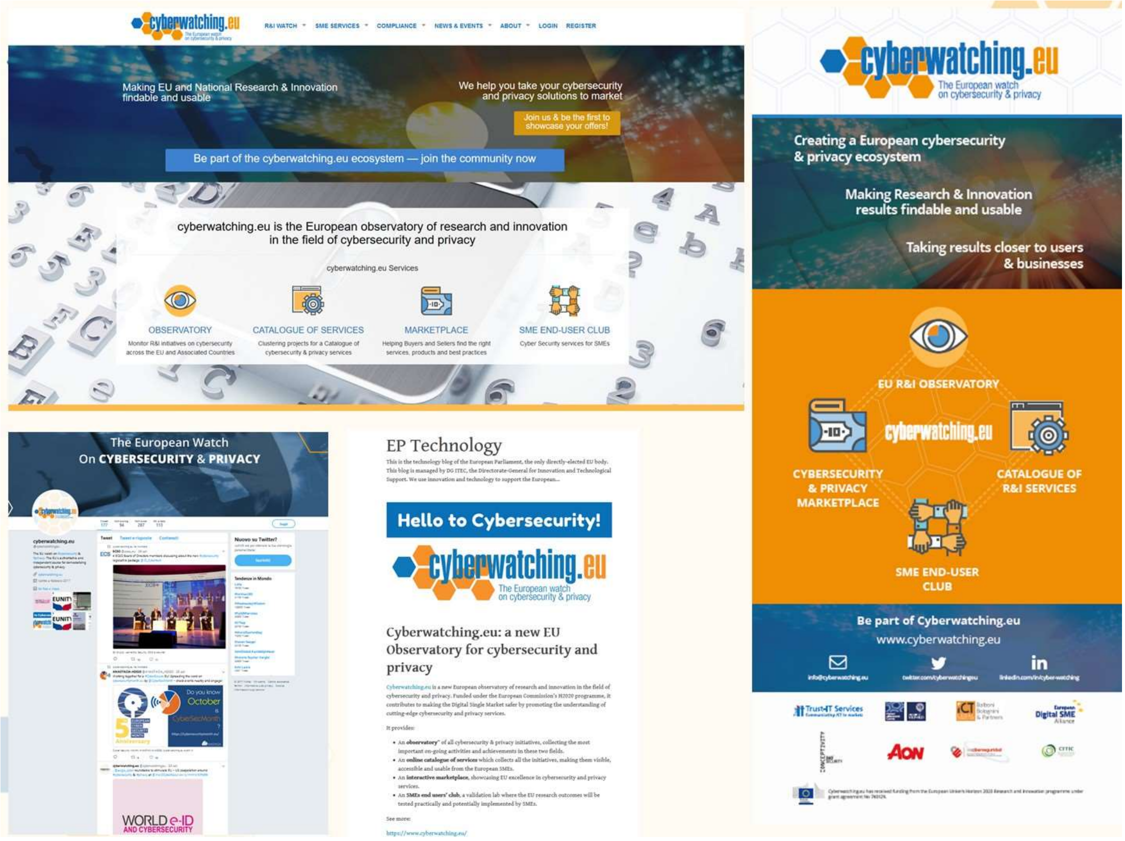
Figure 11 Policy groups activity timeline

4 Branding and printed material

4.1 Current Achievements

cyberwatching.eu has carried out continuous communications from the very outset, setting up the media platform (www.cyberwatching.eu) and social networks, creating collaterals and creating media campaigns on the project launch.

The figure shows a sample of the outcomes achieved so far, including visibility at events (e.g. ECSO), the first Pop up Banner and press coverage of cyberwatching.eu:


cyberwatching.eu
The European watch on cybersecurity & privacy
R&I WATCH
SME SERVICES
COMPLIANCE
NEWS & EVENTS
ABOUT
LOGIN
REGISTER
Join us & be the first to showcase your offers!
Be part of the cyberwatching.eu ecosystem — join the community now
OBSERVATORY
CATALOGUE OF SERVICES
MARKETPLACE
SME END-USER CLUB
The European Watch On CYBERSECURITY & PRIVACY
WORLD e-ID AND CYBERSECURITY
Hello to Cybersecurity!
EU R&I OBSERVATORY
CYBERSECURITY & PRIVACY MARKETPLACE
CATALOGUE OF R&I SERVICES
SME END-USER CLUB
info@cyberwatching.eu
twitter.com/cyberwatchingeu
linkedin.com/in/cyber-watching
Trust-IT Services
Digital SME Alliance
AON
CITIC

Making EU and National Research & Innovation findable and usable

We help you take your cybersecurity and privacy solutions to market

cyberwatching.eu is the European observatory of research and innovation in the field of cybersecurity and privacy

cyberwatching.eu Services

OBSERVATORY: Monitor R&I initiatives on cybersecurity across the EU and Associated Countries

CATALOGUE OF SERVICES: Clustering projects for a Catalogue of cybersecurity & privacy services

MARKETPLACE: Helping Buyers and Sellers find the right services, products and best practices

SME END-USER CLUB: Cyber Security services for SMEs

EP Technology

This is the technology blog of the European Parliament, the only directly-elected EU body. This blog is managed by DG ITEC, the Directorate-General for Innovation and Technological Support. We use innovation and technology to support the European...

Hello to Cybersecurity!

Cyberwatching.eu: a new EU Observatory for cybersecurity and privacy

Cyberwatching.eu is a new European observatory of research and innovation in the field of cybersecurity and privacy. Funded under the European Commission's H2020 programme, it contributes to making the Digital Single Market safer by promoting the understanding of cutting-edge cybersecurity and privacy services.

It provides:

- An **observatory**" of all cybersecurity & privacy initiatives, collecting the most important on-going activities and achievements in these two fields.
- An **online catalogue of services** which collects all the initiatives, making them visible, accessible and usable from the European SMEs.
- An **interactive marketplace**, showcasing EU excellence in cybersecurity and privacy services.
- An **SMEs end users' club**, a validation lab where the EU research outcomes will be tested practically and potentially implemented by SMEs.

See more:

https://www.cyberwatching.eu/

Creating a European cybersecurity & privacy ecosystem

Making Research & Innovation results findable and usable

Taking results closer to users & businesses

Be part of Cyberwatching.eu
www.cyberwatching.eu

Figure 12 cyberwatching.eu dissemination material

In more details, since its beginning cyberwatching.eu has achieved:

- The cyberwatching.eu website online since **M1**
- The Catalogue of Service online since **M1**
- Twitter profile has been created with **337 followers**.
- LinkedIn profile has been created with **128 connections**.
- 1 general Flyer.
- 1 general pop-up banner.
- 1 general presentation.
- 1 press release for the launch of the cyberwatching.eu website.

5 Conclusion

cyberwatching.eu will play an important role in lowering barriers to innovative cyber security and privacy (CS&P) products and services such as those coming from projects funded by the EC, EU member states and associated countries.

This document provides a comprehensive overview of the communication and stakeholder engagement plan for the Cyberwatching.eu project for the first 18 months of the project lifetime. The document provides a full overview of the main project assets and results that will be the focus of communications and dissemination activities led by WP4. A set of KPIs are also presented.

The document also provides a value proposition for each target stakeholder group and a timeline of activities that have taken place in M1-7 and planned activities for M8–18. In addition the communication and dissemination channels that will be used for this are identified.

WP4 is has a key role to play in the project in terms of raising awareness of project results and also of cybersecurity issues to these communities. With a detailed action plan in place devised through both PMB conference calls, consortium Face-to-face meetings and WP4 conference calls, the partners are well organised to deliver this.

www.cyberwatching.eu

@cyberwatchingeu

/in/cyber-watching/

cyberwatching.eu has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740129.