



D5.3 Early validation & end-users club final report

Author(s)	European DIGITAL SME Alliance
Status	Final
Version	1.0
Date	30/07/2021

Dissemination Level

<input checked="" type="checkbox"/>	PU: Public
<input type="checkbox"/>	PP: Restricted to other programme participants (including the Commission)
<input type="checkbox"/>	RE: Restricted to a group specified by the consortium (including the Commission)
<input type="checkbox"/>	CO: Confidential, only for members of the consortium (including the Commission)

Abstract:

Early validation & end-users' club final report refers to the two key outputs of the cyberwatching.eu that are designed for the end-users: cyberwatching.eu Marketplace and SME end-user club. The purpose of this document is to report on the main developments regarding services provided for the end-users, analyse their needs and the feedback received from the SMEs, and to provide recommendations for the future.



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.

Document identifier: Cyberwatching.eu – WP5 – D5.2

Deliverable lead	European DIGITAL SME Alliance
Related work package	WP5 Market Approach and Sustainability
Author(s)	Sebastiano Toffaletti, Justina Bieliauskaite, James Philpot (DIGITAL SME)
Contributor(s)	-
Due date	30/06/2021
Actual submission date	30/07/2021
Reviewed by	Nicholas Ferguson, TRUST-IT and Marina Ramírez Jiménez, AEI
Approved by	cyberwatching.eu project consortium
Start date of Project	01/05/2017
Duration	51 months

Revision history

Version	Date	Authors	Notes
V0.1	03 June 2021	James Phillipot (DSME)	Review and work on of the feedback report delivered in M18; first early draft for the final version (structure, definition of key chapters, etc.)
v0.2	18 June 2021	James Phillipot and Justina Bieliauskaite (DSME)	Main chapters drafted
v0.3	24 June 2021	Sebastiano Toffaletti (DSME)	Internal review, small corrections
v0.4	23 July 2021	James Phillipot and Justina Bieliauskaite (DSME)	Additions based on information collected through the SME workshops
v0.5	27 July 2021	Nicholas Ferguson (Trust-IT)	Internal review
v0.6	28 July 2021	Marina Ramírez Jiménez (AEI)	Internal Review
V0.7	28 July 2021	Justina Bieliauskaite (DIGITAL SME)	Addressing reviewers' comments, final changes and corrections
V1.0	30 July 2021	Nicholas Ferguson (Trust-IT)	Final version & PMB review

Executive Summary

SME end-user club and the Marketplace have been initially defined as key assets of cyberwatching.eu. Both of them aimed to provide services to the end-users of the project, namely European small and medium enterprises (SMEs). However, during the evolution of the project, following the continuous SME needs assessment and user experience feedback, the two concepts have closely merged into a unified cyberwatching.eu service offer to SMEs, offering multiple SME tools and services 'under one roof'.

For this reason, the purpose of this document is to report on the main SME-targeted developments, tools and services provided for the end-user SMEs, explain their needs and feedback, and provide recommendations for the future.

Table of Contents

1	Introduction	6
2	SME needs	7
3	Cyberwatching.eu SME end-user community: tools, services and the Marketplace	10
3.1	SME end-user club: value proposition.....	11
3.2	SME end-user club: assets for SMEs (developed tools & services)	12
3.2.1	GDPR Temperature Tool	12
3.2.2	Cybersecurity Self-assessment for SMEs	13
3.2.3	Cyberwatching Information Notice Tool	13
3.2.4	Cyber Risk Temperature Tool	14
3.2.5	Cybersecurity Label	14
3.2.6	SME Guides	15
3.2.7	SME success stories	18
3.3	SME end-user club: SME workshops	20
3.3.1	First SME workshop in ENISE11 (Leon, Spain)	21
3.3.2	Second SME workshop: workshop with ENISA.....	22
3.3.3	Third SME workshop in it-sa cybersecurity fair	23
3.3.4	Fourth SME workshop: Cyber Investor Days	24
3.3.5	Fifth SME workshop on Teleworking during COVID-19.....	25
3.3.6	Sixth SME workshop: 5G vs Cable: Benefits & Security Risks.....	26
3.3.7	Seventh SME workshop: use and value of the cybersecurity labels for SMEs 27	
3.3.8	Eighth SME workshop. ePrivacy Regulation: what's an impact on SMEs?..	29
3.3.9	Ninth SME workshop: SCHREMS II & DATA TRANSFERS - Decision & Impact on SMEs	30
3.3.10	Tenth SME workshop. Cybersecurity Competence Centre Pilot Projects: SME Impact and Opportunities.....	31
3.4	Cyberwatching.eu Marketplace: value proposition, state-of-the-art and a way forward	32
3.4.1	The cyberwatching.eu Marketplace value proposition	32
3.4.2	Cyberwatching.eu Marketplace: state-of-the-art.....	33
3.4.3	Cyberwatching.eu Marketplace: a way forward.....	36
4	Promotion activities of the Marketplace and SME assets.....	37
4.1	Channels	37
4.1.1	Collaboration with ECSO WG4	39
4.1.2	Events	40
5	Conclusions: validation & future recommendations.....	42

TABLE OF FIGURES

Figure 1 GDPR Temperature Tool	12
Figure 2 Example of cybersecurity self-assessment questionnaire	13
Figure 3 Information Notices Tool	14
Figure 4 Cyber Risk Tool	14
Figure 5 The Cybersecurity Label	15
Figure 6 Essential Guide on Cyber Risk Management.....	15
Figure 7 10 steps for a Cybersecurity-beginner SME	16
Figure 8 Cost of Cyber Insurance	17
Figure 9 10 cybersecurity tips for teleworking	17
Figure 10 SME success stories' gallery: SMEs using cybersecurity and privacy R&D results.....	19
Figure 11 Examples of SME success stories in cyberwatching.eu social media.....	19
Figure 12 Programme of the first SME workshop.....	21
Figure 13 Moments from the first SME workshop.....	22
Figure 14 SME workshop on Security of Personal Data Processing with ENISA.....	23
Figure 15 Moments from the cyberwatching.eu SME workshop in it-sa fair.....	24
Figure 16 Moments from the Fourth SME workshop	25
Figure 17 Promotion of the Fifth SME workshop	26
Figure 18 Sixth SME workshop '5G vs. Cable'	27
Figure 19 Seventh SME workshop. Cybersecurity: use and value of the cybersecurity labels for SMEs.....	28
Figure 20 Eighth SME workshop - promotional banner	29
Figure 21 Moments from the eighth SME workshop.....	29
Figure 22 Ninth SME workshop - communications banner.....	30
Figure 23 Moments from the ninth SME workshop.....	31
Figure 24 Tenth SME workshop promotional banner	31
Figure 25 Moments from the tenth SME workshop	32
Figure 26 cyberwtaching.eu Marketplace landing page.....	34
Figure 27 cyberwatching.eu Marketplace registration form	34
Figure 28 cyberwatching.eu Marketplace benefits explains.....	35
Figure 29 cyberwatching.eu Marketplace solutions.....	36

TABLE OF TABLES

Table 1 SME needs	10
Table 2 List of channels used to promote cyberwatching.eu Marketplace and SME end-user club	39
Table 3 cyberwatching.eu SME assets - key benefits and recommendations	42

1 Introduction

Cybersecurity has, undoubtedly, become one of the leading priorities for the European Union (EU): from security of the small business throughout the EU, to the fight of international cyber-crime, cybersecurity topics dominate the EU agenda. Research and innovation aren't an exception. Since 2013, when the European [Cybersecurity Strategy](#) has been released, the European Commission (EC) has committed to use Horizon 2020 programme in order 'to address a range of areas in ICT privacy and security, from research and development to innovation and deployment'¹. In addition, the further commitment has been made to better coordinate the research agendas between the EU-funded projects and the Member States. Later in 2017, an adoption of the so-called '[Cybersecurity package](#)' has confirmed EU's engagement into cybersecurity research and development by announcing a creation of the cybersecurity competence network and the coordinating European Cybersecurity Research and Competence Centre.

In this context, cyberwatching.eu was launched in 2017 to take up the challenge of monitoring EU and member states' research agendas and project results, creating a platform (the cyberwatching.eu Marketplace) that would bring together cybersecurity demand and supply players, as well as supporting the uptake of cybersecurity and privacy products created by the EU-funded projects. To achieve the latter, cyberwatching.eu has proposed a number of actions, the center of which has been a creation of a cybersecurity marketplace and an SME end-user club which facilitate the dialogue between the EU research and development (R&D) community (both – EU projects, researchers, but also innovative SMEs performing R&D) and the end-user SMEs across the EU.

Through the 50 months project-lifetime until this date (it refers to a delivery time of this deliverable, while a full life-time is 51 months), numerous policy developments in cyber-security landscape have taken place. While a more detailed overview is provided in the D4.7 EU Cybersecurity & Privacy Final Roadmap, it is important to mention those which have had an important impact on SMEs (it is a high-level overview, not an exhaustive list):

- introduction of the EU General Data Protection Regulation (GDPR) in May 2018;
- EU Cybersecurity Act of 2019;
- EC Recommendations of March 2019 to ensure a high level of cybersecurity of 5G networks across the EU, and the resulting 5G toolkit (January 2020);
- New EU Cybersecurity Strategy and NIS2 Directive which were both proposed simultaneously in December 2020;
- ePrivacy proposal (not adopted yet, but having caused a lot of discussions and debates upon its negotiations),
- etc.

All these policy developments, changing requirements and newly emerging needs of customers, as well as consumer awareness and appeal for more privacy and security, have created an urgent need among the SMEs for improved services, solutions which consider cybersecurity and privacy. These aspects have become a selling point for multiple companies which learned to successfully incorporate cybersecurity and privacy by-design to their offers.

¹ https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

However, at the same time, not all SMEs were able to benefit from the opportunities that emerge from this fast-changing approach to security and privacy. Numerous small companies, especially those in traditionally 'analogue' sectors, have been struggling to navigate among different requirements and remain competitive.

This is where cyberwatching.eu has also been instrumental supporting SMEs in their pursuit of advice and guidance to cybersecurity. In this regard, SME guides, tailored SME workshops, thematic webinars and practical tools (such as GDPR Temperature tool, cybersecurity self-assessment tool, cyber risk temperature tool, Information notice tool, Cybersecurity Label) were developed.

This early validation & end-users' club final report, therefore, refers to the key outputs of the cyberwatching.eu which target SMEs. The document aims to report on the main developments and achievements facilitating services for the end-users, analyse the SME needs and feedback received from them, and to provide some insights on potential future actions, supporting SMEs.

This document is comprised of five sections. The first (chapter 2) provides an overview of the needs of SMEs regarding the services provided by the cyberwatching.eu. The second section (Chapter 3) provides details on the tools and services developer for the SMEs, and their value to the SME community. The third section (Chapter 4) reports on the promotion and SME consultation activities taken up by the partners involved, while the fourth final part (Chapter 5) evaluates the feedback coming from the SME users and provides recommendations for the future activities.

2 SME needs

Around 99% of European companies are small and medium enterprises, which are still particularly vulnerable in case of cybersecurity incidents. 60% of all cyber-attacks or breaches are aimed at SMEs, while 68% of them do not have any systematic approach for ensuring cybersecurity in their company². Therefore, European SMEs are one of the main target stakeholders of cyberwatching.eu

It is important to distinguish the two very different types of SMEs that exist in cybersecurity environment:

1. **SME providers** (also called vendors or suppliers) – SMEs that are developing cybersecurity solutions (products or services) themselves. They are mostly highly specialised in one area and do not offer the whole range of cybersecurity solutions. These SMEs often operate in specific niches in domestic markets, with low levels of internationalisation³.
2. **SME users** – ICT-intensive SMEs that use (or could potentially use) cybersecurity solutions. These can be any SMEs, in any sector, typically having low in-house capacities and possibly lower understanding and skills in the field of cybersecurity. They need to buy 'ready-to-use' cyber security products and services. Such services do not include only off-the-shelf software but also many tailored services, such as bishop software and consultancy.

These users can be further broken down into two categories:

² <https://www.smesec.eu/>

³ <http://ecs-org.eu/documents/ecs-cppp-industry-proposal.pdf>

- a. **SMEs** that already operate in ICT or another highly digitised sector, and are rather mature users of cybersecurity solutions (e.g. SMEs offering cloud services – they do not produce cybersecurity solutions by themselves, but use already made services in their daily work),
- b. **SMEs** that normally do not use any cybersecurity solutions, or use only very primitive ones (e.g. hairdresser salon which uses malware software in her/his computer).

For the development of fruitful and effective services for the SMEs, such as the Marketplace and SME end-user club, it is crucial to analyse SMEs' needs that greatly vary from those of large companies. Therefore, led by European DIGITAL SME Alliance (DSME) as part of T5.3, partners took the initiative to engage with SMEs and SME associations in order to understand SMEs' needs and requests regarding the proposed services. It is important to note that SMEs were asked not about their needs in cybersecurity in general, but rather about the specific tools & services that were already offered by cyberwatching.eu or were under development at the time of communication with the SMEs. Most of the gathered feedback concentrated on the following aspects:

1. how the Marketplace and SME end-user club should be designed
2. what and information and additional services should be provide through the end-user club or the Marketplace
3. what added value for business it should create in order to be attractive for the end-user
4. what additional components/tools/services SMEs want to find within the SME end-user community, and how they evaluate those offered to them by cyberwatching.eu

This broad consultation exercise was carried out through informal talks and face-to-face discussions with SMEs and their representatives. Namely, feedback and comments were collected via Q&As and discussions during 8 SME workshops, webinars, dissemination & outreach events. During these activities cyberwatching.eu gave presentations, and held face-to-face meetings with the SMEs and their multiplier organisations, such as SMEUnited, ECSO Working Group 4 (Support to SMEs, coordination with countries and regions) meetings, European DIGITAL SME Alliance's General Assembly, etc. (extended list of the events is provided in the chapter 4).

The main SME needs identified and the comments received from the SMEs are summarised in the table below.

SME needs	SME providers	SME users
Information on cybersecurity landscape	<ul style="list-style-type: none"> • Would like to know more about innovative solutions developed by research community • Understand the key trends and follow the latest innovation in the market • Find out about potential of participating in EU-funded cybersecurity activities 	<ul style="list-style-type: none"> • Would like to know more about cybersecurity and privacy in general • Are interested in existing free solutions or consultations • Prefer information to be easily presented, not very technical • Need guidance among variety of tools, services, solutions
Registration	<ul style="list-style-type: none"> • Fast and simple, respecting GDPR principles 	<ul style="list-style-type: none"> • Fast, simple, not very technical questions

Cybersecurity services to be offered in the Marketplace/ end-user club	<ul style="list-style-type: none"> • Chance to access innovative, new solutions that are not yet widely used elsewhere • Possibility to incorporate offered solutions in its own products/services • Get discounts/ special offers • Wide choice of solutions which are easy to search & filter • Possibility to contact other providers (in case of potential complementarities) 	<ul style="list-style-type: none"> • Simple and easy-to-use solutions that do not require much of a <i>priori</i> knowledge • Guidance to navigate between different solutions ('how to know what my company needs?') • Possibility to get special offers or free / discounted solutions
Level of engagement with cyberwatching.eu	<p>Ready to engage, especially in the following cases:</p> <ul style="list-style-type: none"> • Where visibility is ensured (e.g. participate at events, webinars, submit solution to the Marketplace) • Funding is available (e.g., information on funding opportunities presented, potential to meet investors, etc) • Other concrete benefits for the company are defined (e.g., relevant information on regulations or standards provided) 	<p>Interested in engaging with cyberwatching.eu, but some considerations are made:</p> <ul style="list-style-type: none"> • Linguistic barriers for some companies (content in other languages could be provided) • Information has to be easy and understandable in order to engage (less technical language when speaking about cybersecurity) • Some initial guidance among different cybersecurity solutions is provided (e.g., where to start, what solutions is my company missing to be compliant, what to look for, etc.)
Visibility	<p>Would benefit from additional visibility, would like to be presented as cybersecurity solution providers, offering innovative solutions, leading the European cybersecurity market, and as providers complying with the European privacy requirements and consumers' needs.</p>	<p>Would benefit from additional visibility: would like to be presented as company ensuring at least the basic essential cybersecurity and privacy standards related to its services.</p>
Networking	<ul style="list-style-type: none"> • Would benefit from networking with other providers or research community • Is interested in getting involved to EU cybersecurity R&D&I activities; interested in events targeting the potential clients 	<ul style="list-style-type: none"> • Are interested in meeting providers of cybersecurity solutions, including consultants who could give some advice specific for their own business

Pricing	<ul style="list-style-type: none"> • Are ready to consider paying registration fee amounts (e.g. up to EUR 2,000 per year) in exchange for visibility services that can contribute to their marketing strategies, or help reaching more potential clients; • are ready to consider paying registration fee amounts (e.g. up to EUR 2,000 per year) in exchange of networking with other European cybersecurity front-runners and innovative solution providers; • Having information about R&D projects results is important to understand the latest innovation trends, but is not perceived as the first priority; companies would be ready to pay only if this is coupled with other services (e.g., the two listed above). 	<ul style="list-style-type: none"> • Are not always eager to pay: not many companies are ready to invest to cybersecurity, or would invest a limited amount. Decision usually depends on the digital maturity level of the company, and many other internal factors (general awareness and understanding, senior managers' approach to cybersecurity, etc.); • Many companies tend to prefer free downloadable solutions, or at least trials first. However, easy-to-use, SME-friendly solutions which increases an overall level of cybersecurity could be paid; • Are ready to consider paying a small fee to improve its standing in the market and its image among the potential clients, showcasing itself as a compliant, cyber-secure and privacy-preserving company.
----------------	---	---

Table 1 SME needs

cyberwatching.eu services and tools for SMEs, including the Marketplace and SME end-user club, have been developed keeping in mind this early analysis of the SME needs, and taking into consideration different needs, coming from different types of SMEs.

3 Cyberwatching.eu SME end-user community: tools, services and the Marketplace

As explained above, the cyberwatching.eu Marketplace and SME end-user club were initially developed as two closely inter-related but separate concepts (see M18 report). Within the initial understanding, the separate registrations were needed for both, which was confusing for SMEs and discouraged them from two different registrations. Given feedback received from SMEs, the registration was unified – Marketplace registration form has been the unique form for interested companies to register. Meanwhile, the cyberwatching.eu platform was populated with additional tools and services, specifically targeting SMEs and their needs, therefore, becoming one single community access point. In addition, some documents were made available only for the users registered to the Marketplace.

This approach serves a two-fold goal: 1) it allows more SMEs to access the content designed for them without additional registration barriers; 2) it allows to attract more potentially interested SMEs to first explore the content and then, if interested, also register to the Marketplace.

Therefore, the SME end-user community revolves around the numerous tools and services, most of which can be easily accessible through one click to each interested SME, while further functionality of the Marketplace requires SMEs' registration.

3.1 SME end-user club: value proposition

The SME end-user club has been developed with the main goal in mind: to engage SME end-users as early validators, and give them access to the top cybersecurity innovations developed in Europe: through the Marketplace, as well as providing deeper overview of R&D solutions in the projects' catalogue. However, numerous other needs were identified, while engaging with the SME community, especially, a need for guidance and initial advice, support navigating and choosing in a variety of solutions (what is crucial for a cybersecurity beginner? Where to start?). For instance, if an SME is interested in GDPR requirements, but doesn't know where to start, it could use guiding tools in cyberwatching.eu first, receive advice on its main weaknesses, and then explore the solutions which could help to avoid these.

Therefore, the approach to the end-user club and its function has been expanded, offering variety of different tools and SME guidebooks, as well as success stories of SMEs leading cybersecurity production and adoption in Europe. Having captured an SME's attention, they are then provided with necessary initial awareness about cybersecurity and their needs, other existing solutions and providers, etc., which then leads them towards the Marketplace where they can find the needed solutions, meet the providers, find partner companies.

To sum up, the further value proposition for SMEs has evolved within the cyberwatching.eu:

- For the SME users:
 - Free tools and services (such as guidebooks, GDPR Temperature tool, Cyber Risk Temperature tool, informative webinars and SME workshops, etc.) which help SMEs to assess their needs and understand what solutions they need to look for;
 - Access to cutting-edge cybersecurity and privacy solutions and services;
 - Chance to contact providers of cybersecurity solutions, in some instances also get trained about their usage, or get solutions also tailored towards their need (it is often the case for those solutions offered by cybersecurity projects – e.g., cyberwiser, one of the solutions provided in the Marketplace, offered specialised tailored consultations for SMEs).
- For the SME providers:
 - Opportunity to get visibility to their own solutions and display them in the Marketplace, therefore reaching new potential clients and showcasing their solutions to other innovative providers;
 - Access to cutting-edge cybersecurity and privacy solutions and services, as well as a possibility to understand the main trends;
 - Chance to engage with the key cybersecurity and privacy projects in Europe in various forms: test their services and solutions, get to meet them and learn how to join their community, use their solutions and promote such good practice in cyberwatching.eu;
 - Networking with the relevant cybersecurity actors (e.g., in SME workshops, project's final conference, other international cybersecurity events, etc.);

- Latest information and learning opportunities about the specific aspect of cybersecurity and its regulation (e.g., in SME workshops and webinars).

In addition, all the SMEs, be they cybersecurity solutions' providers or users, could find the following services of the cyberwatching.eu beneficial:

- Possibility to directly contact cybersecurity providers;
- Visibility to the company, e.g., through the "user profile" published in the website, through the social media, success stories, etc;
- free access to tools and guidance from cyberwatching.eu experts on legal aspects of privacy, cyber insurance and certification;
- Visibility opportunities participating in cyberwatching.eu events, offering articles and blog posts, etc;
- Invitation cyberwatching.eu events, webinars, workshops;
- Multiple free-of-charge or reduced-price tools targeting different needs (listed in the section below).

3.2 SME end-user club: assets for SMEs (developed tools & services)

Based on SME needs, identified throughout the project, a set of various assets for SMEs was developed, as it has already been explained above. This section provides an overview of the developed tools and their value for SMEs.

3.2.1 GDPR Temperature Tool

Developed by the ICT Legal, the [GDPR Temperature Tool](#) helps European SMEs to evaluate their GDPR Temperature. The tool can be used as an important preliminary step for SMEs to facilitate their understanding of how they should behave in order to be GDPR compliant and to avoid the risk of sanctions. By answering a set of questions on data processing activities, an SME receives an indication of the company's risk to sanctions, and a customised set of practical and actionable recommendations. The higher the temperature – the higher the risk.

The whole process to complete the questionnaire takes around 15 minutes, while the language used in the questionnaire has been adopted to fit SME needs and avoid legal jargon (terms which might be unknown to SMEs are additionally explained).

During the lifetime of the project, SMEs which have answered the GDPR questionnaire also had a possibility to meet ICT Legal experts and get further advice or guidance, ask relevant questions (during [SME workshop on 10 of May](#), 2021 and the dedicated closed (only for SMEs who used the tool) webinar on 20 July, 2021).



Evaluate your risk of GDPR-related sanctions

Figure 1 GDPR Temperature Tool

3.2.2 Cybersecurity Self-assessment for SMEs

The [Cybersecurity self-assessment tool](#) was developed in collaboration with CyberSec4Europe, CYBERWISER.eu and SMESEC projects, in order to evaluate company's cybersecurity preparedness and to increase awareness on the main aspects to be considered.

Using the tool, SMEs can easily pinpoint security gaps and best practices that should be regularly followed through in terms of: office firewalls and Internet gateways; secure configuration; software patching; user and administrative accounts best practices; malware protection; awareness of password weaknesses and basic risk assessment. The self-assessment can be completed in less than 15 minutes, and having received a score of 50% or more, companies can also acquire a certificate!

Such tool was very appreciated by the representatives of the SME associations (members of SMEUnited), where the tool was presented on the 15 April, however, it was stressed that for cybersecurity-beginner SMEs it would be very helpful to have such tools translated to their local languages, that would ensure much better reach to companies who often do not operate in English, and might have difficulties understanding technical vocabulary in language other than their mother tongue.

The Cybersecurity Best Practices For SMEs Assessment

You have spent 31 sec of 5 min on this page and 31 sec of 30 min in total.

1. Do you have firewalls at the boundaries between your organisation's internal networks and the internet?

☐ Yes
☐ No

2. When you first receive an internet router or hardware firewall device it will have had a default password on it. Has this initial password been changed on all such devices?

☐ Yes
☐ No

3. Is the new password on all your internet routers or hardware firewall devices at least 8 characters in length and difficult to guess?

☐ Yes
☐ No

4. Do you change the password when you believe it may have been compromised?

☐ Yes
☐ No

Page 1 of 13

Next

Figure 2 Example of cybersecurity self-assessment questionnaire

3.2.3 Cyberwatching Information Notice Tool

Another tool developed by the ICT Legal team is the [Information Notice Tool](#). It helps companies to comply with the GDPR requirements (articles 13 and 14) and inform their customers about data being collected. The tool was created reacting to the repeating inquiries and questions of SMEs, related to their Privacy Policies and data protection notices on their websites.

The tool provides a practical checklist that includes all the elements legally required to be presented to the user. It helps companies to improve their transparency towards consumers and avoid fines that may result from misconduct that is not in line with the GDPR requirements. In addition, the tool allows all users to download a report with

information and recommendations in which are included practical steps to be followed, in order to change and improve their current privacy notice.



Figure 3 Information Notices Tool

3.2.4 Cyber Risk Temperature Tool

[The cyber risk temperature tool](#) is another item designed by cyberwatching.eu partner AON. It serves SMEs to get a first understanding of the cyber risks threatening their organisation, and pave the way for putting in place correct risk assessment processes.

The provided questionnaire consists of two main parts: in the first one, the respondent is asked to give a personal assessment of one's company's IT security; while the second part features more technical questions, mainly concerning company's security and cybersecurity strategy. Through the attribution of a score, SMEs are assigned to different profiles according to their level of vulnerability and receive a preliminary cyber risk assessment.

Using this tool, SMEs are encouraged to: assess their specific knowledge of the cyber security within the company; evaluate the methodologies followed within the company; estimate the distribution of administrative fees on the systems; consider the information segmentation policy; check the authentication policies for access to corporate systems; reevaluate assessments carried out previously.



Figure 4 Cyber Risk Tool

The tool complements SME guidebooks discussed in the previous section (especially, the one in cyber risk management), and allows to practically implement some of the tips provided there. After having completed their cyber risk assessment, SMEs are invited to further check information about cyber insurance and its pricing, also available for SMEs on cyberwatching.eu.

3.2.5 Cybersecurity Label

Developed in partnership between SGS, AEI and Trust-IT the [Cybersecurity Label](#) is a vital step in understanding the critical assets a company should protect to run its business, which assets are critical for customers, and to diligently assess all processes and procedures. The Cybersecurity Label is an online tool which has been implemented as a simple online questionnaire. Responses are evaluated according to 8 domains which are the starting point of the general process of certification. This

covers requirements in fields such as software, protocols, services, hardware, infrastructure, security policy, external providers and critical business products. The self-assessment is built on relevant parts of key standards such as ISO 27001, 22301 and the NIST directive. It is essential to help a small business assimilate clear concepts and smooth the path to further action. In the short-term, the report obtained as a result of the self-assessment, will allow companies to implement simple cybersecurity measures to improve their cybersecurity status, without the help of third-parties. In the long-term, the same report will allow companies to save time, money and avoid frustration in their journey to either enable certification or improve compliance to regulations. Additionally, those entities that manage to trespass the defined threshold and obtain the label may use the Mark designed for this purpose, giving them a certain competitive advantage in relation to the security offered by their digital products and services, endorsed by the entity that designed the questionnaire, SGS.



Figure 5 The Cybersecurity Label

3.2.6 SME Guides

Four SME Guides were produced within cyberwatching.eu (<https://cyberwatching.eu/smes-guides>), three of them are only available for the SME users, registered to the cyberwatching.eu, as one of additional motivations for SMEs to register.

3.2.6.1 Essential Guide on Cyber Risk Management

[The Essential Guide on Cyber Risk Management](#) was developed by AON (with contributions from TRUST-IT and DIGITAL SME) to guide SMEs through the risk management process. The Guide explains the key steps SMEs need to take in order identify risks, assess them, and then define possible mitigation measures. Finally, it also provides an overview of potential actions which help SMEs to decide what to do about the residual risks, e.g. – choosing the cyber insurance!

A need for such guidance has been identified already during the first webinar dedicated to cyber risk management ([October, 2018](#)). Although there are different tools and services, helping SMEs to monitor and manage the risks, there is no chance to guarantee 100% protection, therefore, the SMEs have to be able to understand the risks and realise that no matter what tools they would use, some risks

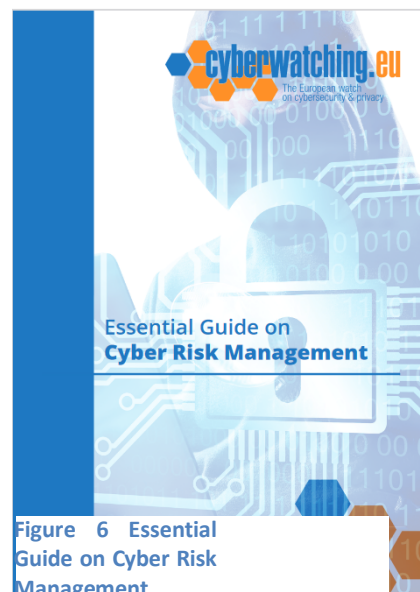


Figure 6 Essential Guide on Cyber Risk Management

will always remain and they have to be ready for it. The processes explained to SMEs in this Guide, help them to understand this in an easy and SME-friendly language, and support their decision making regarding the residual risks.

3.2.6.2 10 steps for a Cybersecurity-beginner SME

DIGITAL SME, after having consulted its members, cybersecurity front-runner SMEs, has developed the basic guidance for all SMEs who have not yet adopted a strategic approach to cybersecurity.

This guidebook titled [10 steps for a Cybersecurity-beginner SME](#), looks at the essential steps which any company should take to ensure the basic level of cyber resilience. The guidebook is meant to support companies in more traditional sectors, just starting their digital transition, to make informed decisions and ensure the baseline level of cybersecurity. In addition, the guidebook raises SME awareness about the main aspects of cybersecurity – while implementing the suggested steps, all SMEs, independently from their digital maturity, are able to notice new aspects of security which they might have never considered before. Having completed the 10 described steps, all SMEs should be able to notice their main vulnerabilities and understand in which areas they would need further external support/advise.

Recently, also ENISA has [published a similar guidebook](#) for businesses, providing 12 steps to secure the businesses. This step by ENISA demonstrates that there is a high demand and need for such guidance because many companies, especially the SMEs, still need support to make the first steps to ensure the necessary basic level of cybersecurity.



Figure 7 10 steps for a Cybersecurity-beginner SME

3.2.6.3 Cost of Cyber Insurance

Another guidebook offered to the SMEs by AON is called [Cost of Cyber Insurance](#). This guidebook has been developed as a follow-up to the multiple questions which SMEs were raising through cyberwatching.eu events once being introduced to cyber insurance as one of the means to manage residual risks within the companies.

As cyber insurance is still rather a novel practice, compared to, for instance, typical liability insurance, and SMEs do not have resources to hire consultants and advisors in this area, some of the most common questions were raised around the price (policy premium) of cyber insurance, existing choices of insurance policies, the exact coverage of such insurance, etc. This guidebook is designed to provide the first preliminary information on these matters, which would help SMEs to make the first decision whether it is worth pursuing further information and investing into such insurance.



Figure 8 Cost of Cyber Insurance

The key information from this Guidebook is further support by the Cyber Insurance FAQs published in the dedicated section of cyberwatching.eu (<https://cyberwatching.eu/cyber-insurance-faq>).

3.2.6.4 10 cybersecurity tips for teleworking

Finally, the forth guidebook for SMEs has been developed as an additional output from the SME workshop [Teleworking during COVID-19: good practices and tips for cybersecurity](#) (25 May, 2020). This SME workshop was organised in French in order to address the specific audience of French SMEs who, due to linguistic barriers, cannot always attend SME workshops. However, in order to extend the main results of the workshop, the expert speakers have put together a three-pager with the main tips for companies around Europe (and globally).

This guidebook is now available in English and is not limited to the registered SMEs, with an aim to these essential tips accessible to all companies.



Figure 9 10 cybersecurity tips for teleworking

3.2.7 SME success stories

As one of its key goals, cyberwatching.eu aims to encourage SMEs to use cybersecurity and privacy R&D results obtained from the EU-funded projects. Although the commercialisation and uptake of the EU project results is quite low, especially in the SME community, the innovation front-runner companies start to understand the value of it. Innovative and high-quality cybersecurity research outputs, integrated within ambitious business offerings, foster innovation and allow better use of internal resources. However, many European SMEs still lack awareness about the possibility to use EU-funded project results, and the benefits that come with it. Therefore, as one of the measures to improve it, the cyberwatching.eu consortium committed to collect best practice examples from SMEs already adopting such practice, inspiring their peers to follow this path too.

The SME best practices were identified by contacting projects who already expose their results in the Marketplace and asking about their result exploitation examples, engaging with SMEs which participated in cyberwatching.eu SME workshops, webinars, concertation meetings and other events, and contacting SMEs who registered at cyberwatching.eu platform. As a result of these activities, 10 SMEs were selected to share their experience and tell about business benefits they got from using cybersecurity and privacy R&D results. The SMEs were selected keeping in mind their geographic distribution (to showcase examples from different parts of Europe), different sectors which they are working in (IoT, healthcare, sensing systems, etc.), and different EU projects whose results they are using.

These SMEs were the following:

- Digioutouch (Estonia), using Fed4FIRE+ project results (<https://www.cyberwatching.eu/smes-success-stories/smes-success-stories-digioutouch>);
- Su.me.tra (Italy), using SMOOTH project results (<https://www.cyberwatching.eu/smes-success-stories/smes-success-stories-sumetra>);
- CS.AWARE (Estonia) which is a completely new innovative spin-off company built on the CS-AWARE project results (<https://www.cyberwatching.eu/smes-success-stories/smes-success-stories-cs-aware>);
- Motivian (Greece), using FORTIKA project results (<https://www.cyberwatching.eu/smes-success-stories/smes-success-stories-cs-aware>);
- IT-LABS (Germany), using UNICORN project results (<https://www.cyberwatching.eu/smes-success-stories/smes-success-stories-it-labs>);
- BioAssist (Spain), using UNICORN project results (<https://www.cyberwatching.eu/smes-success-stories/smes-success-stories-bioassist>);
- TELESTO Technologies (Greece), using EVAGUIDE project results (<https://www.cyberwatching.eu/smes-success-stories/smes-success-stories-telesto>);
- Inotecha (Lithuania), using Tetramax project results (<https://www.cyberwatching.eu/smes-success-stories/sme-success-stories-inotecha>);
- Zanasi & Partners (Italy) which has integrated different projects' outputs (namely, PYTHIA, SOLOMON, DECISMAR, ECHO, FINSEC) to consolidate company's position in the security field, and implement a strategic penetration in the defence market (<https://www.cyberwatching.eu/smes-success-stories/smes-success-stories-zanasi-partners>);
- Cybernetica (Estonia) also used results from the multiple projects - abilities in AEOLUS, UaESMC, PRACTICE, SUNFISH, SafeCloud, BigDecisions, BiggerDecisions and DataBio in order to build its complex and secure programmable multi-party computation

engine (<https://www.cyberwatching.eu/smes-success-stories/smes-success-stories-cybernetica>).

All SME success stories were presented in a dedicated cyberwatching.eu website section and additional publicity for these stories was provided in social media channels. The SMEs were also encouraged to register their profiles in cyberwatching.eu and add their products to the Marketplace.



Cyberwatching.eu engage with a large pan-European community of SMEs, the Consortium collects a number of cases where SMEs have successfully used cybersecurity solutions also through cyberwatching.eu in an SME to SME situation, where an SME provider has served an SME end user.

Discover the SME success stories below!

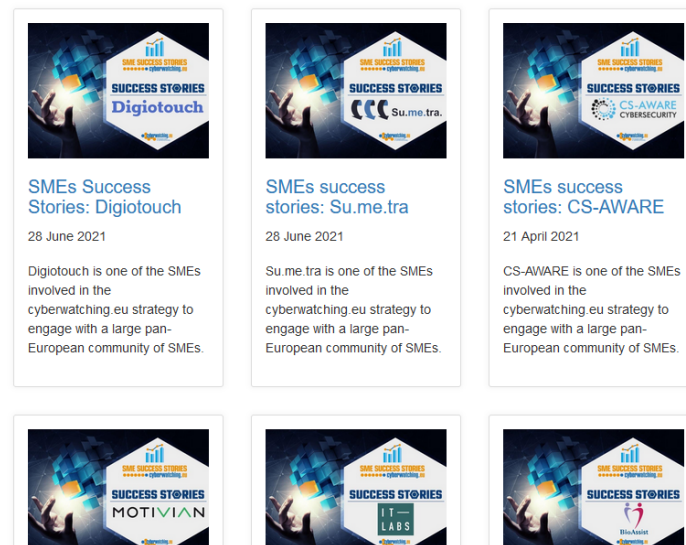


Figure 10 SME success stories' gallery: SMEs using cybersecurity and privacy R&D results



Figure 11 Examples of SME success stories in cyberwatching.eu social media

In each success story, SMEs briefly explain what their companies are doing; what concrete project results they are exploiting and how; what are the benefits for their business; and how they learned about the available project results. Answers to these questions are given in all short articles, provided in the cyberwatching.eu website.

From the collected stories, it became evident that most SMEs find EU R&D projects and their outputs mostly through the Open Calls / Innovation Contests where third-party funding is provided for the companies to integrated project solutions and report their feedback. This proves to be not only an important tool for the projects to validate their outputs, but also a good trigger for companies to engage with the projects and experiment with their outputs. Some SMEs have also mentioned that financial support and technical mentoring which was provided by the R&D projects were important factor which allowed them to successfully integrate and use the solutions.

In addition, this activity also proved that business impact for the SMEs which use EU-project results highly depends on the digital maturity level of a concrete SME. SMEs cybersecurity providers (or at least ICT front-runners developing digital solutions) are more likely to benefit from the EU R&D, as most of the projects do not reach the highest TRL (TRL 9), and can only be integrated as a part (component) of a wider solution. On the other hand, SMEs cybersecurity users, prefer off-the-shelf solutions, where one purchased tool / service would ensure the level of cybersecurity needed by the company. For this reason, such SMEs more often find the needed solutions offered by the market players (other SMEs or corporates) rather than the actual projects.

For most SMEs, the project results they adopted helped to improve some cybersecurity aspects of the digital solutions which they were already using, improve its performance, automatise certain aspects, improve scalability, etc. On the other hand, there were 2 SMEs (Zanasi & Partners and Cybernetica) which integrated results of multiple different projects and significantly strengthened their expertise and business offer. Finally, CS.AWARE is an outstanding example of a spin-off company which was built up specifically to offer services that were developed through the EU project CS-AWARE.

3.3 SME end-user club: SME workshops

10 SME workshops were organised during the project lifetime, covering specifically the topics of SME interest, and answering the needs of different SMEs within the cyberwatching.eu community (both SMEs cybersecurity providers and SMEs cybersecurity users).

All topics for SME workshops were carefully selected, based on changing realities in cybersecurity landscape, political developments, new cybersecurity requirements, and reacting to the feedback or questions commonly received from the SMEs.

The goal of these workshops was to appeal to a wide audience of companies, creating impact and providing useful content for SMEs interested in cybersecurity, as well as to further promote cyberwatching.eu content, its offer to the SME community, and to encourage them registering at cyberwatching.eu

The workshops were organised in different settings: physical when physical events were possible, and online (due to COVID-19 pandemics), some of them were collocated with other events (e.g. it-sa cybersecurity fair, ENISE13, ECSO Cyber Investor Days) in order to gain a wider visibility and effectively allocate the resources available. Furthermore, expert speakers were invited to all workshops in order to provide an impactful, interesting and practical content for the companies.

An overview of all ten workshops is available in the sub-sections below.

3.3.1 First SME workshop in ENISE11 (Leon, Spain)

The [first SME workshop 'Bridging R&I with the Business World'](#) was co-located with ENISE11 conference – the international meeting on Information Security, organised by Spanish National Cybersecurity Institute (INCIBE). The workshop was held on the 25 of October, 2017, and attracted a couple dozens of SMEs, while even wider audience (hundreds of participants) were exposed to cyberwatching.eu flyers and face-to-face discussions during the two-day event.

The SME workshop participants discussed how can SMEs use publicly funded R&I solutions in order to innovate and build new products, and how can cyberwatching.eu support them in this regard (e.g., by offering access to the cybersecurity and privacy Marketplace).

The success story of Spanish company Panda Security who was successfully adopting R&I project results in its business offering was presented by Mr. Raúl Pérez García, Global Presales Manager. Meanwhile, the expert speakers not only presented how can cyberwatching.eu help SMEs in this journey, what potential concerns they might face, and gave an overview of additional services and tools which help to answer such concerns: Ms. Laura Senatore (ICT Legal) spoke about the security and privacy challenges and compliance with GDPR, while Mr. Pablo Montoliu Zunzunegu presented cyber insurance for SMEs.

Although the workshop was designed specifically for SMEs cybersecurity vendors (providers), cybersecurity researchers and public sector representatives were also invited to attend the event.



Figure 12 Programme of the first SME workshop



Figure 13 Moments from the first SME workshop

3.3.2 Second SME workshop: workshop with ENISA

The second SME workshop on the [Security of Personal Data Processing](#) was organised on the 8th October in Athens in collaboration the European Union Agency for Network and Information Security (ENISA), and the support of the Hellenic Data Protection Authority. While the exact number of participants within the entire event is not known as it was only recorded by ENISA, 38 participants were present during the cyberwatching.eu panel.

One of the core obligations for all businesses, including SMEs, acting either as data controllers or data processors, in GDPR is that of the security of personal data. Therefore, the event explored SME preparedness to implement the GDPR – in this session, the discussion was held among cyberwatching.eu consortium members (Mr. Sebastiano Toffaletti from DIGITAL SME and Mr. Paolo Balboni from the ICT Legal), as well as experts: Mr. Apollon Oikonomopoulos from the Greek SME Skroutz and Mr. Vosilis Zorkadis from the Hellenic Data Protection Authority.



Figure 14 SME workshop on Security of Personal Data Processing with ENISA

3.3.3 Third SME workshop in it-sa cybersecurity fair

On the 9th-10th of October, 2020 cyberwatching.eu together with the European DIGITAL SME Alliance invited SMEs registered in cyberwtaching.eu to participate in its [SME workshop at the it-sa expo](#).

The SME workshop was a part of a larger two-days event organised for SMEs at it-sa, one of the most important cybersecurity events worldwide. The two-day event was composed of: 1) business match-making and customised tour in the it-sa on the 9th of October and 2) SME workshop on the 10th of October. In addition, the organisers facilitated some tailor-made activities for the registered SMEs which allowed SMEs to keep updated with the newest trends & innovation in the IT security sector and presented some unique opportunities for business exchanges, networking.

Besides the opportunity to attend cyberwtaching.eu workshop, and participate in the tailor-made programme guiding SMEs through the expo and allowing valuable business exchanges, cyberwatching.eu granted free tickets to enter the it-sa expo. To summarise, the SMEs had an opportunity to: participate in the International forum and its session on cyberwatching.eu; to learn about the main tools and assets for SMEs developed by cyberwatching.eu, and observe the main cybersecurity innovation trends presented together with cyberwatching.eu Radar; meet future business partners and clients & develop their European network, participate in match-making and business speed dating, receive an on-site support provided by DIGITAL SME & German ICT SME association BITMi, participate in informal exchanges & social programme.

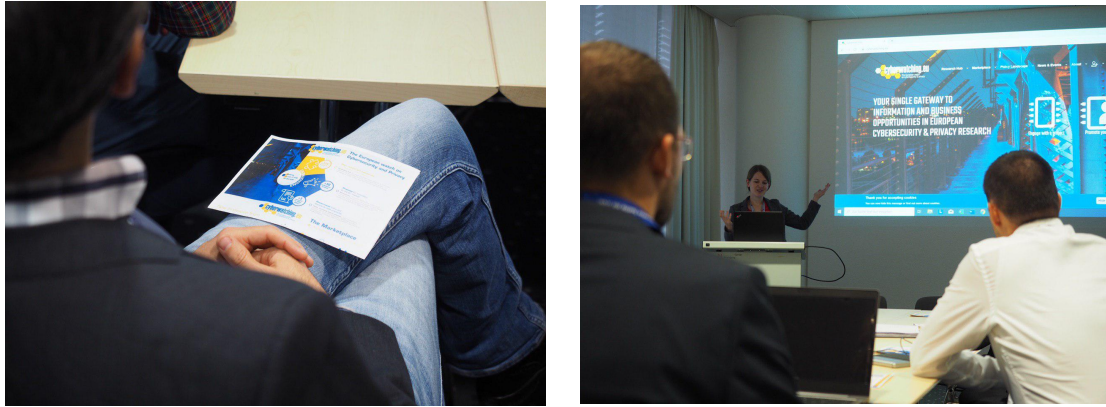


Figure 15 Moments from the cyberwatching.eu SME workshop in it-sa fair

3.3.4 Fourth SME workshop: Cyber Investor Days

The European Cyber Security Organisation (ECSSO) organised its Sixth Cyber Investor Day on 15 October 2019 in Luxembourg.

In a collaboration with ECSSO, a day before the Cyber Investor Day – on 14 October 2019 – participating SMEs and start-ups (21 attendees in total) were welcomed by [cyberwatching.eu to the SME workshop, aiming to prepare cybersecurity companies for their investment pitch](#), help them improve their presentation and public speaking skills, and to present other opportunities available at cyberwatching.eu.

The most promising European cybersecurity SMEs and start-ups got an opportunity not only to pitch their innovative solutions and participate in the strategic business matchmaking sessions offered by ECSSO, but also to improve their pitching skills and explore additional service offer within the cyberwatching.eu

Among all services presented, the SMEs were particularly interested in cyberwatching.eu [Project Radar](#), giving them an opportunity to analyse and assess the main cybersecurity and privacy trends in Europe, see where their solutions might have complementarities with the ongoing projects, and understand the main cybersecurity innovation gaps where SMEs could work with the research community to address them.

This workshop was also an important step strengthening the collaboration between ECSSO and cyberwatching.eu, and the first attempt at providing joint services for the SME audience within ECSSO and cyberwatching.eu SME communities.



Figure 16 Moments from the Fourth SME workshop

3.3.5 Fifth SME workshop on Teleworking during COVID-19

Since the COVID-19 affected SMEs everywhere in Europe, forcing to work remotely even those companies who have never considered ‘going digital’ before, cyberwatching.eu in collaboration with DIGITAL SME France [organised a session dedicated to French SMEs to raise their awareness about the cybersecurity issues of teleworking](#). The session was a result of cooperation with DIGITAL SME France, who had consulted its member companies to shape the topic for the session and understand the main pain-points to be covered during the workshop.

The workshop was held in French and allowed to reach the target audience of French-speaking SMEs, mainly located in Eastern France and Luxemburg. During the online workshop, the participants learned about the cyberwatching.eu Marketplace and its benefits for both end-user SMEs to find and test innovative solutions which can be particularly helpful in times of COVID crisis, as well as for provider SMEs to showcase their cybersecurity services and solutions. In addition, the participants were encouraged to test their cybersecurity knowledge and security level by using the online cybersecurity self-assessment tool for SMEs, that cyberwatching.eu developed in collaboration with the European projects CYBERWISER.eu and SMESEC.

The second part of the workshop was held by two experts in digital security, Mr. Etienne Laveau, Director of Steel PC, an SME which provides IT solutions and equipment to other SMEs, and Mr. Dominique Lo Sardo, Associate Managing Director of OpenField, a management consulting firm specialized in information systems. To begin with, the participants got an introduction to cybersecurity and cyber-attacks. The experts spelled out the consequences of a cyber-attack on companies, and even more on SMEs, highlighting the many potential repercussions, such as slowing down or even stopping the company's activity and/or production, blocking the company's website, damaging its reputation, losing its customer database, losing market share, etc. The

experts then explored the level of risk awareness among participants, describing the specific risks and cyber threats related to teleworking: phishing, ransomware, data theft, Business Email Compromise (BEC) scam, to name a few, and explaining what kind of vulnerabilities might be exploited by cyber criminals. For example, teleworking increases tremendously the attack surface of a company, which includes all the access points of a network that a hacker could use to enter the company's system.

Finally, participants got security recommendations from the experts, who stressed that the best defence against cyber-attacks is awareness. Participants were advised to: never use a public or open network as they are often used to launch attacks against the company; use a VPN (Virtual Private Network) to access the company's resources; install a properly configured firewall when possible; regularly update the software; check that the antivirus is up to date; immediately notify the IT department in the event of a suspicious behaviour (even if minor); lock their PC when not in use; hide their camera when not in use; notify their IT department if they misplace their PC or phone; use strong passwords and delete all their post-it notes with a password on them; define and implement an internal policy for teleworkers; monitor the activity of their external accesses. These tips were further explained and summarised in the SME guidebook '10 cybersecurity tips for teleworking' (see section 3.2.1.4), which is available in English for all SMEs who were not able to participate.

Figure 17 Promotion of the Fifth SME workshop

3.3.6 Sixth SME workshop: 5G vs Cable: Benefits & Security Risks

With SMEs increasingly questioning what will be the impact of 5G to their businesses, how the scandals with the non-EU providers of 5G technology affect their security, etc., cyberwatching.eu together with DIGITAL SME decided to dispel these doubts by organising the workshop [5G vs Cable: Benefits & Security Risks](#). It was held on-line on 12 April, 2021 and attracted 40 SMEs (out of 68 registered).

The main goal of this workshop was to discuss the future of 5G and how it will affect the SMEs, as well as to understand the modern cybersecurity attacks and whether they can be avoided.

The current 5G discussion focuses on the benefits of this technology, especially for industry. But 5G – like any other wireless communication – can be manipulated. Currently, the industry is mostly communicating via wired connections, which makes it hard for attackers to infiltrate the communication. If major industry sectors only rely on 5G networks in the future, they open attack vectors to criminals that weren't there in

the first case. This is why one of the conclusions from the expert speakers in this debate was: Wireless protocols are not redundant communication channels! Therefore, the workshop's expert speakers also tackled the question of equal focus on the security of wireless connections, devices, and applications.

Although the workshop was aimed at mostly SMEs with higher levels of digital maturity (IoT SMEs, SMEs in telecommunications, etc.), expert tips and insights provided in this workshop were important for any company slowly entering the 5G era.

The top part of the image is a promotional poster for the '5G vs Cable' workshop. It features a purple telephone handset and a smartphone. The text on the poster includes: '5G vs Cable', 'BENEFITS & SECURITY RISKS', 'Workshop 12 April 2021 16.00-17.00 CEST', 'DIGITAL SME LIVE', and the cyberwatching.eu logo.

The bottom part of the image is a screenshot of a presentation slide titled 'COUNTRY STUDY - ITALY'. The slide contains several bullet points and a table. The table lists various vendors and their status in Italy's 5G infrastructure.

MNCs	Extra-EU vendors	% of terminated 5G-only services active in the MNC's (2020)
WINDTRE	ZTE	50%
Telecom Italia	Huawei	60%
TIM	Huawei	25%
Ilse	No extra-EU vendors present	0%
Other MNCs	No extra-EU vendors present	0%

The slide also includes a map of Italy showing the current state of 5G deployment and a list of hidden costs in the Italian context.

Figure 18 Sixth SME workshop '5G vs. Cable'

3.3.7 Seventh SME workshop: use and value of the cybersecurity labels for SMEs

The seventh workshop was a result of continuous collaboration with DIGITAL SME France – following the success of the previous SME workshop in France (see 3.3.5), the second topic of interest for the French SMEs was defined.

This time, the discussion evolved around cybersecurity labels, and the workshop was titled [Cybersécurité: Utilisation et utilité des labels pour les PME](#) (Cybersecurity: use and value of the cybersecurity labels for SMEs). It was held on 29 April, 2021 and was conducted in French, targeting mostly SMEs in France, but also in Belgium, Luxembourg and other French-speaking companies. In total, 29 companies, out of 47 registered, showed up at the event.

The objective of this workshop was to present and discuss the use of labels in the cybersecurity sector, showing the example of three complementary labels: 1) the French label "ExpertCyber", which attests and promotes a company's expertise in cybersecurity; 2) The European label "Cybersecurity made in Europe", which

distinguishes companies developing cybersecurity solutions in Europe. Furthermore, the concept for the third upcoming label – 3) the cyberwatching.eu label, designed for SMEs which use digital technologies in any sector (even the more traditional companies).

After introducing these three labels and their complementarity, the discussion focused on the benefits of these labels, particularly for SMEs, for example in terms of visibility, enhancement of their activity and of their image of reliability with their customers. In addition, the importance of labelling and certification for public procurement was also discussed, demonstrating potential ways for SMEs to increase their chances in public tenders.

The speakers of this workshop included Ms. Deborah Goll, representing cyberwatching.eu and its label, Mr. Olivier Marty - président de la Commission IT EBEN who spoke about the ExpertCyber label; Mr. Danilo D'Elia - Senior Policy Manager at ECSO, presenting 'Cybersecurity Made in Europe' label and Mr. Yves Nicloux - Director of Purchase and Public Procurement for the City and Metropolitan Area of Met.

ECSO
The European Cyber Security Organisation (ECSO), established in 2016, is the European Commission's partner in implementing the contractual public-private partnership (cPPP) on cybersecurity.

ECSO unites more than 260 members, representing large companies, SMEs, investors, national and regional public administrations, research centres and academia.

In its six working groups, ECSO addresses the issues of the entire value chain of cybersecurity.

An independent voice of the European cybersecurity ecosystem

USERS & OPERATORS REQUIREMENTS
• Users & operators requirements
• Users & operators requirements
• Users & operators requirements

EDUCATION & TRAINING
• Education & training
• Education & training
• Education & training

TESTING, CERTIFYING & LABELLING PRODUCTS, SERVICES AND SYSTEMS
• Testing, certifying & labelling products, services and systems
• Testing, certifying & labelling products, services and systems

MARKET DEPLOYMENT
• Market deployment
• Market deployment
• Market deployment

Cybersécurité : Utilisation et utilité des labels pour les PME

LES EXEMPLES DU LABEL FRANÇAIS « EXPERTCYBER » ET DU LABEL EUROPÉEN « CYBERSECURITY MADE IN EUROPE »

Webinaire
Jeudi 29 avril 2021
11h00 - 12h00

cyberwatching.eu
The European watch on cybersecurity & privacy

DIGITAL SME
France

Figure 19 Seventh SME workshop. Cybersecurity: use and value of the cybersecurity labels for SMEs

3.3.8 Eighth SME workshop. ePrivacy Regulation: what's an impact on SMEs?

The eighth SME workshop on [ePrivacy Regulation and its impact on SMEs](#) was organised on the 10 May, 2021. With more than 100 participants registered (ultimately, 80 attended) and 155 views on YouTube, this has been the best attended out of 10 workshops. The workshop was co-organised with DIGITAL SME's AI Focus Group, which gathers more than 100 AI SMEs, who also strongly focus on cybersecurity.

Such a high rate of attendance is related to the topic which has been very widely debated at the time and has raised many questions among the SMEs - the first ePrivacy Regulation proposal was published in 2017. Four years later companies have been exhausted of waiting for an ePrivacy Regulation which had been going through an extremely lengthy legislative process. The only certainty in the process was that the new ePrivacy rules will have a large impact on companies, including the SMEs. Therefore, this discussion with the decision makers and data security/privacy experts was organised to bring some clarity and answer SME questions.

The first half of this workshop looked at the current state of the Regulation, its potential impact on SMEs and how it interacts with the GDPR, as well as how the EU approach to data protection is evolving. The session was moderated by Ms. Justina Bieliauskaite from DIGITAL SME, and included guest speakers from the Portuguese Permanent Representation (which by the time had a Presidency over the EU Council), represented by Mr. João Ferreira Pinto, SME privacy expert Mr. Leonard Johard (INDIVID/Brilliance Center B.V) and ICT Legal's expert Mr. Paolo Balboni.

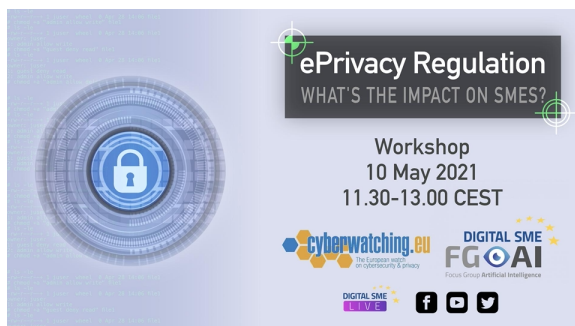


Figure 20 Eighth SME workshop - promotional banner

Meanwhile, the second half allowed participants to discuss their data protection concerns that affect their work – cyberwatching.eu legal experts Ms. Laura Senatore and Mr. Paolo Balboni (ICT Legal) were playing the key role in this part to answer the questions from the attending SMEs. In addition, cyberwatching.eu tools which help SMEs to navigate through EU's requirements (e.g., GDPR Temperature tool) were also presented.

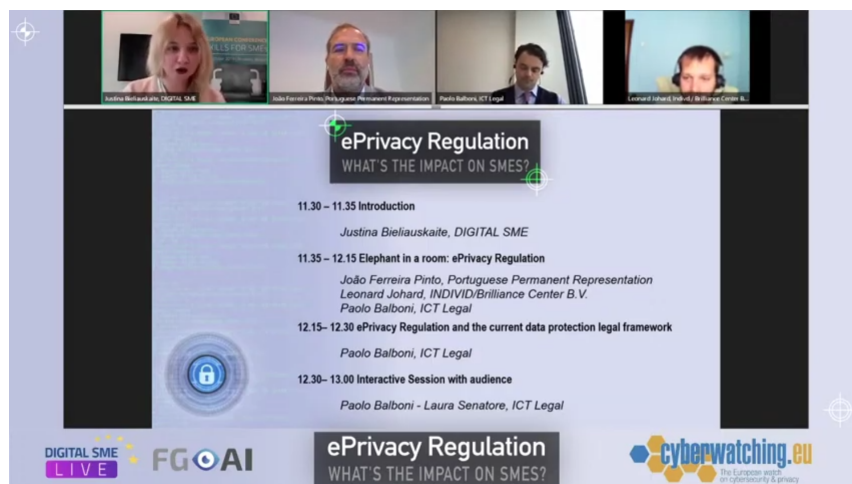


Figure 21 Moments from the eighth SME workshop

3.3.9 Ninth SME workshop: SCHREMS II & DATA TRANSFERS - Decision & Impact on SMEs

Following the success of the eighth SME workshop, and building on some of the questions which were raised during the workshop, it has been decided to further tackle a matter of data transfers to the third countries. Although personal data transfers have already been regulated by the GDPR, it appeared that many SMEs are still not aware of their obligations.

Moreover, additional knowledge has been generated through practical implementation of GDPR and related Court cases.



Figure 22 Ninth SME workshop - communications banner

In July 2020, the EU Court of Justice struck down the EU-US Privacy Shield, a major agreement governing the transfer of EU citizens' data to the United States. The case (C-311/18), referred to as 'Schrems II', after the Austrian activist Max Schrems, who brought the case forward, assessed whether the mechanism used by Facebook Ireland to share European data with Facebook Inc (domiciled in the US) – Standard Contractual Clauses (SCC) – was in violation of European citizens' rights to privacy. The European Court of Justice ruled that while SCC's can be a legitimate mean to transfer data, the EU-US Privacy Shield was not a satisfactory framework to protect the rights of individuals, and therefore was invalid.

In the wake of this decision, the European Data Protection Board (EDPB) has developed Recommendations to ensure compliance with the EU level of protection of personal data when transferring data to third countries. Therefore, during this [SME workshop on Schrems II decision & data transfers](#), Recommendations from the European Data Protection Board were presented and the discussion was held around the solutions that SMEs could deploy to ensure that data transfers are secure. Further to this, the panellists explained the challenges that companies face when undertaking data transfers and ensuring compliance with EU legislation, and the opportunities that this presents.

The workshop was organised on the 30 June, 2021, with the participation of excellent speakers from the EDBP (Mr. Ignacio Gomez Navarro), Encyberisk/ASSINTEL (Mr. Davide Giribaldi) and Legitimis SME (Ms. Cécile Faverdin). In addition, legal expertise and presentation of cyberwatching.eu tools were provided by Ms. Laura Senatore from the ICT Legal. The workshop was attended by 45 SMEs (out of total 63 registered).

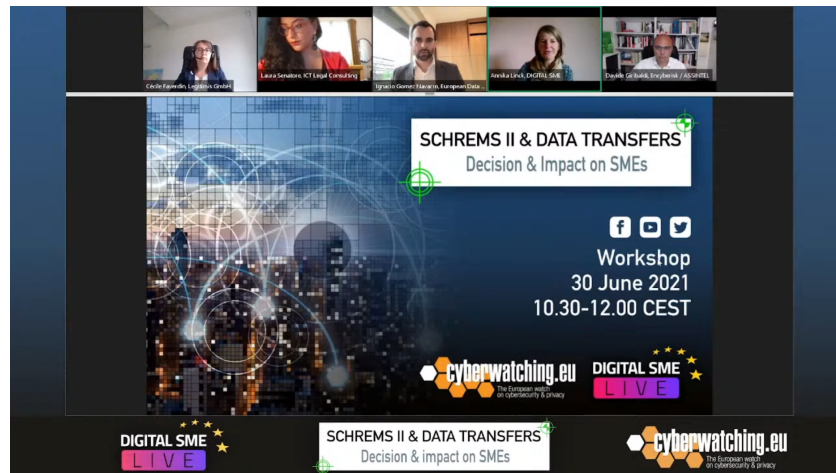


Figure 23 Moments from the ninth SME workshop

3.3.10 Tenth SME workshop. Cybersecurity Competence Centre Pilot Projects: SME Impact and Opportunities

The last tenth workshop was organised building on a close collaboration which cyberwatching.eu has established with the four Competence Centre Pilot Projects from the very beginning of their existence. In early 2019, just a few months after the launch of the Pilot Projects, they were invited to present their planned activities towards the SME community and other cybersecurity stakeholders in a [joint cyberwatching.eu webinar](#) 'Pilots for the European Cybersecurity Competence Networks: how can your SME benefit'. After almost three years of successful collaboration, and towards the end of cyberwatching.eu project lifetime, on the 14 July, 2021, [the pilot projects joined the tenth SME workshop on the Cybersecurity Competence Centre Pilot Projects: SME Impact and Opportunities](#). The workshop saw a participation of 66 SMEs (out of 89 registered).

With the establishment of the European Cybersecurity Competence Centre in Bucharest, the European Commission and Member States are taking steps to ensure that Europe's cybersecurity capacities are strengthened, and that European digital autonomy is secured. SMEs are at the heart of this effort, and the Competence Centre represent an opportunity for SMEs to be directly involved in deciding how our cybersecurity capabilities are developed. Therefore, a joint discussion between the Pilot Projects and DIGITAL SME's Cybersecurity Working Group evolved around the Centres' services to SMEs and their work with the SME community.

Each of the pilot projects presented its work and the main achievements so far, discussing the impact this might have on the European Competence Centre once it is implemented, and any opportunities for SMEs or DIHs to be engaged through participation in the pilots, membership of the Community and engagement with the Network, etc.



Figure 24 Tenth SME workshop promotional banner

More about the conclusions and the main insights from this workshop can be found in the D4.7 EU Cybersecurity & Privacy Final Roadmap.



Figure 25 Moments from the tenth SME workshop

3.4 Cyberwatching.eu Marketplace: value proposition, state-of-the-art and a way forward

The cyberwatching.eu Marketplace is one of the key assets of the project and the most important output for the SME community. Although originally designed with mostly cybersecurity provider SMEs in mind, the Marketplace proved to serve the needs of all SMEs of different digital maturity levels.

As it has been explained above, in order to obtain the registrations of both: cybersecurity providers and users, other cyberwatching.eu SME activities have been designed in a way which generates more leads towards the Marketplace and increases the number of registrations. For instance, during SME workshops, the Marketplace was promoted and references were made for SMEs to join it, while the developed tools for SMEs and their advice also encourages companies to check the latest solutions and join the Marketplace, etc.

This sub-chapter further explains the main value of the Marketplace, and demonstrates its state-of-the-art now, by the end of the project, as well as briefly looks at the sustainability model proposed to keep the Marketplace running.

3.4.1 The cyberwatching.eu Marketplace value proposition

The Marketplace can be used by both: SMEs cybersecurity users and SMEs cybersecurity providers. In the case of providers, the Marketplace is mostly used: 1) as a platform to display their own products, developed by company's internal research and innovation activities, or 2) as a platform to find and purchase the solutions from other producers, or request access to the pre-commercial cybersecurity offering that can later be integrated into their own products or services. Meanwhile, for SMEs cybersecurity users the Marketplace also offers some of the simple off-the-shelf

solutions which can help SMEs of different capacity and digital maturity levels (e.g. solutions offered by CYBERWISER or CANVAS projects).

Therefore, the value proposition of the Marketplace to the SME providers is as following:

- access the top-notch solutions from other European SMEs;
- access to the most innovative pre-commercial cybersecurity solutions from the EU R&D projects (and chance to validate them free-of-charge or use them for the prices cheaper than what market could offer);
- possibility to assess and evaluate one's own solution in a wider ecosystem, better understand the existing offer and the market;
- marketplace is easy to search and filter, and grants an easy direct contact the providers;
- a chance to register own cybersecurity solution and get a promotional space for a product/service;
- possibility to create own provider profile and benefit from extra visibility;
- improved access to the potential clients: Marketplace allows the direct requests from actual end-users actively looking for new cybersecurity and privacy services;
- during the lifetime of the project, registered users also had a chance to get invitations to cyberwatching.eu events, enjoy networking opportunities and additional visibility (e.g. as the providers of the week).

Meanwhile for the cybersecurity users the benefits are also identified:

- access to the most innovative European cybersecurity solutions, some of which are specifically tailored to SME needs and offer an easy-to-use high-quality protection;
- easy to search and filter Marketplace also offers a search possibility accordingly to the sectors, thus, user SMEs from health, transport, finance and many other sectors can quickly find solutions made for them;
- for those SMEs who have previously completed a self-assessment using one of the cyberwatching.eu tools, and have identified certain areas of vulnerabilities, the Marketplace search options help to find the solutions which match the concrete needs;
- direct contact option allows to quickly get in touch directly with the provider, avoiding third-parties, and allowing to negotiate the pricing and other conditions directly.

3.4.2 Cyberwatching.eu Marketplace: state-of-the-art

By the end of the cyberwatching.eu project lifetime, a Version 3 of the Cyberatching.eu Marketplace is available. It can currently still be found in the following URL: <https://cyberwatching.eu/market-products-list>

However, as explained in the sub-chapter below, the marketplace will now evolve into the ECSO SME Hub. Currently, the Marketplace contains 138 product and/or service offers from the European providers (EU R&D projects or SMEs).

The Marketplace landing page offers a possibility to register to the Marketplace and to get own products/services displayed in the Marketplace, or to browse it without the registration (this option is preferred among the cybersecurity users).

MARKETPLACE



MAKE IT EASY FOR BUYERS TO FIND YOU!

The Marketplace is a curated compendium of:

- Outputs from completed, EU-funded research projects
- Products and services offered by providers across Europe

This consolidated collection of Europe-wide, cybersecurity-related information, products and services offers providers unparalleled visibility and accessibility.

To showcase your project or company here and secure a front-row position at the forefront of the European cybersecurity industry, [click here](#).

[Learn more about the marketplace](#)

Filter by service type according to the five functions identified in the NIST Cybersecurity Framework:

Service type:



Target sector:



Search by title:

Figure 26 cyberwatching.eu Marketplace landing page

Those users who chose to follow the registration, are asked a few simple questions about the organisation, its specialisation (area of expertise and operations), and the contact details. The registration has been designed based on the feedback from the SMEs (see D5.2 [Early validation & end-users' club feedback report](#)). After having created its profile, users see their profiles, update them, add their preferences, and, importantly, they can fill in the information about the product/service and upload it to the Marketplace.

Home • Log in • PROMOTE YOUR ORGANISATION, PRODUCTS AND SERVICES

PROMOTE YOUR ORGANISATION, PRODUCTS AND SERVICES

Please register here to promote your organisation, services and products. Please provide all the information requested in order to personalize your private cyberwatching dashboard.

Username *

Names are always published in our database except for persons, companies, agencies, and addresses.

Email address *

Valid email address. All emails from this system will be sent to this address. The email address will never be sold or shared. We will use it if you wish to receive a new password or wish to receive the email address will also be used to send information and updates concerning the services that this website offer.

First Name *

Surname *

Do you represent a cyber security or privacy R&I project? *
☐ Select a value -
☐ Other

Please type your R&I project's url

Organization type *
☐ Select a value -
☐ Other

Category *
☐ Select a value -

Country *
☐ Select a value -

What Cybersecurity and Privacy services does your organisation provide? *

☒ **Identify**

- ☐ Governance & Risk Management
- ☐ Business Environment
- ☐ Asset Management

☒ **Protect**

- ☐ Identity Management & Access Control
- ☐ Awareness and Training, Data Security
- ☐ Information Protection Processes and Procedures
- ☐ Maintenance
- ☐ Protective Technology

☒ **Detect**

- ☐ Anomalies and Events
- ☐ Security Continuous Monitoring
- ☐ Detection Processes

☒ **Respond**

- ☐ Response Planning
- ☐ Communications
- ☐ Analysis
- ☐ Mitigation

☒ **Recover**

- ☐ Recovery Planning

What C&I services are you interested in? *

☒ **Identify**

- ☐ Governance & Risk Management
- ☐ Business Environment
- ☐ Asset Management

☒ **Protect**

- ☐ Identity Management & Access Control
- ☐ Awareness and Training, Data Security
- ☐ Information Protection Processes and Procedures
- ☐ Maintenance
- ☐ Protective Technology

☒ **Detect**

- ☐ Anomalies and Events
- ☐ Security Continuous Monitoring
- ☐ Detection Processes

☒ **Respond**

- ☐ Response Planning
- ☐ Communications
- ☐ Analysis
- ☐ Mitigation

☒ **Recover**

- ☐ Recovery Planning

Subscribe to our newsletter and stay up to date with cyberwatching.eu latest news and results

☐ Cyberwatching Newsletter

[Privacy Policy Section](#)

News

Are you ready for the challenge? Join our M-Sec Online Contest by 24 August

Do you have an innovative business idea that addresses one of M-Sec's smart city challenges? Are you interested in security and privacy issues of IoT devices and apps? Then apply by 24 August, participate at the M-Sec Online Contest between 9 and 10 September and get the chance to design, develop and present your business idea before a panel of international experts

Future Events

3rd International Workshop on Next Generation Security Operations Centers (NG-SOC 2021)

New H2020 project, SOCOWALLS (500000) has been selected and will be the 3rd International Workshop on Next Generation Security Operations Centers (NG-SOC 2021) will be held in conjunction with the 18th International Conference on Availability, Reliability and Security (ARES 2021) - Rio de Janeiro, September 11 - August 20, 2021, Venues, Avaiable

B-Sec Project Online Contest


Do you have an innovative business idea that addresses one of M-Sec's smart city challenges? Are you interested in security and privacy issues of IoT devices and apps? Then apply by 24 August, participate at the M-Sec Online Contest between 9 and 10 September and get the chance to design, develop and present your business idea before a panel of international experts

Figure 27 cyberwatching.eu Marketplace registration form

Following the decision on Marketplace's sustainability model jointly with ECSO, some additions to the registration are now being implemented, making some changes to the company profile information collected in the Marketplace; allowing a creation of the new user types (e.g., to include investors and paid users).

Additional information about the benefits of joining the Marketplace is also presented, by linking Marketplace's landing page with further pages explaining displaying the benefits.

WHY JOIN THE MARKETPLACE



Calling Innovators across Europe!

Join our curated compendium of

Brand-new results

from
EU-funded
research projects

New services

from
EU start-ups,
micro-businesses &
SMEs

Quick and easy registration
for all providers

[Register here](#)

Your Benefits

Free visibility across Europe and beyond

+2K social media followers

+4K monthly website visits

Receive RFIs and RFQs directly in your inbox

Join and present at our events and webinars

Feature as Provider of the week


Network with our growing community

Free and easy
to register publish your project results or company services

[Register now](#)

MAKE IT EASY FOR BUYERS TO FIND YOU!

THE CYBERWATCHING.EU MARKETPLACE



Innovators are at the very heart of Europe's new industrial strategy which charts a course for it transition towards digital leadership. Europe's industrial strengths include high quality research, and a vibrant start-up ecosystem and a mature infrastructure, key elements of the cybersecurity landscape. Cybersecurity is a top priority in Europe with the EU investing in research and innovation since the early 1990s. A rich array of large and small businesses, universities and research organisations ensure there is a constant flow of new results, services and skills emerging.

The EC-funded project cyberwatching.eu has created a marketplace which captures these diverse innovations and is home to the many results of R&I projects. By building and nurturing a community of dynamic innovators in cybersecurity & privacy areas, the project has created a grass roots environment for innovation exploitation and sustainability opportunities. This natural framework connects research results with both the demand and supply sides.

With many results from H2020 projects featured, EU SMEs have also taken advantage of the platform and published their own innovative solutions on the platform. Users can preview and validate new leading-edge services, showcase their own solutions to potential users or partners who can support them in the evolution from prototype to real market solutions. In addition, users can provide early validation and feedback, thus possibly steer the direction of future development and research.

The Marketplace is an excellent chance also for end-users, in particular SMEs, which can benefit from services and solutions supplied by R&I projects, having the opportunity to both test and implement beyond the state-of-the-art cybersecurity solutions. This gives them a competitive advantage and the opportunity to attract more customers, create personalised services, sell premium cybersecurity- & privacy-enhanced services, and produce cybersecurity & privacy solutions.

Having its results published on the marketplace entitles a provider, being an EU-funded project or a SME, to receive a series of benefits which include:

- Getting free visibility
- Receiving RFI and RFQs in the inbox directly through the marketplace.
- Being featured as Provider of the week, which means being highlighted among all the services in the marketplace and getting extra promotion on cyberwatching.eu website and social media channels
- Receiving Cyberwatching.eu free newsletter, in order to be constantly updated about Cyberwatching.eu

News

Are you ready for the challenge? Join our M-Sec Online Contest by 26 August

Do you have an innovative business idea that addresses one of M-Sec's smart city challenges? Are you interested in security and privacy issues of IoT devices and apps? Then apply by 26 August, participate at the M-Sec Online Contest between 9 and 10 September and get the chance to design, develop and present your business idea before a panel of international experts

[All news](#)

Future Events

3rd International Workshop on Next Generation Security Operations Centers (WG-SOC 2021)

Two H2020 projects, SOCRATES (<https://www.socrates.eu/>) and SAPPAN (<https://sappan-project.eu/>) jointly organize the WG-SOC 2021 workshop, to be held in conjunction with the 16th International Conference on Availability, Reliability and Security (ARES 2021) - <http://www.ares-conference.eu/>

August 17 – August 20, 2021, Vienna, Austria

17/08/2021 to 20/08/2021

BUSINESS IDEAS FOR SMARTER, SUSTAINABLE AND MORE SECURE CITIES

Apply by 26 August 2021

M-Sec Project Online Contest

Do you have an innovative business idea that addresses

Figure 28 cyberwatching.eu Marketplace benefits explains

As mentioned above, the Marketplace products and services can be viewed without registration as well. Therefore, interested buyers may first see what are the potential solutions on the marketplace, and register after having found the necessary product. The Marketplace view is demonstrated in the Figure 30 below:

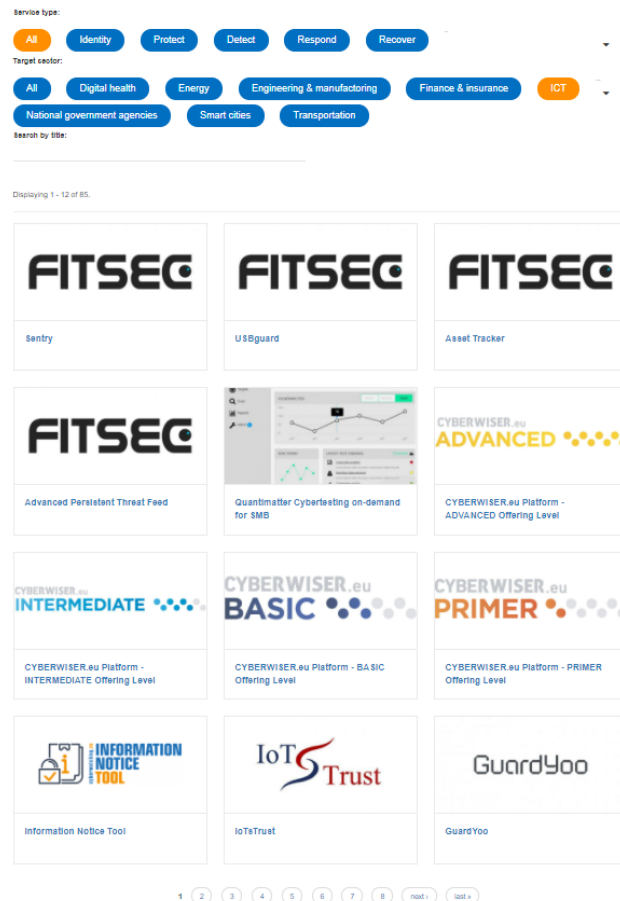


Figure 29 cyberwatching.eu Marketplace solutions

Finally, in the Figure 30 one might also see the displayed filters which allow users to easily browse among the solutions. The filtering is offered by:

- Sector (ICT; health, energy, finance, transportation, Smart Cities, etc)
- NIST classification (Identify, Protect, Detect, Respond and Recover).

Such classification was also preferred by industry as most SMEs are relying on NIST approach to cybersecurity solutions' classification. It is also aligned with ECSO WG4 preferences and the future vision for the ECSO SME Hub.

3.4.3 Cyberwatching.eu Marketplace: a way forward

As a result of the close collaboration with ECSO and especially its Working Group 4 on the support to SMEs, coordination with countries and regions, the Marketplace will be sustained and continue to exist after the cyberwatching.eu project lifetime. This will be done through the transition process, re-vamping cyberwatching.eu Marketplace to match ECSO's requirements and will allow its transition to become ECSO's SME Hub.

This process will benefit both: cyberwatching.eu Marketplace because it will be sustained and curated by ECSO, it will enjoy even better exposure to cybersecurity industry, and it will be further expanded with new ECSO members joining in; while

ECSO, whose project has been only in the starting phase, will benefit from the already functioning cyberwatching.eu marketplace, and additional users who are currently not yet the members of ECSO. Finally, with the EU cybersecurity strategy moving towards the direction of creating one and unified cybersecurity landscape, driven by the joint stakeholder community, it only makes sense that separate communities, such as ECSO and cyberwatching.eu are merging their effort to achieve greater impact, and bring together cybersecurity users and providers.

Such transition towards ECSO's SME Hub is a result of the MoU signed between ECSO and cyberwatching.eu in April, 2021, thus the Marketplace will soon be handed-over to ECSO who will become the exclusive owner of the platform and responsible for its promotion (while TRUS-IT Services will be hosting it). However, a several changes are being implemented and are about to be finalized by the end of M51, based on the current agreement and SME needs defined with ECSO:

- Redesign of some company profile information in the marketplace.
- Addition of new functionalities including jobs corner and inclusion of new fields related to standardisation
- Addition of new user types to include investors and paid users
- Integration of CRAFT database into SME Hub
- Payment module for premium membership
- Alignment of registration fields between CRAFT and marketplace in order for SME registration to be semi-automated.
- Retagging of content according to NIST taxonomy.
- Rebranding of visual identity based on ECSO template.

To sum up, all cybersecurity providers (and the registered users), as well as their cybersecurity and privacy solutions which have been registered to and displayed in the Marketplace will now be sustained, and will enjoy even greater benefits by becoming part of ECSO's SME Hub. This will lead to a stronger and less fragmented cybersecurity providers' ecosystem, which in turn will contribute towards European digital sovereignty.

4 Promotion activities of the Marketplace and SME assets

Numerous activities to promote the cyberwatching.eu Marketplace and SME end-user club have taken place during the project. While the more detailed report and the exhaustive list of such activities will be presented in the D4.9 Final Communication & Stakeholders Engagement Report, this chapter provides an overview of the main promotion channels and activities, which were used to engage with SMEs.

4.1 Channels

While there were multiple various interactions with the stakeholders all around Europe, promoting cyberwatching.eu SME services and assets, and helping to engage with the SME community, the table below summarises the most important channels that have been used to target the end users. This list is not exhaustive list, and is built considering the most impactful channels, while more information about all the outreach actions, as it has already been mentioned, can be found in the D.4.9.

Channel	How has it been used?
European DIGITAL SME Alliance membership and WG CYBER	<p>SME member network was informed about the Marketplace and invited to join it, as well as other assets offered by the project (via e-mails, during the Board meetings and joint events, through the Working Groups, social media activities, newsletters, website page promotion, General Assembly meetings, etc.).</p> <p>Specific attention was given to project's validation and promotion through the internal Working Group on Cybersecurity (WG CYBER), which was instrumental when testing/ consulting about the additional assets offered by the project, which supported the tenth SME workshop, engaged in numerous other activities. In addition, WG members were also offered as speakers to multiple cyberwatching.eu webinars and other events.</p>
ECSO and ECSO's WG4	<p>ECSO members were continuously informed about the progress of the project, and all new developments and key assets were presented to ECSO's WG4. ECSO has become the key partner to coordinate the effort and sustain the Marketplace. In addition, ECSO's experts participated in numerous SME workshops and cyberwatching.eu webinars, while one joint SME workshop was also organised.</p>
European (ICT) clusters	<p>Project consortium (with a lead of AEI) has analysed potentially interested European clusters and has grouped them into two categories: specific clusters in ICT and Cybersecurity and clusters of other categories (energy, health, food) which may be in need of cybersecurity solutions. In total, more than 300 clusters have been identified, and half of them have already been contacted. Later on, some of the selected priority clusters with particular attention to cybersecurity were identified and engaged to closely collaborate organizing common events, reaching to their SMEs and promoting the developed cyberwatching.eu SME assets to their communities. These clusters include: ClujIT, GAIA, AEI Ciberseguridad, The Hague Security Delta, as well as DIGITAL SME France, Cyber Wales, Bavarian IT Security and Safety Cluster and Italian Digital SME Alliance. D4.2 EU Cybersecurity and Privacy cluster engagement report. 1st Report, D4.5 EU Cybersecurity and Privacy cluster engagement report 2nd Report, D4.6 EU Cybersecurity and Privacy cluster engagement report. 3rd Report and D4.8 Cluster Engagement 4th Report provide a full overview of this activity.</p>
Digital Innovation Hubs	<p>Digital Innovation Hubs (DIHs) is one of the main tools which European Commission has put forward to foster SME (and public service) digitalization and support their digital transition. Therefore, DIHs play a key role in</p>

	<p>raising SME awareness about cybersecurity and informing them about the existing tools and services.</p> <p>Collaboration with multiple DIHs has been established through the project duration, with a specific attention to those largely interested in cybersecurity: Cybersecurity Innovation Hub in Czechia, Mycrocyber (Italy); DIH4Sm@rtRegions (Portugal); DIH4Society (Romania); Health Hub (Greece). Finally, a very important collaboration has been established with the CyberDIH (coordinated by the AEI Ciberseguridad), as it is going to sustain most of the tools developed by cyberwatching.eu for the SMEs. Details on this engagement is also provided in D4.8.</p>
Cyber Competence Pilot Projects	Security Center
	All four cybersecurity competence center pilot projects have established their own communities of cybersecurity users and providers, therefore, also bringing together interested SMEs. Therefore, collaboration through the common events, cross-dissemination activities, and even development of the cybersecurity self-assessment tool (with CyberSec4Europe) were implemented.
Online resources	Various social media channels (firstly those of cyberwatching.eu itself, and the consortium partners, and other engaged stakeholders) have been used for promotion and outreach towards the SMEs.
Events, workshops, etc.	Most of the promotion and dissemination has been done during numerous events organised or attended by the project partners, this is there most of the face-to-face engagement with SMEs was carried out, and multiplier organisations were also engaged. A list of the most important events for the SME engagement is in the sub-section 4.1.2 below.

Table 2 List of channels used to promote cyberwatching.eu Marketplace and SME end-user club

4.1.1 Collaboration with ECSO WG4

ECSO (European Cybersecurity Organisation) is a non-for-profit organisation which operates as a contractual Public-Private Partnership in the field of cyber security. ECSO members include a wide variety of stakeholders which are of the interest for the cyberwatching.eu: large companies, SMEs and Start-ups, research centres, universities, end-users of cyber security products and services, operators, clusters and association as well as European Member State's local, regional and national administrations, etc. The main objective of ECSO is to support all types of initiatives or projects that aim to develop, promote, encourage European cybersecurity, including cyberwatching.eu

ECSO's internal Working Group 4 *Support to SMEs, coordination with countries and regions* is particularly important for cyberwatching.eu consortium due to its outreach to SME community (mostly, to the providers of cyber security solutions). It also serves as a perfect platform to promote the Marketplace and SME end-user club.

Continuous collaboration with ECSO, and especially with WG4, has been established through the joint efforts of DIGITAL SME, CONCEPTIVITY and TRUST-IT. Cyberwatching.eu Marketplace and other SME community assets have been

presented and discussed in numerous WG4 meetings, as well as other ECSO events (e.g. WG4 meeting in Helsinki, September 2017, cyber security scaleups and industry leaders matchmaking event in Milan in September 2018, ECSO Cyber Investor Days in 2019, ECSO Partnership Board in 2020, etc.).

As it has been explained above, the main results of the continuous engagement with ECSO have been the Memorandum of understanding signed between ECSO and cyberwatching.eu (Trust-IT), and paving the path for the sustainability of the Marketplace as an ECSO SME Hub. However, in addition to this MoU, other means of collaboration were also important addressing the SMEs: common events were organised (such as ECSO Cyber Investor Day in 2019, joint together with cyberwatching.eu SME workshop), ECSO was invited to SME workshops, cyberwatching.eu webinars, and the Concertation meetings, while cyberwatching.eu representatives got a chance to present the project in ECSO's internal and external meetings, especially in the WG4.

4.1.2 Events

The following list demonstrates variety of events where the cyberwatching.eu Marketplace and other assets for the SME community were promoted, and where SMEs were targeted in order to receive their feedback, and later, to encourage their registration.

M1-M18:

- Digital Assembly 2017 (July 2017, Valetta, Malta) Participation of DSME at conference panel on cyber-security – informal networking talks with SMEs, clusters and SME associations.
- ECSO Working Group 4 meeting (September 2017, Helsinki, Finland) – presentation of cyberwatching.eu, collection of the feedback.
- cyberwatching.eu SME workshop in INCIBE's International Meeting on Information Security 2017 (October 2017, Leon, Spain) – workshop with cyberwatching.eu community, presentation of the Marketplace and SME end-user club, collection of the feedback.
- Eastern Partnership Business Forum (October, 2017, Leon, Spain) – distribution of flyers, informal talks with SMEs and business associations.
- ISSE conference (November 2017, Zaventem, Belgium) – presentation of cyberwatching.eu Marketplace and SME end-user club, discussion with the participants
- Investing day for European Cyber security companies (February 2018, Paris, France) – informal discussions and cyberwatching.eu presentation to the companies.
- Cyberwatching.eu concertation meeting (April 2018, Brussels, Belgium) – cyberwatching.eu presentations, discussions, dissemination of materials.
- Meeting with CAN (April, 2018, Milan, Italy) – presentation of cyberwatching.eu and its Marketplace and SME end-user club to Italy's biggest SME association – CNA.
- European DIGITAL SME Alliance Board meeting (May 2018, Brussels, Belgium) – presentation of cyberwatching.eu upcoming Marketplace and SME end-user club, distribution of flyers.
- CEBIT (June 2018, Hannover, Germany) – distribution of flyers, discussion with SMEs.
- #INVESTCYBER ECSO event (September 2018, Milan, Italy) – presentation of cyberwatching.eu, informal discussions with SMEs.

- ENISA and cyberwatching.eu workshop (October 2018, Athens, Greece) – presentations by cyberwatching.eu community, presentation of the Marketplace and SME end-user club, informal talks with SMEs.
- Annual event workshops and presentation at innovation park at CyberSec event, October 2018
- cyberwatching.eu webinars (June, July, September, October 2018) – presentations of cyberwatching.eu Marketplace and SME end-user club.
- ECSO Working Group 4 conference calls – discussions mostly regarding the Marketplace, SME end-user club briefly presented.
- ENISE Event, an International Meeting on Information Security (October 2018, León, Spain) is a meeting to promote the cybersecurity industry in Spain. Participation of AEI Ciberseguridad in a stand and presentation of the Marketplace and SME End-User-Club to more than 50 interested companies
- II Cybersecurity Forum Castilla and León, (October 2018, Valladolid, Spain), a business meeting organized to raise awareness about the importance of cybersecurity in SMEs. AEI Ciberseguridad, among several initiatives, spoke about the Cyberwatching.eu project

M18-M36:

- Digital skills for SMEs and industry: finding, training and recruiting ICT talents event in Lagrogn (2018 November 11) – cybersecurity awareness identified as one of the skills gaps, where cyberwatching.eu services are presented as one of the answers helping to cover the gap
- EU-GCC Study Trip to Brussels (2019 September 23) – meeting with the SME organisations and public authorities from the GCC countries, cyberwatching.eu was presented as one of SME-enabling public initiatives, a good practice example to support local SMEs
- CyberCamp 2018, organised by INCIBE in Málaga (Spain) from 29 November to 2 December 2018 – a presentation from AEI on the Marketplace and their benefits for SMEs
- Building a Cybersecurity Eco-system to Secure European Society (Community of Users on Secure, Safe and Resilient Societies Thematic Group 4: Cyber Issues) (2019 March 28) – a joint panel between cyberwatching.eu and the Pilot Projects
- Italian Digital SME Alliance meeting (2019 July 3) – presentation of all cyberwatching.eu assets and services for SMEs, including the Marketplace
- ECSO General Assembly (2019 June 18) – one-on-one engagement and presentation of cyberwatching.eu
- ECSO Board meeting (2019 October 3) – verbal discussions about the partnership with cyberwatching.eu and a short update on the project's progress
- It-sa cybersecurity fair (2019 October 8) – cyberwatching.eu SME workshop was organised, but also flyers distributed and roll-up presented in the fair, one-on-one engagement took place
- SKILLS FOR SMEs: Supporting the adoption of cybersecurity, Big Data and IoT by SMEs (2019 October 15) – cyberwatching.eu mentioned as one of the good practice examples to support cybersecurity adoption among SMEs
- FIC in Lille (2020 January 28) – cyberwatching.eu booth was hosted in France's biggest cybersecurity industry fair, and one-on-one SME engagement took place

- ECSO Partnership Board (2020 February 19) – reference to cyberwatching.eu in the discussions regarding the EU funding, existing and future initiatives
- DIGITAL SME General Assembly (2020 May 14) – progress and new assets of cyberwatching.eu were presented to SMEs and their associations
- Cybershare online conference (2020 May 29) – presentation of cyberwatching.eu and the Marketplace was made
- EESC event on Sustainability and Digitalisation (2020 November 25) – cybersecurity was named as one of the important puzzle pieces for the sustainable digitalisation of companies, cyberwatching.eu referred as a tool to support SME effort in it
- Meeting with Belgian business association Agoria (2020 December 14) – presentation of cyberwatching.eu assets and Marketplace
- Meeting with NL Digital cluster (2021 January 11) - presentation of cyberwatching.eu assets and Marketplace
- VODAFONE Roundtable discussion Recovery & Resilience: Digitalisation of SMEs (2021 April 22) – cyberwatching.eu referred to as a good practice example providing tools to encourage SME resilience and cybersecurity
- SMEUnited Digital Working Group meeting (2021 April 15) – the final outcomes, the Marketplace and the upcoming cybersecurity Label were presented to SME associations, members of SMEUnited

5 Conclusions: validation & future recommendations

During the project lifetime, continuous engagement with SME community was carried out, leveraging on opportunities to present cyberwatching.eu assets and receive valuable feedback through one-on-one engagement, events, webinars and workshops with SMEs and their representatives (business associations, clusters).

All project activities were specifically shaped to take into consideration the identified needs of SMEs: projects tools and resources, as well as workshops were designed to match specific SME needs and cover the topics of their interest.

The key resources (tools and cybersecurity Label), demanded by the SME community, will be sustained after the project lifetime to benefit SMEs (see more in D5.4) and hosted by the CyberDIH, while European DIGITAL SME Alliance will provide meaningful linkages to the resources, and will guide its members (especially those members engaged in cybersecurity and digitalisation Working Groups) to visit and consult the CyberDIH. Meanwhile, another major resource – cyberwatching.eu Marketplace will be made available to SMEs through ECSO SME Hub, which will bring interested SMEs to even closer community of cybersecurity users and providers.

All key assets developed for and delivered to the SME community during the cyberwatching.eu lifetime are summarised in a table below, including the main benefits that companies received, and the feedback which feeds into the future recommendations.

Table 3 cyberwatching.eu SME assets - key benefits and recommendations

cyberwatching.eu SME asset	Key benefits for SMEs	Recommendations
SME tools (GDPR)	- Initial free-of-charge self-assessment on various	- Provide basic tools in various European

Temperature Tool; Cybersecurity Self-assessment for SMEs; cyberwatching Information Notice Tool) Cyber Risk Temperature Tool and Guidebooks)	<p>cybersecurity and privacy aspects.</p> <ul style="list-style-type: none"> - Increased awareness about the main risks and challenges which company is facing in terms of cybersecurity and privacy. - Reduced risks to be exposed to sanctions or cybersecurity attacks. - A valuable first step towards securing the company. 	<p>languages, to make them more accessible to all SMEs.</p> <ul style="list-style-type: none"> - Ensure a visibility of and knowledge about such tools to avoid duplication of effort (creation of similar tools by different players); - Support the sharing and promotion of already existing tools (e.g., via the EDIH network, EEN, etc.)
SME cybersecurity Label	<ul style="list-style-type: none"> - Light-certification mechanism which serves as the first (preparatory) step towards required certification. - A simplified and SME-friendly approach to certification, easy-to-understand process. - Low price compared to other existing certifications. - Marketing advantage towards competitors: certificate shows a good level of cybersecurity which company ensures. - Increased standings when bidding for public procurement tenders. 	<ul style="list-style-type: none"> - Encourage public administrations to prioritise certified, cybersecurity ensuring and privacy compliant SMEs. - Ensure clarity and harmonisation of requirements for SMEs, provide guidance and simplified certification procedures. - Where possible, promote a wide use and acceptance of light-weight cybersecurity certification vs. burdensome requirements.
Marketplace	<p>Different benefits for cybersecurity users and providers (defined in greater detail in 3.4.1).</p> <p>Value to the SME cybersecurity providers:</p> <ul style="list-style-type: none"> - access the top-notch solutions from other European SMEs; - access to the most innovative pre-commercial cybersecurity solutions from the EU R&D projects; - possibility to assess and evaluate one's own solution in a wider ecosystem; - marketplace is easy to search and filter, and grants an easy direct contact the providers; - a chance to register own cybersecurity solution and get a promotional space for a product/service; 	<ul style="list-style-type: none"> - Support the development of one and centralised European cybersecurity Marketplace, avoiding duplications and fragmentation. - Support actions and activities to bring European cybersecurity providers together with the user community. - Encourage a development of the unified stakeholder ecosystem, where demand and supply sides can closely work together and exchange. - Encourage public administrations to use European cybersecurity solutions. - Provide support activities to innovative European cybersecurity providers to enter global markets, attract international

	<ul style="list-style-type: none"> – possibility to create own provider profile and benefit from extra visibility; – improved access to the potential clients <p>Meanwhile for the cybersecurity users the benefits are:</p> <ul style="list-style-type: none"> – access to the most innovative European cybersecurity solutions; – easy to search and filter Marketplace also offers a search possibility accordingly to the sectors; – direct contact option allows to quickly get in touch directly with the provider, avoiding third-parties, and allowing to negotiate the pricing and other conditions directly. 	<p>funding and approach global clients.</p>
SME workshops	<ul style="list-style-type: none"> – Possibility to get direct answers to the most urgent trending questions and issues regarding cybersecurity and privacy. – New skills and knowledge offered by variety of cybersecurity, privacy and business experts. – Networking and cooperation opportunities among SMEs. – Tips, guidance and advice regarding cybersecurity and privacy. – A chance to meet decision makers, cybersecurity research community, standardisation experts and other relevant stakeholders. 	<ul style="list-style-type: none"> - Encourage SME-tailored discussions on cybersecurity matters (e.g, inviting experts who can present complex topics in a simple way for less technical companies) - Promote dialogue between SME community (cybersecurity users and providers), decision makers, researchers and other stakeholders via EU Cybersecurity Competence Center and its Stakeholder Community.
SME success stories	<ul style="list-style-type: none"> – Visibility and positive branding for the companies which implemented successful practices. – Inspiring stories and motivation for companies reading the stories. – Additional ideas and inspiring practices for EU-funded projects, allowing to understand what attracts companies to exploit their solutions. 	<ul style="list-style-type: none"> – More supporting actions should be taken to encourage the exploitation of project results, especially, by SMEs, and raise SME awareness about availability of such project results. – Encourage projects to pro-active use existing marketplaces with a solid SME base (e.g., explore opportunities with ECSO Hub). – To voice more SME success stories on EU

		level, invite such role-model SMEs to the industry events, etc.
--	--	---