D3.8 From Research to Standards in Cybersecurity

Author(s)	CONCEPTIVITY
Status	Final
Version	v1.0
Date	30/07/2021

Dissemination Level

X	PU: Public
	PP: Restricted to other programme participants (including the Commission)
	RE: Restricted to a group specified by the consortium (including the Commission)
	CO: Confidential, only for members of the consortium (including the Commission)

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 – WP – D3.8	
Deliverable lead	**CPT**
Related work package	**WP3**
Author(s)	**Mark Miller, Victoria Menezes Miller, CPT**
Contributor(s)	**AEI, TRUST-IT, UXOF, ICT-Legal, DSME**
Due date	**30/04/2021**
Actual submission date	**30/07/2021**
Reviewed by	**David Wallom (UOXF)** **Anastasia Botsi (ICTL)**
Approved by	
Start date of Project	**01/05/2017**
Duration	**51 months**

Revision history

Version	Date	Authors	Notes
v0.1	02.03.2020	V. Menezes Miller (CPT)	1st structure
v0.2	04.05.2020	M. Miller, V. Menezes Miller (CPT)	Structure revised
v0.3	30.06.2020	M. Miller, V. Menezes Miller (CPT)	Draft
v0.4	04.06.2021	M. Miller, V. Menezes Miller (CPT)	Draft
v0.5	06.07.2021	M. Miller, V. Menezes Miller (CPT)	Revised following N. Ferguson's draft
v0.6	16.07.2021	M. Miller, V. Menezes Miller (CPT)	Contributions request
v0.7	20.07.2021	M. Ramirez (AEI)	Sections 2.4, 2.7, 2.7.2 to 2.7.14, 3.6, 4
v0.8	20.07.2021	D. Wallom (UOXF)	Section 2.6, 4
v0.9	20.07.2021	N. Ferguson (Trust-IT)	Sections 3.1, 3.3
V0.9	23.07.2021	A. Botsi (ICTL)	Section 1, 2.5

V0.10	23.07.2021	M. Miller, V. Menezes Miller (CPT)	Re-structuring following contributions, Sections 2, 3, 8
V0.11	25.07.2021	M. Miller, V. Menezes Miller (CPT)	Sections 2, 3, 8
V0.12	25.07.2021	M. Miller, V. Menezes Miller (CPT)	Full edit
V0.13	26.07.2021	Nick Ferguson, Niccolò Zazzeri (Trust-IT)	Contributions in section 7 and 8
V0.14	26.07.2021	D. Wallom (UOXF)	Section 4
V0.15	26.07.2021	J. Bieliauskaite (DSME)	Section 3
V0.16	26.07.2021	M. Miller, V. Menezes Miller (CPT)	Glossary, Section 8
V0.17	27.07.2021	M. Ramirez (AEI)	Section 4.1, 6
V0.18	27.07.2021	N. Ferguson, Niccolò Zazzeri (Trust-IT)	Section 3, 3.1.2, 3.1.5
V0.19	28.07.2021	M. Miller, V. Menezes Miller (CPT)	Full edit, Section 2
V0.20	28.07.2021	M. Miller (CPT)	Final Edit / Review before Internal Review Process
V0.21	29.07.2021	M. Miller, V. Menezes Miller (CPT)	Modifying to include 1st Internal Review comments
V0.22	30.07.2021	M. Miller, V. Menezes Miller (CPT)	Modifying to include 1st Internal Review comments; full final edit.
V1.0	30/7/2021	Nicholas Ferguson (Trust-IT)	Final version and PMB review

Executive Summary

Cyberwatching.eu has been on the forefront of addressing the key issue of standards (and that issue is trust), via the in-project development of the Light Cybersecurity Label, which is a key result of this project that will "live on" well beyond the lifetime of cyberwatching.eu. Thus, this is proof that the European Commission Horizon 2020 funding has been well spent in the pursuit of addressing the needs of the cybersecurity ecosystem and for European citizens and the broader society to have "trustworthy" systems and solutions that enable SMEs and even any organisation to bring key trusted innovations to the European and global markets. Furthermore, the Light Cybersecurity Label can be achieved within limited budgets and even used by those with limited resources (human and other) with a genuine opportunity for SMEs to sell their "trusted" solutions. This is truly part of the long-lasting legacy of the cyberwatching.eu project.

In addition to describing and explaining in detail the Light Cybersecurity Label, this deliverable also aims to provide a snapshot of the ongoing innovations and efforts to address certification and related standards within Europe, while recognizing at the same time that the situation is not static, but rather constantly evolving. The deliverable also illustrates the EC projects, ECSO efforts, ENISA efforts and other aspects and work in the research and standards area so that a clear picture can emerge for the readers of this document. At the same time, it must be noted that this is only a "snapshot" in time, such that the evolution will continue beyond this current timeframe. Efforts of organisations such as Working Group 1 of the European Cyber Security Organisation (chaired by the CEO of CONCEPTIVITY) will be contributing even further to the development of the cybersecurity certification framework well beyond the lifetime of the cyberwatching.eu project.

It is in this context that this deliverable aims to briefly summarise what has occurred up to this moment, what is currently happening and what could be possible in the future.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

1 Introduction

Cybersecurity certification and standards go hand in hand in addressing the issue of trust with respect to the view of the users and the European citizens. Traditional methods of certification address systemic approaches and must be adapted to the fast-evolving realm of cybersecurity. Inevitably, industry led initiatives have been the most prevalent, but often these are driven by the largest industry and research players, such that the standards and certification solutions developed are not always suitable for SMEs (Small and Medium Enterprise) which comprise a large proportion of the innovations going forward currently.

Companies, in particular SMEs, are nowadays experiencing cyber-attacks on a daily basis. A cyber-attack can cost them on average €25,000[1]. Smaller businesses are often targeted and hit harder, suffering repeat attacks which can lead to damaged reputations and potential business closure. Despite this environment, cybersecurity is still often an after-thought for many small businesses, with only half of European SMEs investing adequately to address the issue.

In this deliverable, we seek to show not only what cyberwatching.eu has developed with the Light Cyber Security Label, but also some of the other initiatives that exist and are ongoing. We hope to share an idea of the current landscape, while at the same time demonstrating that our Light Cyber Security Label fills a much need niche especially for the innovating SME community.

This deliverable also demonstrates that the cyberwatching.eu project identified a need (the SME-friendly certification / Label) and in turn is answering that clear market need with a genuine “fit for purpose” solution. All too often, certification and the related standards have been designed by and for the large industrial players, and as such SMEs have most often been left out of the picture. Our Light Cybersecurity Seal changes that picture entirely with a tool that is truly SME-friendly.

This deliverable is structured, as follows:

Chapter 2; Overall background and evolution during the lifetime of cyberwatching.eu

Chapter 3: An overview of cyberwatching.eu’s focus on standards and certification

Chapter 4: An overview of projects involved in standards and certification research and tools (as extracted from the Project’s Observatory).

Chapter 5 to 7: Summary of the current European labels or seals in certification

Chapter 8: Conclusions and Recommendations

[1] Article from Hiscox Cyber Readiness Report 2021: https://www.hiscox.com/articles/average-annual-cost-cyber-attacks-us-small-business-25k-reveals-hiscox

2 Background and evolution

Cybersecurity certification is a perceived need in the eyes of European users of technology who understand that technology can be used to gather data and also to abuse the different electronic devices that have become so ubiquitous in the current environment and at the current time. Nowadays, it is hard to live today in society without being a technology user and at times the risks are not often well understood by the users. Hence, the basic demand does exist to have "trusted" solutions that can be understood in the basic sense by the European Citizen and by the cybersecurity ecosystem such that these trusted solutions can be used with a certain perceived positive feeling of security. Given that SMEs in Europe are the engine for many of these innovations, it is of key importance that they can achieve some kind of a trusted status for their solutions and technology and as such can be sold in the European and global markets in the same way that the large industry players have done. In essence, SME-friendly certification and standards are a way to do this. In this chapter we are providing updates on previous and ongoing efforts.

2.1 ENISA Cybersecurity Framework Update

"Regulation (EU) 2019/881 (Cybersecurity Act), establishes a European cybersecurity certification framework for ICT products, services and processes. ENISA participates in this new framework, by preparing candidate certification schemes on the request of the European Commission and/or the European Cybersecurity Coordination Group (representation of Member States).

Standardisation is playing an important role in the framework, as the Act states the following:

- *There is a need for closer international cooperation to improve cybersecurity standards, including the need for definitions of common norms of behaviour, the adoption of codes of conduct, the use of international standards, and information sharing, promoting swifter international collaboration in response to network and information security issues and promoting a common global approach to such issues.*
- *The European cybersecurity certification schemes should be non-discriminatory and based on European or international standards, unless those standards are ineffective or inappropriate to fulfil the Union's legitimate objectives in that regard.*
- *The certificate or the EU statement of conformity shall refer to technical specifications, standards and procedures related thereto*
- *A European cybersecurity certification scheme shall include at least the following elements:*
    - *[..] references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements."*

The mission of ENISA in the area of the EU cybersecurity certification framework is outlined as follows: "To pro-actively contribute to the emerging EU framework for the ICT certification of products and services and carry out the drawing up of candidate certification schemes in line with the Cybersecurity Act, and additional services and tasks".[2]

ENISA illustrates a general concept for the role of standards in the evaluation and certification process as presented in Figure 2-1.

[2] From ENISA website: https://www.enisa.europa.eu/topics/standards

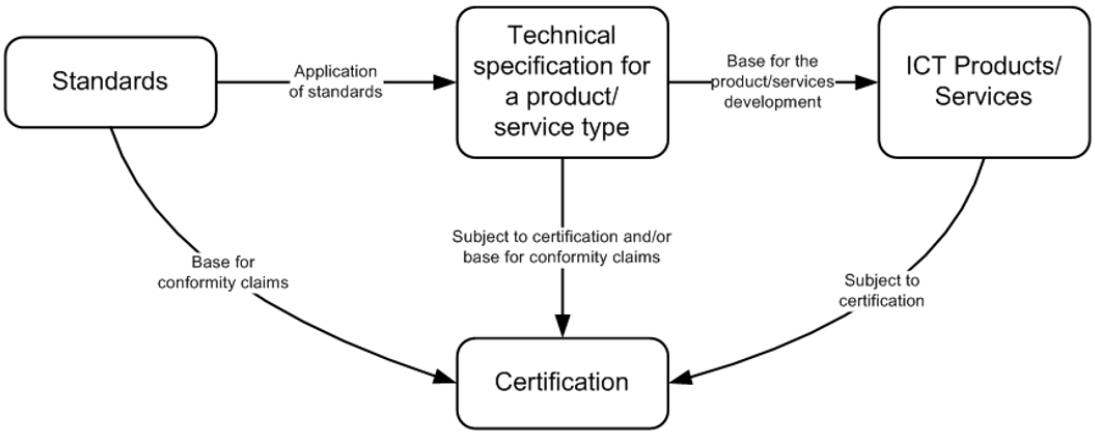

Figure 2-1: ENISA's general concept general concept for the role of standards in the evaluation and certification process

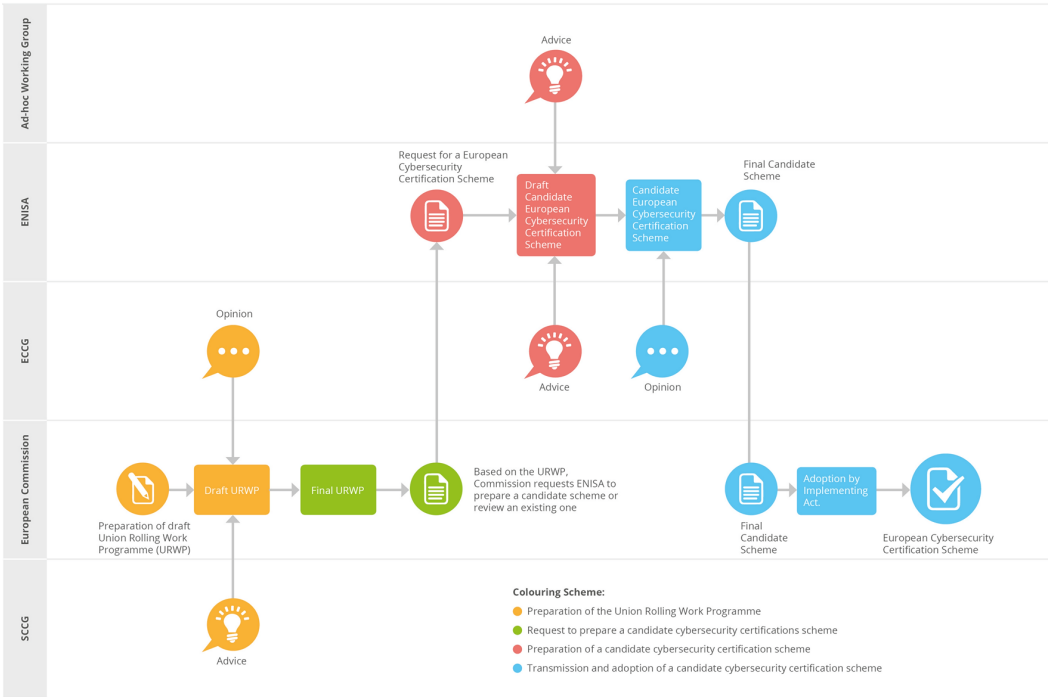

Figure 2-2: ENISA's view of Stakeholder's Interactions in the Cybersecurity Certification Framework[3]

2.2 European Cybersecurity Certification Group (ECCG)

The European Cybersecurity Certification Group was established to help ensure the consistent implementation and application of the Cybersecurity Act.

Description of the European Cybersecurity Certification Group (ECCG)[4]
The ECCG has the following tasks:

[3] Cybersecurity Certification Framework, downloaded from ENISA's website, full view available at https://www.enisa.europa.eu/topics/standards/certification/certification_graph_08.jpg/image_view_fullscreen

[4] Description of ECCG as taken from the Europen Commission's website at https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-group

to advise and assist the Commission in its work to ensure the consistent implementation and application of the Cybersecurity Act, in particular regarding the Union rolling work programme, cybersecurity certification policy issues, the coordination of policy approaches, and the preparation of European cybersecurity certification schemes;

- to assist, advise and cooperate with ENISA in relation to the preparation of a candidate scheme;
- to adopt an opinion on candidate schemes prepared by ENISA;
- to request ENISA to prepare candidate schemes;
- to adopt opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes;
- to examine relevant developments in the field of cybersecurity certification and to exchange information and good practices on cybersecurity certification schemes;
- to facilitate the cooperation between national cybersecurity certification authorities under the Cybersecurity Act through capacity-building and the exchange of information, in particular by establishing methods for the efficient exchange of information relating to issues concerning cybersecurity certification;
- to support the implementation of peer assessment mechanisms in accordance with the rules established in a European cybersecurity certification;
- to facilitate the alignment of European cybersecurity certification schemes with internationally recognised standards, including by reviewing existing European cybersecurity certification schemes and, where appropriate, making recommendations to ENISA to engage with relevant international standardisation organisations to address insufficiencies or gaps in available internationally recognised standards.

Members
The ECCG is composed of representatives of national cybersecurity certification authorities or representatives of other relevant national authorities. A member of the ECCG cannot represent more than two Member States. Stakeholders and relevant third parties may be invited to attend meetings of the ECCG and to participate in its work.

The European Cybersecurity Certification Group meetings agendas
The ECCG meets regularly, usually during plenary sessions. The agenda is proposed by the secretariat and agreed on by all members.

2.3 European Cyber Security Organisation (ECSO)

Organisations such as the European Cyber Security Organisation (ECSO) have specifically designed working group efforts which are intended to address this need for certification, by providing options for pathways including via composition (integration) certification recommendations and looking at specific frameworks such as common criteria in order to find more user friendly and efficient ways of achieving certification without any loss of level of security.

Through its Working Group 1, ECSO Working Group established itself as a fully-fledged European stakeholder in supporting the development of European certification schemes, standards and legislations (member of the SCCG, MoU with ETSI, CEN/CENELEC, collaboration with ENISA and JRC).

- ECSO WG1 brings together certifiers, manufacturers, system integrators and service providers to:
- Understand the challenges of the industry in using standards and certification schemes
- Understand the needs of the market to identify the gaps in standardisation and propose a roadmap for priorities
- Define what harmonisation means towards a European cyber security certification framework
- Focus on the testing and validation of the supply / value chain in Europe

Important publications resulting from ECSO's Working Group 1 are:

- 12/2020, WG1 MEMBERS - European Cyber Security Certification: Challenges ahead for the roll-out of the Cybersecurity Act (Download file from ECSO's web site).
- 11/2020, WG1 MEMBERS - Product Certification Composition Document (Download file from ECSO's web site),
- 9/2019, WG1 MEMBERS - European Cyber Security Certification: Assessment Options (Download file from ECSO's web site).
- 12/2017, WG1 MEMBERS - State of the Art Syllabus: Overview of existing Cybersecurity standards and certification schemes v2 (Download file from ECSO's web site).
- 12/2017, WG1 MEMBERS - European Cyber Security Certification: A Meta-Scheme Approach v1.0. (Download file from ECSO's web site).
- 6/2017, WG1 MEMBERS - State of the Art Syllabus: Overview of existing Cybersecurity standards and certification schemes (Download file from ECSO's web site).

2.4 Standards Bodies

In Deliverable 3.3, the role of the standards bodies is described in detail. Many studies have been undertaken by ENISA in cooperation with ETSI and CEN CELENEC. These studies are available online on ENISA's web site under "Publications"[5]. The work of ETSI's TC Cyber's work is split across 9 key areas: understanding the cybersecurity ecosystem, IoT security and privacy, cybersecurity for critical national infrastructures, protection of personal data and communication, enterprise and individual cybersecurity, cybersecurity tools, support to EU legislation, forensics, and quantum-safe cryptography. A glimpse of future topics can be seen from ETSI's TC Cyber's roadmap in cybersecurity as illustrated Figure 2-3.

[5] ENISA Publications undertaken with ETSI and CEN CENELEC available online at ENISA in cooperation with ETSI and CEN CELENEC has worked on multiple studies, available under Publications.

Figure 2-3: ETSI future possibilities in upcoming standards

2.5 Regulatory Framework

In Deliverable 3.3, the regulatory framework is described. The topics influencing certification in key areas are provided in the following subsections.

2.5.1 General Data Protection Regulation" (GDPR)

The goal of the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, better known as "General Data Protection Regulation" (GDPR) is to further harmonise data privacy laws across Europe, by gathering the most highly respected standards or principles around the world and applying them to protect EU citizens' data privacy.

When it comes to certification, the GDPR establishes certification mechanisms with the objective of demonstrating compliance. Certification mechanisms in the GPDR are distinguished in certifications, data protection seals and marks. A certificate is "a statement of conformity" with a specific set of requirements. A seal or mark can be evidence of the successful completion of the certification procedure and accompanied by a visual representation (e.g., a logo or symbol) which demonstrates that the object of the certification has been independently assessed in a certification procedure and

conforms to specific requirements of regulations, standards and technical specifications. [6]

2.5.2 European Data Protection

The European Data Protection Board (EDPB) mentions that certification can work as an accountability tool. [7] Certification mechanisms are advantageous due to their ability to improve transparency for data subjects[8] but also for commercial relationships, for example between controllers and processors. [9] Article 42(1) GDPR provides that certification mechanisms shall be established for the purpose of demonstrating compliance with the GDPR of processing activities.

In addition, the GDPR gives examples of the areas where approved certification mechanisms can be used as tools to demonstrate compliance with obligations of controllers and processors including for the implementation and demonstration of appropriate technical and organisational measures as referred in Articles 24(1), (3), 25 and 32(1), (3); as well as for sufficient guarantees from processor to controller or from sub-processor to processor based on Article 28(5) paragraphs 1 and 4 respectively.

Nonetheless, it is important to clarify certification is a voluntary process to assist in demonstrating compliance with the GDPR, and not a mandatory obligation or requirement. [10] The adherence to approved certification mechanisms must however be considered by supervisory authorities as a mitigating factor when exercising their powers, especially for the imposition and amount of administrative fines.[11]

The Cybersecurity Act supports the GDPR's introduction of certification mechanisms as a tool for compliance. It has the potential to establish certification mechanisms which directly tackle scenarios of data processing in ICT products and services, while at the same time satisfying the requirements of Article 42 of the GDPR.

2.6 Four Large Competence Centre Network Pilot Projects

"To strengthen European cybersecurity capacity, the Commission proposed the creation of a new European Cybersecurity Industrial, Technology and Research Competence Centre and a network of national coordination centres. The Centre which will be situated in Bucharest will pool expertise and align European development and deployment of cybersecurity technology. It will work with industry, the academic community and others to build a common agenda for investments into cybersecurity, and decide on funding priorities for research, development and roll-out of cybersecurity solutions, for example, through the Horizon Europe and Digital Europe Programmes).[12]"

For the realisation of a European Cybersecurity Industrial, Technology and Research Competence Centre with a Network of National Coordination Centres (CCCN), the

[6] Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation, version 3, 4 June 2019, para. 18, available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_en
[7] Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation, version 3, 4 June 2019, para. 4, available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_en
[8] Recital 100 GDPR clearly encourages organisations to rely on certification mechanisms in order to enhance transparency and compliance with the GDPR, and hence allow data subjects to assess the level of data protection of relevant products and services.
[9] Ibid.
[10] Article 42(3) General Data Protection Regulation.
[11] Article 83 (2(j)) General Data Protection Regulation.
[12] From CyberSec4Europe website at https://cybersec4europe.eu/our-community/

European Commission launched a pilot phase under the Horizon 2020 programme. In support of this, the pilot projects CONCORDIA, ECHO, SPARTA and CyberSec4Europe started at the beginning of 2019 with similar goals to assist the EC during the establishment of the CCCN.

Currently, the four pilot projects are running to lay the groundwork for the Competence Centre and Network. They involve more than 170 partners and collaborate closely under the brand Cyber Competence Network. Representatives from the four pilots are collaborating in a set of focus groups, ranging from governance, education and communications to cyber ranges, roadmapping and threat intelligence."[12]

2.6.1 CONCORDIA

Cybersecurity cOmpteNCe fOr Research and InnovAtion
Website: https://www.concordia-h2020.eu/

"CONCORDIA is a consortium of more than 50 partners from academia, industry and public bodies. Its mission is to integrate Europe's excellent cybersecurity competences into the network of expertise to build the secure, resilient and trusted ecosystem for European Digital Sovereignty."[13]

"A **Cybersecurity Competence Network** with leading research, technology, industrial and public competences. **CONCORDIA** provides excellence and leadership in technology, processes and services to establish an user-centric EU-integrated cyber security ecosystem for digital sovereignty in Europe."[14]

Work Package 5, Task 5.3 "This task will focus on the certification and standardization activities of the project. First, it will deliver a comprehensive certification and standardization strategy to be followed and further refined throughout the duration of CONCORDIA. This strategy starts by updating the analysis performed during the proposal writing with the review of certification procedures, standards, and best practices that are relevant to this project. The objective is to ensure alignment with the technologies to be developed (WP1), as well as the pilots (WP2). To this end, the project will monitor continuously the evolving certification, standardization and best practices landscape, in order to timely identify other initiatives that may be linked to CONCORDIA areas of interest."[15]

- Deliverable D5.1: 1st year report on exploitation, dissemination, certification and standardization
- Deliverable D5. 2nd year report on exploitation, dissemination, certication and standardization(M24)[16]

2.6.2 CyberSec4Europe

Cyber Security for Europe
Website: https://cybersec4europe.eu/

"CyberSec4Europe is a consortium of 43 partners across 20 Member States and two Associated Countries. With over 100 cybersecurity projects between them, the

[13] Description from Cyber Competence Network, Convergence Event at https://cybercompetencenetwork.eu/events/past-events/convergence/concordia-session/
[14] From CONCORDIA website at https://www.concordia-h2020.eu/
[15] From CONCORDIA Deliverable D5.1 at https://www.concordia-h2020.eu/wp-content/uploads/2020/05/D5.2-1stYearReportOnExploitationDisseminationCertificationandStandardization.pdf
[16] CONCORDIA Deliverables for downloading at: https://www.concordia-h2020.eu/deliverables/

CyberSec4Europe consortium partners cover a wide spectrum of cybersecurity issues: 14 key cybersecurity domain areas, 11 technology/applications elements and nine crucial vertical sectors. CyberSec4Europe's **main objective** is to pilot the consolidation and future projection of the cybersecurity capabilities required to secure and maintain European democracy and the integrity of the Digital Single Market. CyberSec4Europe has translated this broad objective into measurable, concrete steps: three policy objectives, three technical objectives and two innovation objectives.

Work Package 8 "Standardization" maintains contact and collaboration with standards developing organisations (SDOs) with the aim of linking the technical work of the project to standards. In addition to maintaining contacts with the (European) SDOs and the relevant cybersecurity committees, this work links the technical work of the project to standards and standards to the project and, in so doing, assessing the appropriateness of the existing standardisation procedures for the cybersecurity goals". [12]

The following CyberSec4Europe deliverables related to standards have been published:

- Deliverable 8.1: Cybersecurity Standardization Plan
- Deliverable 8.2: Project Standards Matrix (together with the Standards Matrix)
- Deliverable 8.3: Cybersecurity Standardization Engagement Plan 2[17]

2.6.3 ECHO

European network of Cybersecurity centres and competence Hub for innovation and Operations
Website: https://echonetwork.eu/

"The ECHO consortium consists of 30 partners from different fields and sectors including health, transport, manufacturing, ICT, education, research, telecom, energy, space, healthcare, defence & civil protection. The main objective of ECHO is to strengthen the proactive cyber defence of the European Union, enhancing Europe's technological sovereignty through effective and efficient multi-sector and multi-domain collaboration. The project will develop a European Cybersecurity ecosystem, to support secure cooperation and development of the European market, as well as to protect the citizens of the European Union against cyber threats and incidents."[18]

⇒ ECHO Security **Certification Scheme**: Development of sector specific security certification needs within EU Cybersecurity Certification Framework from ENISA.
⇒ Deliverable D2.9 : ECHO Cybersecurity Certification Scheme[19]

2.6.4 SPARTA

Website:

"The SPARTA consortium consists of 44 core partners.

[17] CyberSec4Europe Deliverables for downloading at https://cybersec4europe.eu/publications/deliverables/
[18] Description from ECHO website. https://echonetwork.eu/
[19] ECHO Deliverable for downloading at: https://echonetwork.eu/deliverables/

Mission: Re-imagining the way cybersecurity research, innovation, and training are performed in Europe across domains and expertise, from foundations to applications, in academia and industry.
Impact: SPARTA will create a long-lasting community capable of collaboration to define, develop, share, and evolve solutions that will help practitioners prevent cybercrime and enhance cybersecurity.
Vision: Become a unique innovation force in cybersecurity with transformative impacts on European Union economy, infrastructures, society and democracy."

Certification Organization and Support:
Given the growing threats that connected systems face, it has become important to protect IT-based infrastructures and systems sufficiently. Cybersecurity certification is one way to help engineers design more secure systems. Over the years, many cybersecurity standards and certifications schemes have been created at both European and international level. In the context of the European digital single market, it is important to have a simple cybersecurity certification scheme that is recognized throughout all European countries. To move in this direction there is a need to analyse different national European cybersecurity initiatives as well as international efforts in order to identify commonalities and differences. Standards and certification schemes can be classified in different ways. Some standards and schemes have been designed for products and others for processes and services. Other standards are sector-specific such as in transport or aeronautics. Others focus on specific technologies, e.g., networks or cloud computing. More widespread adoption of cybersecurity certification in the design of connected products and services will be successful only if certification is perceived as cost-effective and that it effectively improves the quality of products and services. For certification to be more widely adopted in security engineering, there is a clear need to design more agile certification processes, to better integrate certification in the security engineering process, and to improve the effectiveness of certification schemes.

Final goal: Identification of commonalities and differences between national cybersecurity certification initiatives and recommendations for convergence at the European level:

- D11.1: International and national cybersecurity certification initiatives
- D11.2: Cybersecurity compliant development processes[20]

[20] SPARTA Deliverables for downloading at https://www.sparta.eu/deliverables/

3 Cyberwatching.eu's Engagement in Projects, Standards and Certification

Standardisation and certification is one of the main pillars of the cyberwatching.eu projects and is the central topic of WP3 activities. Throughout the lifetime of the project we have engaged directly with EC-funded projects in order to understand how they are addressing this topic and also to gather data for our own deliverables and reports. Using the mapping and radar-related activities and strong community engaged through the cyberwatching.eu website and events, we have been able to carry out a series of activities which are detailed below.

3.1.1 Survey 2018 - Gaps in Cybersecurity Standards and Certification

A survey was launched in 2018 to obtain feedback from the EU cybersecurity projects, cybersecurity users (public and private sectors), and cybersecurity products and services providers to identify the gaps in cybersecurity standards and the certification environment. The results of this survey are given in Deliverable D3.3 "White Paper on cybersecurity standard gap analysis "[21].

3.1.2 Webinar 2018 - Cybersecurity standards & certification Challenges

On September 5, 2018, a webinar on the challenges faced in the area of standards and certification took place. During this webinar, the issues of the gaps in cybersecurity certification, including harmonization were covered. In addition, the areas of trust, GDPR, governance, risk management, among other topics of interest within the cybersecurity community were discussed[22]. Although this webinar was specifically dedicated to the topic of standards and certification, the topic has been addressed in the majority of other webinars organised by cyberwatching.eu[23].

3.1.3 White Paper 2018 - Gaps in Standardization and Certification

In October 2018, cyberwatching.eu published its Deliverable D3.3 "White Paper on Gaps in Standardization and Certification"[21] following thorough research and containing feedback from the stakeholder community. The focus of this deliverable is to address the issue, with a white paper, of identifying the gaps in cybersecurity standards (and hence also certification). This is done using the methodology of focused desk research, first and foremost, in order to gather together and to summarize all of the key efforts that have gone before. We thereafter survey the cybersecurity research, industry, public sector and user communities in order to get inputs into identifying the perceived gaps.

3.1.4 April 2021 – 7th 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, 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.

[21] Cyberwatching Deliverable D3.3 available online at: https://www.cyberwatching.eu/d33-white-paper-cybersecurity-standard-gap-analysis
[22] Agenda and topics of 2018 Webinar available online at: https://www.cyberwatching.eu/cybersecurity-standards-and-certification
[23] https://www.cyberwatching.eu/webinar

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.

3.1.5 Concertation Event 2021 - Priorities, trends & clustering in R&I landscape

Arriving at the end of the Cyberwatching.eu project, a key feature of the Fourth Concertation event held on July 13, 2021, was to discuss new partnership opportunities between projects based on the **EU Project Radar.** Indeed, the Radar was used to demonstrate current funded activities in some of the topics covered in the calls, identifying for participants the projects working in technical areas or vertical sectors. The radar was also highlighted as a useful tool for the process of proposal writing in terms of quickly accessing reliable statistics on these topics such as funding levels and number of projects funded. The key takeaways are available in the Conclusions to this Deliverable. Standardisation and Certification was also a topic included in Concertation 2018 (see Deliverable D3.2[24]) and 2019 see Deliverable D3.4[25]) as described in the aforementioned deliverables.

3.1.6 Concertation Event 2021 – "Standards and certification of a trusted Digital Europe"

The last Concertation Event for Cyberwatching.eu project took place on July 13, 2021. A session was devoted to standards and certification with key players participating, namely:

- Roberto Cascella, ECSO, presenting "***ECSO WG 1 Standardisation, certification and supply chain management***" (Presentation attached as Annex A)
- George Sharkov, European DIGITAL SME Alliance & SBS, presenting "***Supporting European participation in the standardisation process***" Presentation attached as Annex B)
- Chatzopoulou Argyro, TÜV TRUST IT GmbH, presenting "***Linking Standardisation and Certification - Plans for the future"*** (Presentation attached as Annex C)

[24] https://www.cyberwatching.eu/d32-european-cybersecurity-and-privacy-research-innovation-ecosystem

[25] https://www.cyberwatching.eu/d34-eu-cybersecurity-legal-and-policy-aspects-preliminary-recommendations-and-road-ahead

- Chaired by Mark Miller, CONCEPTIVITY & Cyberwatching.eu

The key takeaways from this Webinar with respect to this session are given in the Conclusions to this Deliverable.

4 From Research to Innovation

Within the academic domain, there are a number of different activities that are looking into the different types of cybersecurity labelling and their effectiveness. An area where this approach may be of critical importance is of course within newly emerging critical areas such as the Internet of Things, Artificial intelligence and Industry 4.0. Within all of these we are seeing the emergence of technical systems which will either dynamically connect and facilitate the interaction of autonomous or semi-autonomous components on a hitherto unprecedented scale or create algorithms or services which will directly impact members of society in nearly every walk of life. Key to the challenge within these domains is how the different contributors in terms of software and hardware systems will all have to work to comply with standards of a technical and non-technical nature. It is essential for instance that we move towards meaningful cybersecurity badging for IoT devices where the providers of these technologies will range from large well-recognised multinational corporations to the back-office provider of globalisation which will not already have a trusted reputation developed. All of these must be equally secure at the point of deployment.

For Artificial Intelligence there is of course emerging codes of practice about how these technologies are utilized to ensure they are utilized under an appropriate code of ethics. Through organization such as the Alan Turing Institute [26] and recent publications such as Bostrum & Yudkowsky - The Ethics of Artificial Intelligence, there is an ever-increasing body of research into both the ethical application of AI but also how ethics apply to AI systems themselves. It is therefore only logical that at some point a labelling system of products or services is developed in compliance with contemporary legislation that is established in the area. This will, it is hoped, give consumers confidence in these tools or services, while also demonstrating how they comply with existing legislation.

There is a well-developed community of research in the cybersecurity and trust of these critical areas and it is essential that we see these blue skies research outputs move through the innovation space to become adopted in future. Therefore seeing some of these areas being supported by specific Horizon Europe funding calls is good though they currently focus on the technical rather than whole system issues and so will require these new activities to align with other projects or outputs that are supported through other mechanisms.

4.1 European Projects – Research and Innovations

One of the tasks performed along these four years has been the characterization of the projects in the EU project radar. This includes information collected and managed by projects themselves for the purposes of the project hub web pages and also the MTRL self-assessment. The information provides an evaluation of the projects' market maturity and their affinity with Priorities for the definition of a Strategic Research and Innovation Agenda in Cybersecurity. This has made it possible to determine the alignment between the results obtained and the trends set by Europe, in order to determine whether it is necessary to maintain the established strategy or identify areas in which it is necessary to reinforce investment are identified. The result of this analysis is reflected in Deliverable D2.8 Recommendations report on R&I needs.

[26] https://www.turing.ac.uk

4.1.1 Projects related to standardization and certification

Based on the analysis performed in Deliverable D2.8, we have identified 53 projects (26% of the projects on the radar) addressing the priority "Approaches, methods, processes to support cybersecurity assessment, evaluation and certification", although most of them are related to threat detection and mitigation tools and techniques: identifying potential threats, providing a list of prioritized response actions, and delivering a means to execute these responses. There are quite a lot of projects developing tools for cyber risk assessment and even cyber culture assessment.

On the other hand, there are not so many projects that delve into certification and / or standardization schemes.

5	ANASTACIA	70	MITIGATE	166	SPEAR	223	SECREDAS
7	ARMOUR	71	MUSA	168	DEFEND	225	CYBERSECURITY
14	certMILS	73	NeCS	172	CONCORDIA	227	SAFECARE
24	COMPACT	98	PRIVACY FLAG	174	SPARTA	229	SPHINX
30	CYBECO	105	REASSURE	175	CyberSec4Europe	231	SECONDO
33	CYRail	124	SMESEC	176	ECHO	236	D-FENCE
36	DEFENDER	131	STOP-IT	178	PDP4E	239	InfraStress
40	DOGANA	132	STORM	185	PANACEA	242	CYBERCULT
46	EU-SEC	134	SUPERCLOUD	188	SecureIoT	245	EnergyShield
50	FutureTrust	143	VESSEDIA	201	CyberSure	250	PHOENIX
52	GHOST	146	WISER	207	CLTRe	263	SDN-microSENSE
55	HERMENEUT	155	CYBER-TRUST	209	GO 4G		
58	KONFIDO	159	FUTURE TPM	217	CUREX		
64	MAS2TERING	165	POSEIDON	222	RESISTO		

Table 4-1: Projects in the priority "Approaches, methods, processes to support cybersecurity assessment, evaluation and certification"

Of the projects listed above in table 4-1, 30 have carried out an MTRL self-assessment at least once as reported in D2.8. The matrix lists the projects, classifying their TRL scores, which classifies the technology readiness in each project in IDEA, PROTOTYPE, VALIDATION and PRODUCTION, and their MRL scores, which classifies the market readiness in Not marketable yet, Need to improve marketing, Ready to commercialize and Product stable (**Error! Reference source not found.**).The projects identified hereafter are those that most clearly address the certification and/or standardization schemes.

TRL
IDEA
PROTOTYPE
VALIDATION
PRODUCTION

MRL
Not marketable yet (NMY)
Need to improve marketing (NTIM)
Ready to commercialize (RTC)
Product stable (PS)

Table 4-2: Legend for MTRL

Only 5 out of the 21 finished projects are Ready to commercialise, 5 are not marketable and 11 Need to improve some marketing capabilities.

None of the 9 ongoing projects are Ready to commercialise, 3 are not marketable and 6 Need to improve some marketing capabilities.

N	Project	End	IDEA	PROTO	VALID	PROD
5	ANASTACIA	01/12/2019			NMY	
24	COMPACT	01/10/2019			NTIM	
40	DOGANA	01/08/2018			RTC	
46	EU-SEC	01/12/2019			NTIM	
50	FutureTrust	01/05/2019			NTIM	
52	GHOST	01/04/2020			RTC	
55	HERMENEUT	01/04/2019			NTIM	
58	KONFIDO	01/10/2019		NMY		
71	MUSA	01/12/2017		NTIM		
124	SMESEC	01/05/2020			NTIM	
131	STOP-IT	01/05/2021				RTC
155	CYBER-TRUST	01/04/2021			NTIM	
159	FUTURE TPM	31/12/2020	NMY			
165	POSEIDON	01/10/2020			NTIM	
168	DEFEND	01/05/2021			RTC	
175	CyberSec4Europe	22/07/2020	NMY			
176	ECHO	01/02/2023			NTIM	
178	PDP4E	30/04/2021			NTIM	
185	PANACEA	31/12/2021		NTIM		
188	SecureIoT	20/12/2020			RTC	
217	CUREX	01/11/2021			NTIM	
222	RESISTO	01/04/2021			NMY	
223	SECREDAS	01/04/2021			NTIM	
227	SAFECARE	30/11/2021			NTIM	
229	SPHINX	31/12/2021	NMY			
231	SECONDO	01/12/2022	NMY			
239	InfraStress	01/05/2021			NTIM	
245	EnergyShield	01/06/2022	NTIM			
250	PHOENIX	31/08/2022	NMY			
263	SDN-microSENSE	30/04/2022			NTIM	

Table 4-3: MTRL results of certification and standardization projects

The projects identified hereafter are those that most clearly address the certification and/or standardization schemes.

4.1.2 ARMOUR

Large-Scale Experiments of IoT Security Trust

Solutions that allow the occasional testing, test environment and **certification** of large-scale IoT deployments validating the Security, Privacy and Confidence of new deployments. ARMOUR developed a certification methodology based on the ETSI proposal by combining the two approaches of testing and risk assessment and it applies model-based testing approaches to large-scale IoT systems.

4.1.3 certMILS

Compositional security certification for medium- to high-assurance COTS-based systems in environments with emerging threats
Website: https://certmils.eu/

A security certification methodology for Cyber-physical systems (CPS). The "MILS" in certMILS stands for "Multiple Independent Levels of Safety/Security", indicating that

certMILS uses a special kind of operating systems called "separation kernel" (SK). This kind of operating system focuses being highly deterministic and reliable and puts user functionality into the application layer. Compositional security **certification** for medium- to high-assurance COTS-based systems in environments with emerging threats:

- MILS Security Architecture Templates
- Strategy for Security Certification of the Development and Product Lifecycle in High Assurance Industrial Cyber-Physical Systems
- A Platform Approach for Fusing Safety and Security on a Solid Foundation Pilots: Smart grid, railway, subway

4.1.4 CyberSec4Europe

Cyber Security for Europe
Website: https://cybersec4europe.eu/
See Section 2.6.2.

4.1.5 CyberSure

CYBER Security InSURancE — A Framework for Liability Based Trust
Website: https://www.cybersure.eu/

It is a programme of collaborations and exchanges between researchers aimed at developing a framework for creating and managing cyber insurance policy for cyber systems. The purpose of creating such policies will be to enhance the trustworthiness of cyber systems and provide a sound basis for liability in cases of security and privacy breaches in them. The framework will be supported by a platform of tools enabling an integrated risk cyber system security risk analysis, certification and cyber insurance, based on the analysis of objective evidence during the operation of such systems. The development of the CyberSure platform will be driven by **certification**, risk analysis and cyber insurance scenarios for cyber system pilots providing cloud and e-health services.

4.1.6 ECHO

European network of Cybersecurity centres and competence Hub for innovation and Operations
Website: https://echonetwork.eu/
See Section 2.6.4.

4.1.7 EU-SEC

The European Security Certification Framework
Website: https://www.sec-cert.eu/

Framework for multiparty recognition between trustworthy cloud services security certification: The framework defines the principles, criteria, processes and technical capabilities for the mutual recognition between various National, International and sector specific cloud security certifications and attestations.

Continuous Auditing based security **certification** for trustworthy cloud services: Continuous auditing-based certification relies on tools, methods and processes that allow for security properties of cloud services being checked with a frequency that depends on the service level/qualitative objectives (SLO & SQO) agreed upon between the parties. EU-SEC aims to enhancing trustworthiness and transparency in the ICT supply chain through business cases developed and piloted by industrial partners.

4.1.8 FutureTrust

Future Trust Services for Trustworthy Global Transactions
Website: https://www.futuretrust.eu/

FutureTrust project will address the need for globally interoperable solutions through basic research with respect to the foundations of trust and trustworthiness, actively support the **standardisation** process in relevant areas, and provide Open Source software components and trustworthy services which will ease the use of eID and electronic signature technology in real world applications. In particular the FutureTrust project will extend the existing European Trusted List (TL) infrastructure towards a "Global Trust List", develop a comprehensive Open Source Validation Service as well as a scalable Preservation Service for electronic signatures and seals and will provide components for the eID-based application for qualified certificates across borders, and for the trustworthy creation of remote signatures and seals in a mobile environment.

4.1.9 KRAKEN

BroKeRage and MArKet platform for pErsoNal data
Website: https://www.krakenh2020.eu/

KRAKEN is a trusted and secure personal data platform with state-of-the-art privacy aware analytics methods (with guarantees on metadata privacy, including query privacy). The KRAKEN project aims to enable the sharing, brokerage, and trading of potentially sensitive personal data, by returning the control of this data to citizens (data providers) throughout the entire data lifecycle.

KRAKEN will **standardize** different IT solutions thanks to featuring the (privacy-preserving) integration of independently obtained data sources from subjects consenting to different analyses. The project combines, interoperates, and extends the best results from two existing mature computing platforms developed within two H2020 actions: CREDENTIAL and MyHealthMyData. Creating economic value and innovative business models for 'personal data spaces' and supporting the Digital Single Markets' data economy by incentivizing parties, in particular SMEs, to actively engage in the data market.

4.1.10 OCGN

Traditional Organised Crime and the Internet: The changing organization of illegal gambling networks

The project examines online gambling and extortion networks. The objectives of this research are:

- establish tools and technique that facilitate management of internal/external cyber-threats to online gambling sector
- validate tools and techniques that will facilitate the management of internal/external cyber-threats to online gambling sector
- set **standards** of information management
- set **standards** of dissemination and flows of information to cybersecurity centres from online gambling sector in EU

This is to be achieved by:

- interviews with key individuals (systems managers at online sites and law enforcement)
- analyse data for information flows and breaking down volume of information into accessible data for internal and external use.
- analyse current decision-making processes/systems and processing information

- analyse exchange of data to improve and implement best practice available in cybersecurity across EU online gambling sites

4.1.11 PANACEA

Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for dAta and people
Website: https://www.panacearesearch.eu/

The PANACEA project provides all healthcare actors with an assessment and system monitoring audit workflow to easily run conformity assessment and engineering assessment.

The PANACEA project has developed, with three European Healthcare Centres, a people-centric toolkit of nine tools, to assess and improve the cybersecurity readiness of healthcare socio-technical systems (ICT, networked medical devices, staff) and of medical device/system lifecycles. It includes software-based innovative tools:

- dynamic risk assessment, based on a multi-layer attack graph model including "human" and "business" layers, and automatic generation of mitigation recommendations,
- inter-organizational secure information and heavy images sharing,
- regulatory compliant security-by-design and certification of systems/medical devices,
- machine-to-machine and smartphone-based facial identification (also with masks).

It also includes non-technical tools, influencing staff behaviour and supporting the management through:

- contextualized risk governance models,
- educational voiceless videos,
- methodology to produce behavioural "nudges",
- methodology to maximize cybersecurity return-on-investment,
- guidance for contextualized deployment of previous tools.

Potential integrated use of the nine tools' is a further innovative feature, supporting full plan-do-check-act and multi-disciplinary approaches to cybersecurity preparedness.

4.1.12 PHOENIX

Electrical Power System's Shield against complex incidents and extensive cyber and privacy attacks
Website: https://phoenix-h2020.eu/

PHOENIX aims to offer a cyber-shield armour to European EPES infrastructure enabling cooperative detection of large scale, cyber-human security and privacy incidents and attacks, guarantee the continuity of operations and minimize cascading effects in the infrastructure itself, the environment, the citizens and the end-users at reasonable cost.

PHOENIX will realise 3 strategic goals:

1. Strengthen EPES cybersecurity preparedness by employing security a) "by design" via novel protective concepts for resilience, survivability, self-healing and accountability, and b) "by innovation" via adapting, upgrading and integrating a number of TRL5 developments to TRL7-8 and validating them in real-live large scale pilots;
2. Coordinate European EPES cyber incident discovery, response and recovery, contributing to the implementation of the NIS Directive by developing and validating at national Member States and pan-European level, a novel fully decentralized inter-DLTs/blockchain based near real-time synchronized cybersecurity

information awareness platform, among authorized EPES stakeholders, utilities, CSIRTs, ISACs, CERTs, NRAs and the strategic NIS cooperation group;
3. Accelerate research and innovation in EPES cybersecurity by a novel deploy, monitor, detect and mitigate DevSecOps mechanism, a secure gateway, privacy preserving federated Machine Learning algorithms and establishment of **certification** methodologies and procedures through a Netherlands-based Cybersecurity Certification Centre.

4.1.13 PRIVACY FLAG

Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployments
Website: https://privacyflag.eu/

Privacy Flag is developing a set of tools to enable citizens to check whether their rights as data subjects are being respected, and tools and services to help companies comply with personal data protection requirements.

⇒ **Privacy Certification**: https://privacyflag.eu/pf-tools/privacy-certification-scheme/

4.1.14 SAPPAN

Sharing and Automation for Privacy Preserving Attack Neutralization
Website: https://sappan-project.eu/

A platform for sharing and automation to enable privacy preserving and efficient response and recovery utilizing advanced data analysis and machine learning. SAPPAN will provide a cyber threat intelligence system that decreases the effort required by a security analyst to find optimal responses to and ways to recover from an attack. SAPPAN will enable a European level perspective on advanced cyber security threats detection, response, and recovery making four key contributions that go beyond existing approaches: (1) privacy-preserving aggregation and data analytics including advanced client-side abstractions; (2) federated threat detection based on sharing of anonymised data and sharing of trained machine learning models; (3) **standardisation** of knowledge in the context of incident response and recovery to enable reuse and sharing; (4) visual, interactive support for Security Operation Center operators.

4.1.15 SECREDAS

Cyber Security for Cross Domain Reliable Dependable Automated Systems
Website: https://secredas-project.eu/

SECREDAS stands for “Product Security for Cross Domain Reliable Dependable Automated Systems”. It looks at security, safety and privacy across multiple application domains: Road, Rail and Health. The project consortium will build a reference architecture for Secure and Safe Automated systems compliant with the new GDPR Regulation. It will develop a framework for multi-concerned security-safety verification and testing. Increased safety and privacy of IoT devices integrated in vehicles. A prototype of a radar/5G component capable of operating in the 76-81 GHz frequency band. Develop guidelines for continuous multi-concern (safety and security) **certification** including assessment methods.

4.1.16 SMESEC

Protecting Small and Medium-sized Enterprises digital technology through an innovative cyber-SECurity framework
Website: https://www.smesec.eu/

The main goal of SMESEC is to identify what are the needs from the SME perspective and translate them into requirements for a unified framework, which will eventually consist of the SMESEC partners' contributed products. The products can cover a wide range of security market segments, and it is expected that the unification will bring even higher added value to the products and the Framework.

High quality cyber-security solutions attractive to companies and organizations with restricted budget; increase protection by focusing on increasing awareness and training for SMEs and their "insiders"; consolidating international and European links and harmonizing solutions with general **standards** and directives; ready to market solutions.

The suite supports SMEs in managing network information security risks and threats and identifying opportunities for implementing secure, innovative technologies for the digital market. As a benefit, the framework shall allow SMEs not only look at cyber-security as an obstacle but also as an opportunity for business.
USE CASES: Smart City, Industrial IoT, Smart Grid, E-voting

4.1.17 SPHINX

A Universal Cyber Security Toolkit for Health-Care Industry
Website: https://sphinx-project.eu/

SPHINX aims to introduce a health tailored Universal Cyber Security Vulnerability Assessment and **Certification** Toolkit, thus enhancing the cyber protection of the Health and Care IT Ecosystem and ensuring patients' data privacy and integrity. A Holistic Cyber Security vulnerability assessment toolkit, that will be able to proactively assess and mitigate cyber-security threats known or unknown, imposed by devices and services within a corporate ecosystem.

4.1.18 STANDICT 2023

Supporting European Experts Presence in International Standardisation Activities in ICT
Website: https://standict.eu/

StandICT.eu 2023[27] is a EU framework project H2020 Coordination and Support Action with the central goal to ensure a neutral, reputable, pragmatic and fair approach to support European and Associated states presence in the international ICT standardisation scene. The project manages the StandICT.eu Fellowship Programme, a series of 10 Open Calls, providing €3 million funding to support and incentivise participation of European standardisation specialists in key international and global SDOs and consortia.

It has also created the ICT Standardisation Observatory – (EUOS)[28] providing an exhaustive mapping of the global Standards arena in a range of crucial technological domains made possible by the reinforced EU presence in the international ICT Standardisation scene through Fellowship Programme and strengthened synergies with ongoing programmes at an EU and national level.

Finally, the project also shapes "the next generation of European Standards experts" through education initiatives and training, aiming ultimately to become a key reference point for engagement in ICT Standards activities both for industry and Academia.

[27] https://www.standict.eu/
[28] https://www.standict.eu/euos

4.1.19 VESSEDIA

Verification Engineering of Safety and Security Critical Dynamic Industrial Applications

VESSEDIA proposes to enhance and scale up modern formal methods-based software analysis tools to enable using them on a wider range of applications than embedded safety-critical applications (in the Nuclear, Transportation, Energy supply, Process control and Space areas). Developers will benefit rapidly from the outcome of the project when developing connected applications. At the forefront of connected applications is the Internet of Things (IoT), whose growth is exponential and whose security and safety risks are real (for instance in hacked smart phones or smart home devices). VESSEDIA will take this domain as a target for demonstrating the benefits of using our tools on connected applications. Impacts on quality assurance, security evaluation and certification, from tooling and methodological standpoints.
USE CASES:

- Contiki OS environment (operating system for the IoT)
- CEA's use case, MPL routing
- DA's use case: several interacting applications (an experimental Aircraft Maintenance System application prototype, a datalink (DL), a blockchain application, a software gateway and a security proxy)

4.1.20 VISION

Visual Privacy Management in User Centric Open Environments

The VisiOn project developed a visual privacy platform to help public entities deliver safe and privacy-enhanced e-government services that meet the highest privacy standards and nowadays necessities, and offer citizens greater and personalised control over their data.

A validated set of business plans and models for the commercial exploitation of the project results (tools, services, platform), along with strategies of reaching potential customers.

5 ECSO's Cybersecurity label Made in Europe

"CYBERSECURITY MADE IN EUROPE" is an industry-driven marketing tool, designed to promote European cybersecurity companies and increase their visibility on the European and on the global market.

Figure 5-1: ECSO's Cybersecurity label "Made in Europe"

The ECSO Cybersecurity Label "Made in Europe" was launched in July 2020.

The Label serves as a market differentiator based on geographic location.

- The Label raises awareness of the strategic value of cybersecurity companies originating in Europe and developing their business based on trusted European values.
- The Label increases companies' visibility among potential business partners, end-users and cybersecurity investors.

European cybersecurity companies from the European Union Member States, the European Free Trade Association (EFTA) and European Economic Area (EEA) countries, as well as the United Kingdom (UK) can apply for the Label.

Applications are assessed by the qualified issuing associations, recognised by ECSO. Eligible companies can submit their applications to any qualified issuing association and will not be bound to the country in which their European headquarters are located. The Label is intended to designate the geographic – European – origin of a company and does not claim to measure the quality of its products and services. In order to qualify for the Label, European companies will be required to prove that:

- They are headquartered in Europe;
- They do not have any major ownership/control from outside of Europe;
- Europe is their primary place of business with more than a half of its cybersecurity R&D activities and staff located there;
- They provide trustworthy cybersecurity products and solutions, as defined in ENISA's 'Indispensable baseline security requirements for the secure ICT products and services';
- They respect European data and privacy requirements, defined by the EU's General Data Protection Regulation (GDPR).

Only ECSO authorised partners can issue the Label. Prospective companies can choose any qualified issuer of their choice regardless of the country in which their European headquarters are located. A list is provided on the ECSO web site[29].

[29] ECSO's Made in Europe Cybersecurity Label: http://www.ecs-org.eu/initiatives/cybersecurity-made-in-europe

6 AEI's Cybersecurity Seal

The background of the AE Cybersecurity Seal is given in Deliverable 3.3, Section 2.4[21]

In brief, the AEI Cybersecurity Seal for Organizations is a certification scheme that includes the security requirements that any organization must meet when it needs to demonstrate, in accordance with the requirements of the scheme, that it has the systems and physical and logical security measures necessary to protect their assets from the various threats that may cause damage to the organization's services or capabilities.

Figure 6-1: AEI Cybersecurity Seal Logo

The seal recognizes the company's compliance with a series of security requirements that include, but are not limited to Communications protocols, Data Protection, Infrastructure, Human Resources, Providers, Services. This seal goes beyond adhering to codes of conduct, since it integrates regulations, international standards and best practices into its specifications:

- LPIC or Law 8/2011, of April 28, which establishes measures for the protection of critical infrastructures and its RPIC regulation
- LOPD or Organic Law 15/1999, of December 13, on the protection of personal data
- ENS or National Security Scheme
- ISO 27001: 2014 Information technology. Security techniques. Information Security Management Systems (ISMS). Requirements.
- ISO 22301: 2013 Protection and security of citizens. Business Continuity Management System (SGCN). Specs.

The Cybersecurity Seal for Organizations is drawn up by the industry itself and provides its approved consultants with a reference methodology to implement security in accordance with the requirements of the Seal itself. The evaluation audit is carried out by an independent certifying entity, the currently authorized entity being Société Générale de Surveillance SA (SGS) Spain.

The certification mark used during the granting of the Label is managed by AEI. Only certified organizations (that have applied to join the Reference Framework and for which the AEI has opened a file, assigned the corresponding evaluation and agreed to its inclusion in the registry of organizations that meet the requirements of the Reference Framework) are authorized to use the Trademark of Certification. The use of this Mark is subject to certain conditions.

Proconsi, an ICT company specialized in the development and integration of IT solutions with more than 30 years of experience, based in Léon, was one of the first certified companies[30], and they have a team of certified consultants to support any company that wishes to obtain the AEI cybersecurity seal.

[30] Proconsi Website : https://www.proconsi.com/certificados-de-calidad-de-software-y-de-servicios-proconsi

IBERAVAL, S.G.R. is a Guarantee Company with extensive experience in Financial Services, specialists in providing financial solutions for freelancers, small and medium-sized companies of all sectors and business activities. Aware that operational and organizational risk management implies a continuous risk assessment in each of the key and critical points, Iberaval accredits this commitment with certification, since 2017, with the AEI Cybersecurity Seal for Organizations that involves a daily effort to comply with the requirements stablished in the Reference Framework.

7 Cyberwatching.eu's Cybersecurity Label

The Cybersecurity Label targets Europe's small businesses, especially start-ups and micro-SMEs that are approaching the IT security assurance landscape for the very first time. Created in a partnership between SGS, one of the leading global testing, inspection and certification companies, the Cybersecurity Label represents an important first step for small-sized companies to understand their current cybersecurity weaknesses. This means that they are better informed on their current status, how to act to improve their cybersecurity posture and potentially explore the benefits of certification.

Figure 7-1: Cyberwatching.eu Cybersecurity Label

With the EU Cybersecurity Act coming into force less than a year ago to provide an EU-wide harmonised framework to certify ICT products and services, cybersecurity certification can be a market differentiator for businesses. Certifications can help companies act with confidence and assure their customers and partners of their ability to defend themselves from cyberattacks and data breaches. However, for an SME, micro-enterprise or start-up, taking the first steps to certification can be both complex and daunting.

With so many standards, schemes and methodologies around, the landscape can be confusing. The Cybersecurity Label is a robust but lightweight first step for small businesses to carry out a self-assessment to understand where their weaknesses and priorities lie. Businesses need to carefully analyse their cybersecurity posture. It 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 is organised into 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 label is unique in helping companies to carry out a self-assessment which 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 long-term, companies can save time, money and avoid frustration in their journey to either enable certification or improve compliance to regulations.

The Label will be sustained by Cyberwatching.eu and its consortium partners which include the Spanish cybersecurity cluster AEI. It will also become one of the key assets of the Spanish Cybersecurity Innovation Hub CyberDIH. It is set up to support SMEs and is part of a broad EU-wide network of national hubs. The Label has value not only to European SMEs, but also to the whole ecosystem in terms of helping companies to improve their cybersecurity posture. This is key to creating a trusted digital economy in Europe and can be a vital asset for CyberDI's network of SMEs that are part of the cybersecurity innovation hub.

7.1 Description

Thus, in 2020, the innovative idea to have a light cybersecurity label was born. Trust-IT and AEI in partnership with SGS Spain (AEI member and current vice-president) reached agreement on the creation of a lightweight cybersecurity label for SMEs.

SGS is a leading and global provider of inspection, testing, verification and certification services. It is recognized as the global benchmark for quality and integrity. With 142 years of history, experience and insights, everything they do is underpinned by their ethics and Business Principles, ensuring they uphold the highest standards of conduct.

The label was designed to sit within the broader certification landscape and support services to SMEs. The tool aims to provide SMEs with a low-cost solution for assessing and subsequently showcasing their cybersecurity posture, thereby lowering the barriers of SMEs in starting the general process of certification.

The following partners were involved in the design, development and roll-out of the label, as follows:

- SGS: for Label content
- Trust-IT: for technical implementation, hosting and promotion
- AEI: for sustainability through CyberDIH and future promotion

An MoU was signed between Trust-IT (as cyberwatching.eu partner) and SGS to establish a working partnership and a sub-contract was agreed with SGS for the input into the initial design phase, content definition and creation for the actual texts questionnaire which makes up the content of the label. It also included activities on testing and promotion of the label.

The approach of this Cyberwatching.eu service is SME-oriented, with the intent to make certification more democratic and widespread, bringing companies, especially SMEs, closer to cybersecurity certification standards.

The tool has been organised as a simple online questionnaire in which SMEs can be evaluated according to 8 domains which are the starting points of the general process of certification:

1. Requirements for the Software
2. Requirements for the Protocols
3. Requirements for Services
4. Hardware requirements
5. Requirements for Infrastructure
6. Security policy and associated regulations
7. Requirements for External Providers
8. Requirements for "Critical Business Products

According to the scoring of each domain the tool presents SMEs with an observation of the areas in which they are lacking and need improvement.

The tool aims to provide SMEs with a low-cost solution for assessing and subsequently showcasing their cybersecurity posture, thereby lowering the barriers of SMEs in starting the general process of certification.

The tool is an online resource for SMEs sustained by collaboration between AEI (the platform for promotion), Trust-IT (the technical implementation and maintenance) and

SGS (the label assessor and provider) and will continue beyond the lifetime of the project. Trust-IT is responsible for the co-design and technical implementation of the online tool. SGS provides the workflow process for applicants while AEI promotes the cybersecurity label to their network and members.

7.2 Implementation

As highlighted in D5.4 “Sustainability Strategy Final version”, the label was designed to sit within the broader certification landscape and support services to SMEs. The tool aims to provide SMEs with a low-cost solution for assessing and subsequently showcasing their cybersecurity posture, thereby lowering the barriers of SMEs in starting the general process of certification.

The implementation of the Cybersecurity Label was based on the following steps:

- Design phase –October 2020 - January 2021
- Development –February - May 2021
- Testing phase - June 2021
- Launch – July 2021
- Roll out – July 2021

During the Design phase several calls were held mainly between Trust-It, SGS and AEI to agree on the following steps:

- Scope and purpose of the tool
- Technology, roles of partners and user workflow
- Content of the tool
- Pricing

Similarly to the other tools developed by Cyberwatching.eu, the Cybersecurity Label has been designed as a simple online questionnaire in which SMEs can be evaluated according to 8 domains which are the starting points of the general process of certification.

1. Requirements for the Software
2. Requirements for the Protocols
3. Requirements for Services
4. Hardware requirements
5. Requirements for Infrastructure
6. Security policy and associated regulations
7. Requirements for External Providers
8. Requirements for "Critical Business Products

All questions for each section are provided in Annex 1. Relevant parts of key standards such as ISO 27001, 22301 and the NIST directive have been used to shape the questions.

The questions have been designed by building upon the experience of SGS and are meant to be easy to understand, yet fully covering all the aspects an SMEs needs to take into account. Each question is associated with a simple Boolean scoring which in the end reflects the posture of the organization.

According to the scoring of each domain the tool presents SMEs with an observation of the areas in which they are lacking and need improvement. This is reflected in a downloadable report that SMEs can download after completing the tool.

On the other hand, the total scoring of each domain is taken into account for the release of the actual Label based on a 71% threshold of correct answers, so that only SMEs exceeding the threshold can download the actual Label in addition to the overall report.

The tool is directly accessible from the home page of www.cyberwatching.eu where a dedicated landing page is explaining its purpose and the benefits for organisations, as given below:

Figure 7-2 Cybersecurity Label landing page

From the landing page, SMEs can request the use of the Label and start their workflow. Regarding the user workflow, this is articulated in different steps:

- SMEs who request to use the Cybersecurity Label need to register an account on www.cyberwatching.eu and provide some basic organisational details.
- An automatic email with the details provided is then sent to AEI who is the partner responsible to check and validate the SMEs data.
- Upon validation, an automatic email is sent back to the SME with a secured link to proceed to the payment of 150-euro fee trough PayPal or credit card.
- Once the payment is received, the SME can complete the questionnaire and download the report.

The questionnaire is organised in 111 questions divided into 8 domains and subdomains. SMEs can navigate through the 8 domains and have the possibility to save a draft of their submission and come back to it at any time before the final submission to be evaluated.

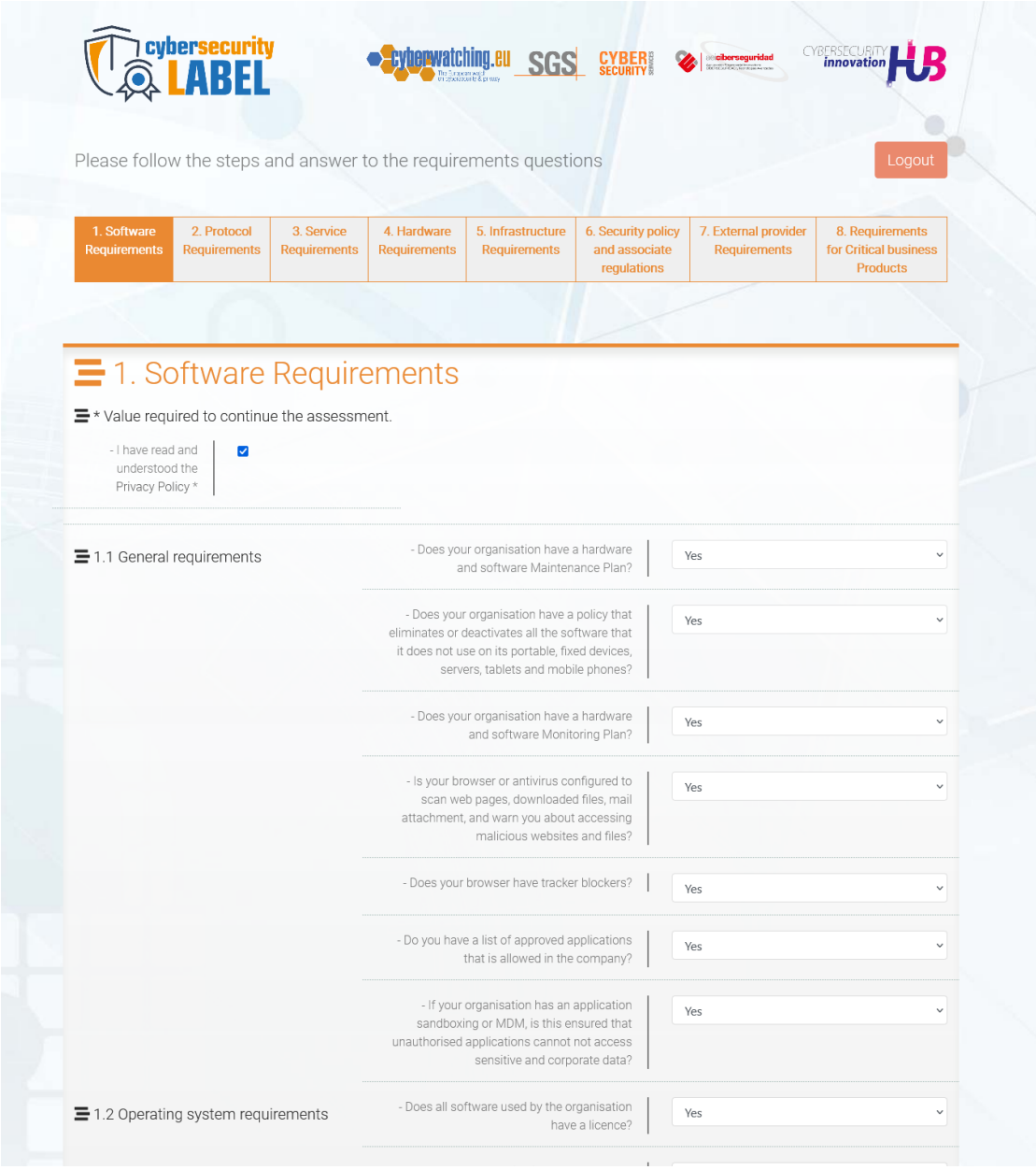

Figure 7-3 Example of Cybersecurity Label questionnaire

Once completed, the tool reports an overall evaluation of the posture of the SMEs, together with a breakdown indication of the scoring in each domain so that SMEs can see at a glance the areas where they need to improve. The report can be downloaded in PDF format.

As described above, if the evaluation exceeds the 71% threshold, the actual Cybersecurity Label is issued and can be downloaded in PDF format.

Figure 7-4: Example of Cybersecurity Label report

The certification mark used during the awarding of the Label is managed by AEI.

When an organization displays this mark, it attests that it has successfully passed the self-assessment above the threshold established for it and that it is registered by AEI in the corresponding business registry.

Only organizations registered by the AEI are authorized to use the Label Mark. The use of this Mark is subject to the following conditions:

1. The Brand must be reproduced respecting the proportions of the image, using the logo shown with the established colours and fonts.
2. Carrying out the self-evaluation questionnaire is voluntary, but in the event of awarding the Label (and the certification mark associated with it), compliance with the rules indicated in this section is mandatory.
3. The certification mark and its logo must, at all times, be associated with the name of the organization that has obtained it. Under no circumstances should the certification mark or Logo be used in a way that could mislead any interested party in the organization.

Before the official launch, the Label was tested internally by Trust-IT, SGS, AEI and DSME who highlighted bugs and improvements for the user experience.

As described in D5.4 “Sustainability Strategy Final version”, the Label will be a key asset for the Cyberwatching.eu sustainability plan. Partners involved in the Cybersecurity Label sustainability strategy will be SGS, AEI and Trust-IT.

SGS and AEI will promote the tool as part of the Spanish Cybersecurity Innovation Hub – Cyberdih with dedicated campaigns, marketing effort and ensuring that follow up activities will be carried out with SMEs using the tool. Trust-IT will cover the role of technical partner, taking care of the hosting of the tool and managing technical issues.

7.3 Results

With the label being launched in July, usage statistics will not be included in this report but rather in the final activity report of Cyberwatching.eu (Deliverable D1.4).

7.4 Promotion and Sustainability Plan

The label was promoted at a number of events prior to its launch in order to already disseminate the result in particular to both the policy-related and SME communities.

The full launch took place at the final cyberwatching.eu Concertation meeting where a keynote presentation was provided which highlighted the main benefits of the label not only to the SME community but also to the cybersecurity ecosystem, placing it within the broader value chain of certification.

Event	Date	Target stakeholders
Cybersecurity: Use and usefulness of labels for SMEs	29 April 2021	SMEs
Developing SME cybersecurity resilience	5 May 2021	SMEs, policy makers & EU Projects
FIWARE Cybersecurity day	13 May 2021	SMEs & policy makers
How to reactively defend against advanced cyber threats	20 May 2021	EU Projects
Shaping the future of cybersecurity – 4th Concertation meeting	13 July 2021	SMEs, policy makers & EU Projects

Table 7-1: Promotion of Light Cybersecurity Label

A highlight of the last Concertation Event of Cyberwatching.eu project was the launch of the Light Cybersecurity Label. The Label was presented by Lucio González Jiménez, SGS in a presentation entitled “***The Cybersecurity label powered by Cyberwatching.eu – A lightweight path to better cybersecurity for SMEs***”. The presentation slides are attached as Annex A.

A press release was released and published on the day of the launch as well as a series of social media posts which gained until now 3.600 impressions. A dedicated newsletter promoting the Label was also sent to an audience of 1113 users, gaining a 19% open rate and 1.4% click rate.

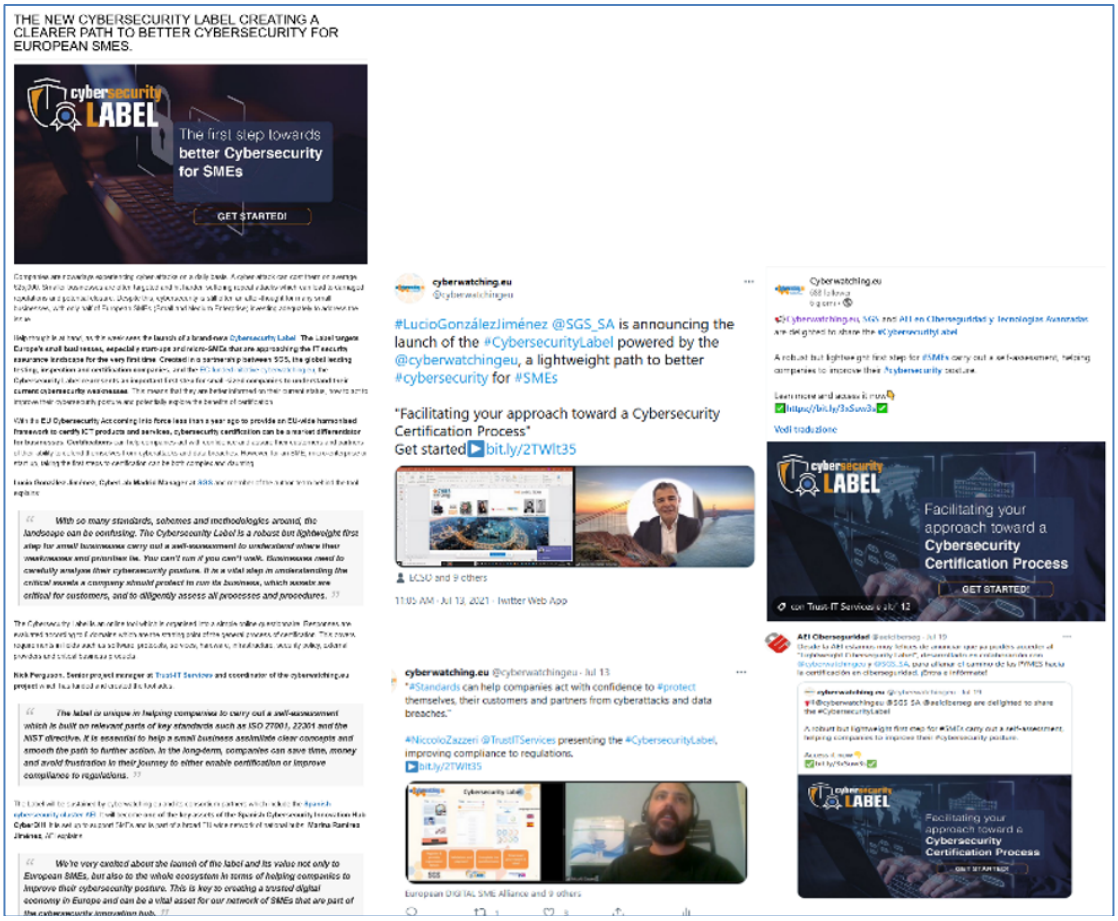

Figure 7-5: Examples of promotional campaign for Cybersecurity Label

A communication package was created for all partners to share through their networks and involving also the Cybersecurity Clusters with whom Cyberwatching.eu had engaged the most, namely ClujIT, CyberWales, Hague Security Delta and GAIA.

A visual banner has been created and used on the current Cyberwatching.eu homepage to promote the tool in the dedicated section about resources for SMEs. The visibility of the Label will be increased in the new version of the Cyberwatching.eu homepage which is currently under structural and graphical revamp as depicted in the Figure below and detailed in D4.9 “Final Communication & Stakeholders Engagement Report”.

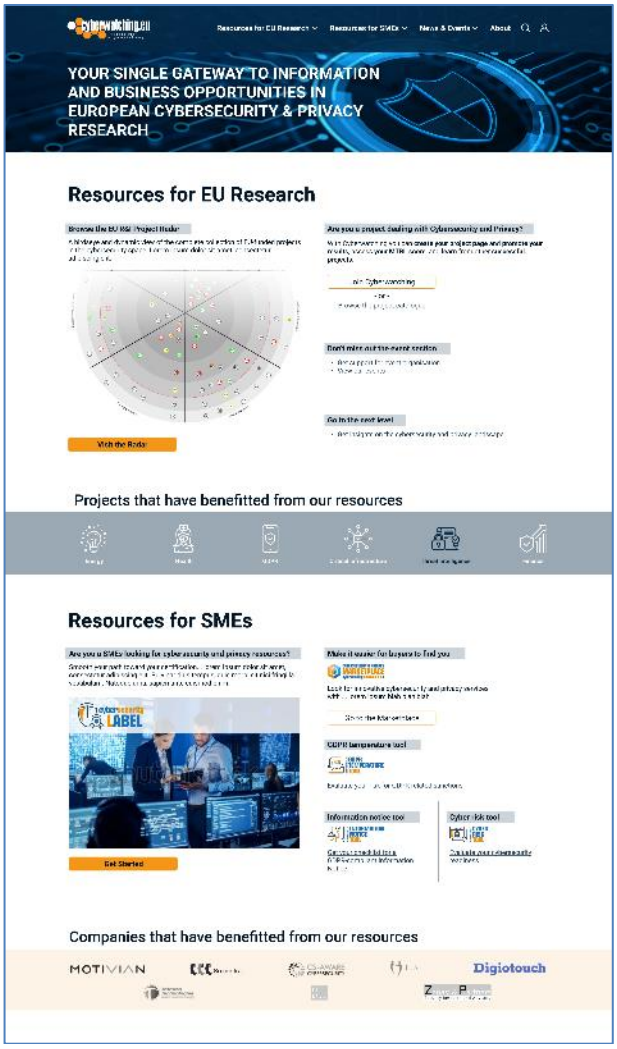

Figure 7-6: Mockup of the new Cyberwatching.eu homepage

AEI will sustain the label beyond the project, as part of the services offered by the Cybersecurity Innovation Hub (Cyber DIH)[31], the European Digital Innovation Hub (EDIH) candidate to be part of the European Network of EDIH[32].

The Cyber DIH is a digital ecosystem around cybersecurity and advanced technologies, which has INCIBE (National Institute of Cybersecurity) as a reference centre and has been promoted by the Regional Government of Castilla y León and the AEI (national cybersecurity cluster), to bring the benefits of digitalization to companies, and help them accelerate their adoption of digital technologies, especially designed to improve an industry 4.0.

The Label will be part of the resources for SMEs and public entities to help them in their digital transformation processes. Within these services, four tools developed in the framework of the Cyberwatching.eu project will be offered, i.e.:

- the GDPR Temperature Tool,
- the Information Notice Tool,
- the Cyber Risk Tool and
- the Cybersecurity Label.

[31] https://www.cyberdih.com/en/
[32] https://digital-strategy.ec.europa.eu/en/activities/edihs

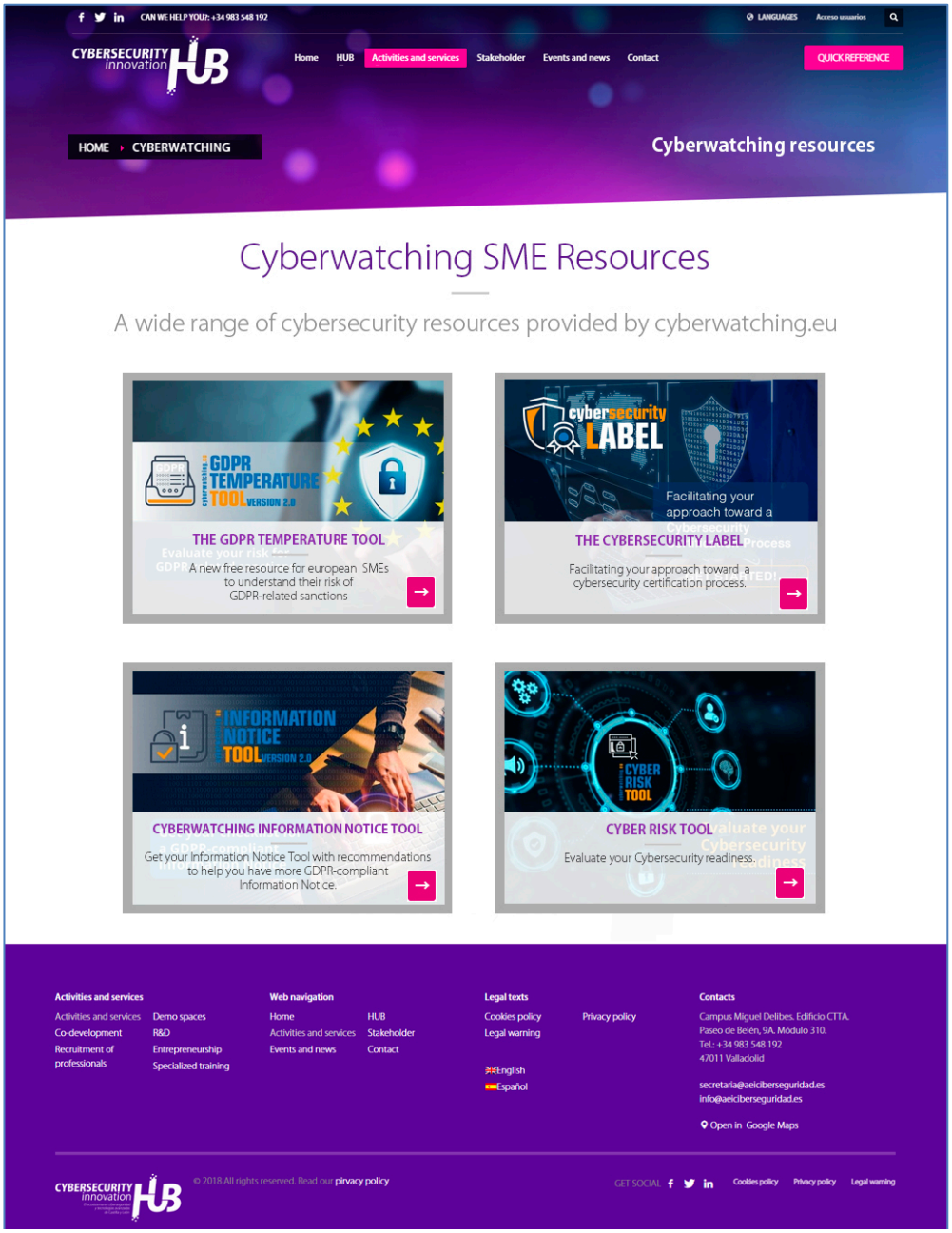

Figure 7-7: Cyberwatching.eu suite of services offered to the public

The afore-mentioned four services will be part of the services designed to be part of the proposal for the EDIH call (expected by September 2021). All these services have operational and maintenance costs, therefore including these services (and their costs) as part of the proposal, in the event that the Cyber DIH is designated as an EDIH, enables the costs to be 50% funded by the EC. But EDIHs are subject to comply with KPIs, that will be yearly verified by the EC, so there is a need to count on a communication plan for the provided services.

The four tools can be seen as first steps for other services within the EDIH, even they can be seen as previous interactions before acquiring any other commercial service offered by the different stakeholders in the EDIH.

The overall communication plan for the Cyber DIH is under definition, but here are some of the main channels for communications actions to promote the Cyber DIH and their services:

- Cyber DIH website as main entry point
- cyberwatching.eu website
- cyberwatching.eu newsletter, Cyber DIH newsletter and AEI newsletter
- Email campaign to cyberwatching community
- Email campaign to Cyber DIH & AEI, INCIBE and Regional Government of Castilla y León database
- Distribution to external media channels
- Press releases

The Social media channels of Cyber DIH -AEI, INCIBE and Regional Government of Castilla y León- & cyberwathing.eu) have widely disseminated the Light Cybersecurity Label. A set of communication actions are also under definition:

- AEI will promote the label through the engaged clusters: ClujIT, GAIA, CyberWales, The HSD, ITSecurity, DigitaSME France, Italian Digital SME Alliance.
- AEI will promote the label within the network of regional clusters of different sectors (10 clusters in Castilla y León region).
- As a member of CONETIC (a national confederation of ICT associations), AEI will also promote the label through this network.
- Direct promotion for AEI members in the annual general assembly.
- Get a commitment from Board of Directors of AEI to promote the label within their networks.
- Sign agreements with other clusters and assess the possibility of a reduction in the label fee for members coming from those clusters.
- Joint promotional actions together with INCIBE and the Regional Government.
- AEI will promote the label through other EDIH candidates that are signing MoUs with AEI.
- Promotion to other EDIHs through the Digital Transformation Accelerator (a figure that will build, grow and support the network).

8 Conclusions & Recommendations

Certification is the key to engendering trust and generating understanding in reliability when purchasing digital products and services. The EU is already working on a common certification framework to assess that digital products and services that have been certified in accordance to a defined scheme to meet the specified requirements. But the security certification processes for digital products and services are usually complex, long and expensive, something difficult to afford for an SME with limited financial and human resources.

User trust is key in the adoption of key new technologies such as IoT and AI etc. without which there could be significant resistance. As such having meaningful cybersecurity badging, that displays technologies having passed stringent testing frameworks will be required. As such research into the quality of a number of existing and competing frameworks has shown variable quality, adoption and understanding as clear barriers to uptake up until now. Ensuring that providers of these marks are independent of both providers and consumer organisation will in the longer term though boost their popularity and therefore see them as desirable by technology or solutions providers and a requirement by the consumer before they are willing to let them for example enter their home.

The EU Cybersecurity Act is a major step forward towards the creation of a single European market for cybersecurity products and services. However, despite the rising concerns about information security risks, the lack of adoption of cybersecurity solutions is yet a real risk for Europe, especially considering that 99% of businesses in the EU are small businesses, which suffer the high complexity and lack of adaptation of schemes, standards and certification to their needs.

The cybersecurity labels/seals recently launched are a very positive step forward. The work we have done in cyberwatching.eu is addressing this by providing awareness raising activities online resources for SME or micro-enterprise that need to approach cybersecurity from the start. This is especially true for the recently launched Cybersecurity Label which is helping SMEs wanting to start a certification process by helping them with practical and low-cost guidance on where to start, before starting a typical process involving reaching out to a Consulting firm to implement standards or technical specifications. By collaborating with SGS, the Label is based on a self-assessment questionnaire that has been designed following the standards of quality of a certifying entity with more than 140 years of experience.

With the key synergy with Spanish Cybersecurity Innovation Hub – CyberDIH as a sustainability effort, cyberwathing.eu will ensure that SME assimilates clear concepts, smoothing the path to further action and ensuring that SMEs understand the landscape they are working in and the key elements that are addressed by the Cybersercurity act.

8.1.1 Recommendations from Cyberwatching.eu results

The following recommendations are gathered from cyberwatching.eu deliverables and summarise the main priorities that cyberwatching.eu has identified regarding standardization and certification since the project started in 2017.

D2.8 “Recommendations report on R&I needs“ – July 2021
R1. Give value to the results of projects already developed, not only forcing to incorporate a section on previous initiatives in the Horizon Europe proposals, but

also promoting among organisations the different tools that allow consulting and taking advantage of the results of previous projects, such as the Cyberwatching.eu Project Radar[33], the Horizon Results Platform[34] or the Horizon Result Booster[35].
R2. Promote clustering activities as a way to encourage collaboration between projects, joint dissemination and exchange of good exploitation practices, including the possibility of joint exploitation or joint future developments.
R3. Encourage projects to do intermediate self-evaluations, beyond the mandatory reviews with the EC, to check that their project is progressing correctly at the technological and market level. The self-assessment should be done by the same person in the project.
R8. Development of certification schemes and standards should be encouraged.

Other **recommendations from the projects**, collected during the clustering activities.

- Make GDPR compliance easier for small enterprises (Start-ups and SMEs), that usually do not have the strength or the knowledge to understand what they shall do to be compliant.
- Foster and coordinate standardization efforts towards new generation of cyber-security systems, which leverage the collaboration between providers of digital services and infrastructures.
- Promote the adoption of certification schemes and award those providers that give visibility of security features in their products.
- More standardisation and common frameworks are needed to be adopted on IoT applications which are dispersed “silos” so far, and even more on Security / Cyberthreat common standards. EC could support with joint efforts on a common/standardised framework adopted by all “big players.
- Improve the investment in continuous human resource training to facilitate the uptake of innovative solutions.

D3.3 “White Paper on cybersecurity standard gap analysis – October 2018

Recommendations in brief

1. The issues of **Mutual Recognition** and **Harmonisation** must be addressed due to the national nature of many standards and certification systems.
2. Further efforts must be made in order to raise awareness concerning the available **accepted standards and certification**, as well as the certification process in case of multi-party composition of products and solutions.
3. EC funding should be targeted toward **Raising Awareness and Education in Cybersecurity Standards and Certification** for both the Public and Private sectors.
4. **International Cooperation** is an area for opportunities to benchmark best practices and standards that may already exist as a way to not “reinvent the wheel”, however, caution is urged in taking care not to immediately co-opt existing standards that may put European industry at a disadvantage.
5. The **cost issue for SMEs** looking toward standards and cybersecurity certification must be addressed. SMEs must be able to access standards and the related certification without breaking the bank. **Self-assessment** and other **low-cost solutions** must be explored.
6. The R&I community should look address the fast-evolving area of **Internet of Things (IoT)** with respect to cybersecurity standards and certification.

[33] Cyberwatching.eu Radar: https://radar.cyberwatching.eu/radar
[34] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-results-platform
[35] https://www.horizonresultsbooster.eu/

7. Elaborate a **common research agenda** across EU Member States (MS). Through the vehicle of the ERC, open specific calls for projects in the area of cybersecurity with clear aims and requirements in developing in areas of relevance to standards in cybersecurity.

D3.6 "Report on Concertation Activities" – July 2021

Recommendations from Concertation Event Session "Priorities, trends and clustering in the R&I landscape" (Deliverable D3.6):
 	
Main takeaways:
• Digital sovereignty and autonomy needs to be achieved in Europe. The landscape is very active in this respect with the launch of the Joint Cybersecurity Unit, the EU Competence Centre, and the Cybersecurity Act
• Similarly, these are key themes of the HE and DE. Both build on past activities and it is imperative that proposals should look into results, reuse them and build upon them.
• Proposals should use the Live EU Project radar to see how they can maximise and build on results:
  ○ Funding on HE topics + related statistics
  ○ MTRL scores to understand the state of the art
  ○ Identify results and cite them

Recommendations from Concertation Event Session "Standards and certification of a trusted Digital Europe" Main takeaways: • International standards should be (re-)used as much as possible for cybersecurity certification: EU intervention here is key. • Mapping of standards (and de-facto standards) by ECSO and Concordia are important. However, the standards are in specific areas and don't cover the complex landscape. New standards and systematic effort is needed and a common taxonomy for SMEs • Standards experts should use EC services and resources such as StandICT.eu[36] to contribute to standardization process and contribute to the EC's Open Consultation on Cybersecurity standards. • New solutions and new funding through HE to further address emerging technologies and CS and privacy challenges - Security and privacy by design are essential concepts • Clear guidelines or practical tools on data protection for design for emerging technologies like blockchain are required. Cooperation and coordinated approach are needed appropriate methodologies for privacy by design to be implemented.

Cybersecurity certification has been identified as a key requirement for trust and with all of the efforts undertaken, Cyberwatching.eu is actually fulfilling a key need with the Light Cyber Security Label, given the context and the efforts being undertaken within other projects, within the standards development organisations and within associations such as AEI and ECSO. We look forward to the future where more SME-friendly solutions can be made available, while at the same time our Light Seal provides a significant benefit for SMEs in the cybersecurity ecosystem.

[36] https://www.standict.eu/

Annex A. **ANNEXES**

A.1. PRESENTATION SLIDES - Roberto Cascella, ECSO, presenting "ECSO WG 1 Standardisation, certification and supply chain management" available here[37]

A.2. PRESENTATION SLIDES - George Sharkov, European *DIGITAL SME Alliance & SBS, presenting "Supporting European participation in the standardisation process" available here*[38]

A.3. PRESENTATION SLIDES - Chatzopoulou Argyro, TÜV TRUST IT GmbH, presenting "Linking Standardisation and Certification - Plans for the future" available here[39]

37 https://www.cyberwatching.eu/sites/default/files/ECSO%20WG%201%20Standardisation%2C%20certification%20and%20supply%20chain%20management.pdf

38 https://www.cyberwatching.eu/sites/default/files/Supporting%20European%20participation%20in%20the%20standardisation%20process%20.pdf

39 https://www.cyberwatching.eu/sites/default/files/Linking%20Standardisation%20and%20Certification%20-%20Plans%20for%20the%20future.pdf

Annex B. **GLOSSARY**

Term	Explanation
AI	Artificial Intelligence
CAPE	Continuous Assessment in Polymorphous Environments
CEN	Comité Européen de Normalisation
CENELEC	European Committee for Electrotechnical Standardization
certMILS	Compositional security certification for medium- to high-assurance COTS-based systems in environments with emerging threats"
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
Cyber DIH	Cybersecurity Innovation Hub
CyberSec4Europe	Cyber Security for Europe
CyberSure	CYBER Security InSURancE — A Framework for Liability Based Trust"
DEP	Digital Europe Programme
EAP	Extensible Authentication Protocol
ECCC	European Cybersecurity Competence Centre and Network
ECCG	European Cybersecurity Certification Group
ECHO	European network of Cybersecurity centres and competence Hub for innovation and Operations
ECSO	European Cyber Security Organisation
EDIH	European Digital Innovation Hub
ETSI	European Telecommunications Standards Institution
ENISA	European Agency for Network and Information Security
EU-SEC	The European Security Certification Framework
FutureTrust	Future Trust Services for Trustworthy Global Transactions
GDPR	General Data Protection Regulation
KRAKEN	BroKeRage and MArKet platform for pErsoNal data
LCL	Lightweight Cybersecurity Label
MoU	Memorandum Of Understanding
MTRL	Market & Technology Readiness Level
NIST	National Institute of Standards and Technology
OCGN	Traditional Organised Crime and the Internet: The changing organization of illegal gambling networks"

Term	Explanation
PANACEA	Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for dAta and people
PHOENIX	Electrical Power System's Shield against complex incidents and extensive cyber and privacy attacks
PRIVACY FLAG	Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployments
R&I	Research and Innovation
SAPPAN	Sharing and Automation for Privacy Preserving Attack Neutralization
SECREDAS	Cyber Security for Cross Domain Reliable Dependable Automated Systems
SME	Small and Medium Enterprise
SMESEC	Protecting Small and Medium-sized Enterprises digital technology through an innovative cyber-SECurity framework
SGS	Société Générale de Surveillance
SPARTA	Strategic programs for advanced research and technology in Europe
SPHINX	A Universal Cyber Security Toolkit for Health-Care Industry
VESSEDIA	Verification Engineering of Safety and Security Critical Dynamic Industrial Applications
VISION	Visual Privacy Management in User Centric Open Environments