Cyber Security for Europe

D4.1

Requirements Analysis from Vertical Stakeholders

Document Identification	
Due date	31 July 2019
Submission date	31 July 2019
Revision	14.0 (30 April 2020)

Related WP	WP4	Dissemination Level	Public
Lead Participant	UPS-IRIT	Lead Author	Afonso Ferreira
Contributing Beneficiaries	FORTH, KAU, UMA	Related Deliverables	D4.2, D5.1

Abstract:
This deliverable reports on the initial findings and recommendations from Task 4.1 – *Vertical stakeholders engagement and consultation*. This task focuses on engaging all CyberSec4Europe vertical stakeholders (end users and industrial participants) so as to collect their requirements, to help them define their important problems and to lay the foundation for the roadmap. Through a diverse set of approaches that include targeted questionnaires, one-on-one interviews, and common brainstorming workshops, this task collects feedback (i) on the important problems that stakeholders face and (ii) on realistic approaches to deal with them. The consultation and engagement have been extensive, so as to ensure that all of the key issues are being identified. This task also provides feedback to Task 3.1 for the methodology definition on research topics.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

This document describes requirements, as identified by the stakeholders of CyberSec4Europe, for the seven vertical areas that have been defined in the project: Open Banking, Supply Chain, Privacy-preserving Identity Management, Security Incident Reporting, Maritime Cybersecurity, Medical Data Exchange, and Smart Cities. The findings and recommendations are based on the works of Task 4.1, which focuses on engaging the vertical stakeholders of the project, so as to collect their needs, the problems they face, and the challenges they will be forced to meet in the near future. A combination of methods was used for eliciting the requirements from the stakeholders, and receiving their feedback on important cybersecurity problems and approaches needed to deal with them for their respective economic sectors. These methods comprised online questionnaires, structured interviews, a number of brainstorming workshops, and desk research. The conclusions of our analyses, presented in this document, show that the stakeholders envision resilient systems, infrastructures, and societies as their common objective. It emerges from this task that their needs will only be fulfilled by an environment that wisely encompasses regulation, incentives, structural reorganisations, and capacity building, along with research and deployment of new technologies, as detailed in the text.

Document information

Contributors

Name	Partner
Mahdi Akil	KAU
Cristina Alcaraz	UMA
Pierre-Henri Cros	UPS-IRIT
Afonso Ferreira	UPS-IRIT
Simone Fischer-Hübner	KAU
Carmen Fernandez-Gago	UMA
Hans Hedbom	KAU
Lejla Islami	KAU
Javier Lopez	UMA
Evangelos Markathos	FORTH

Reviewers

Name	Partner
Cristina Alcaraz	UMA
Marco Angelini	ENG
Pierre-Henri Cros	UPS-IRIT
Afonso Ferreira	UPS-IRIT
Simone Fischer-Huebner	KAU
Carmen Gago	UMA
Javier Lopez	UMA
Evangelos Markathos	FORTH
Victoria Menezes Miller	CONCEPT
Mark Miller	CONCEPT

History

0.01	29/05/2019	Afonso Ferreira	ToC on Template
0.1	06/2019	All partners	Started writing all sections
1.0	19/06/2019	All partners	Sections 3.x completed in draft
2.0	24/06/2019	All partners	Sections 2 and 4 completed in draft
3.0	26/06/2019	All partners	Sections 3.x revised
4.0	27/06/2019	IRIT	Annex ready
5.0	28/06/2019	All partners	Sections 2 and 4 revised. Sections 1 and 5 ready
6.0	30/06/2019	Afonso Ferreira	Abstract, Executive Summary, Tables, and Lists ready
7.0	10/07/2019	UMA	Final revision on selected parts of the document
8.0	12/07/2019	KAU	Final revision on selected parts of the document
9.0	29/07/2019	FORTH	Final revision on selected parts of the document
10.0	30/07/2019	Afonso Ferreira	Final revision of whole document
11.0	27/03/2020	All partners	First round of revision from review completed
12.0	03/04/2020	All partners	Cross-reading completed
13.0	07/04/2020	Afonso Ferreira	Second round of revision from review completed
14.0	08/04/2020	Afonso Ferreira	Final document revised from review
14.0	30/04/20	Ahad Niknia	Final check and prepare to submit

List of Contents

List of Figures

List of Acronyms

ABC	Attribute-Based Credentials
ACPR	Prudential Control and Resolution Authority
AISP	Account Information Service Providers
API	Application Program Interfaces
ASPSP	Account Service Payment Service Providers
CEO	Chief Executive Officer
CERT	Cyber Emergency Response Team
CII	Critical Information Infrastructure
CPS	Cyber Physical Systems
CTAP	Client-to-Authenticator Protocol 2
DAWEX	A company partner of the project
DG CONNECT	Directorate-General for Communications Networks, Content and Technology
DG MARE	Directorate-General for Maritime Affairs and Fisheries
DG MOVE	Directorate-General for Mobility and Transport
DLT	Distributed Ledger Technology
EEA	European Economic Area
EHR	Electronic Health Record
EMSA	European Maritime Safety Agency
ENISA	European Network and Information Security Agency
FHIR	Fast Healthcare Interoperability Resources
FIDO	Fast IDentity Online Alliance
FORTH	The Foundation for Research and Technology - Hellas
GDPR	General Data Protection Regulation
IBAN	International Bank Account Number
ICS	Industrial Control Systems
ICT	Information and Communication Technologies
IDM	Identity Management

IDS	Intrusion Detection Systems
IMO	International Maritime Organization
IRIT	Institut de Recherches en Informatique de Toulouse
ISAC	Information Sharing and Analysis Centre
ISO	International Organization for Standardization
KAU	Karlstad University
KYC	Know Your Customer
LPA	Local Public Administration
MISP	Malware Information Sharing Platform
NATO	North-Atlantic Treaty Organisation
NGO	Non-Governmental Organisation
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
PET	Privacy Enhancing Technologies
PISP	Payment Initiation Service Providers
PKI	Public Key Infrastructures
PLC	Programmable Logic Controllers
PSD2	Payment Services Directive 2
RTU	Remote Terminal Units
SIEM	Security Information and Event Management
SIQS	Self-Initializing Quadratic Sieve
SME	Small and Medium Entreprise
TLP	Traffic Light Protocol
UMA	University of Malaga
UPS	University Paul Sabatier
USA	United States of America

1 Introduction

This document describes stakeholders' requirements for the seven vertical areas that have been defined in the CyberSec4Europe project, namely:

- Open Banking
- Supply Chain
- Privacy-preserving Identity Management
- Security Incident Reporting
- Maritime Cybersecurity
- Medical Data Exchange
- Smart Cities

For each one of the above areas, Task 4.1 focuses on a process that engages the vertical stakeholders, so as (i) to collect their requirements, (ii) to help them define their important problems and (iii) to lay the foundation for the roadmap to be designed within related tasks in WP4. Therefore, this process collected the stakeholders' **needs**, the **problems** they face, and the **challenges** they will be forced to meet in the near future.

This work in Task T4.1 differs from the work in Work Package WP5, which focuses on a well-defined case study (or demonstrator) for each Vertical area, while WP4 in general (and task T4.1 in particular) takes a holistic view of each vertical area, in order to build a Research and Innovation roadmap for both the mid- and long-term. Accordingly, the main lines of enquiry were as follows.

- What are the requirements of each vertical area?
- What are the important problems in each vertical area?
- Are there realistic approaches to deal with these problems?

To collect the information in a structured way, the following main activities were performed:

1. Anonymous surveys were collected from both the project participants and the broader community
2. Targeted interviews with specific stakeholders were conducted
3. Several face-to-face co-design workshops (i.e. physical meetings) with selected stakeholders (including end users) were held

VERTICAL AREAS

OPEN BANKING

SUPPLY CHAIN

PRIVACY-PRESERVING IDENTITY MANAGEMENT

SECURITY INCIDENT REPORTING

MARITIME CYBERSECURITY

MEDICAL DATA EXCHANGE

SMART CITIES

4. Desktop-research was conducted to enrich the input data
5. A final face-to-face workshop in the presence of stakeholders, where the collected inputs were consolidated.

This deliverable presents the results of this significant effort. At this point it should be noted that the intended goal of this task was not to collect all the possible requirements from all possible stakeholders. Such an exercise would require a tremendous amount of effort and would be beyond the scope of this pilot project. On the contrary, this deliverable is the result of a focused exercise in highlighting the needs of the ecosystem presented by the project partners and their constituencies. In this dimension, the results will be useful because (i) they highlight the requirements of the community in the area of cybersecurity and privacy, and (ii) they show the way toward realistic approaches for possible solutions. Furthermore, in the framework of different tasks in WP2, WP3, WP4, and WP5, the stakeholders will have the opportunity to provide additional feedback during the course of the project, because this is a "living approach" to looking at these issues.

1.1 Structure of the Document

The rest of this document is organized as follows. Section 2 presents the methodology that was followed. Section 3 presents a detailed analysis of the information that was collected from the stakeholders and end users, Section 4 presents the commonalities that were found in all verticals' requirements, and Section 5 presents the main conclusions.

2 Methodology

A combination of methods has been pursued for eliciting the stakeholder's requirements, and receiving their feedback on important Cyber Security problems and approaches needed to deal with them for their respective areas of expertise. These methods comprised (i) online questionnaires, (ii) structured interviews and (iii) a brainstorming workshop, as presented below. The methods were chosen to conduct qualitative and explorative research allowing to analyse the problem space and requirements for solutions in more depth, rather than simply deriving statistical figures. This approach was complemented by desk research, where and when needed.

2.1 Online Questionnaire

An online survey questionnaire was designed in cooperation with WP2. Participants were asked about overall cybersecurity goals for Europe, key cybersecurity conditions that need to change, key capabilities and technologies that are required to achieve a change. For this, free-text fields allowed participants to fill in text of varying lengths. The instrument of an online questionnaire was chosen to reach a large number of vertical experts, who could not all be interviewed due to the inherent time and availability restrictions.

The survey questionnaire was designed to collect exploratory information. In order to meet the survey's objectives, a small number of preliminary interviews with target respondents have been arranged to clarify ideas about what information would be required in the survey.

The partners involved in the survey implementation discussed the questions wording before pre-testing the questionnaire. Open questions were chosen instead of closed questions, because the respondents were asked to give a reply to a question in their own words, revealing the issues that are most important.

The questionnaire was worded to encourage respondents to provide accurate and complete information. For example, respondents were allowed to choose "other" as an option among the choices that were provided and to specify this choice. For designing the survey, a set of survey tools was tested in collaboration with WP2, and the possibility of using SurveyGizmo and CyberConnector (a collaborative environment proposed by a project partner) was analysed. It was then decided to move to the EU Survey tool because it is GDPR compliant and it has the added value of coming from an EU domain.

The survey completion time was taken into consideration when deciding on the number of questions, trying to balance the survey goals with the total number of questions asked. Once the survey was implemented, it was tested before sharing the link with the stakeholders[1].

The survey was first distributed to all project partners via the CyberSec4Europe mailing lists to all project and pilot partners. It was then sent to the coordinators of the other three pilots, for distribution among their own set of partners. The recipients were requested to forward this questionnaire within their ecosystems. Thus, it was then distributed further via a “snowballing” effect.

The online survey was hosted by the EUSurvey platform[2] of the EU Commission during April and May 2019. For collecting the survey replies, informed consent was obtained from the participants in compliance with the GDPR (General Data Protection Directive). In total, 57 answers for the survey were collected until the end of May.

The questionnaires answers were not evenly distributed across all application areas of interest. We therefore tried to conduct interviews especially with stakeholders from the vertical application areas of expertise, for which we received a low number of survey responses to compensate that lack of distribution.

2.2 Structured Interviews

Interviews were chosen as an instrument to obtain more detailed and qualitative data, which allowed to receive more detailed explanations and deeper insights into Cyber Security problems and challenges.

It was decided to conduct a structured interview with six concrete questions, which resulted in the interviewers asking each participant exactly the same list of questions in the exact same order. The first question Q1 had the purpose to collect demographic data in a form allowing to easily anonymise the results to be published and to clearly identify the application area for which the answers will apply. Questions Q2 to Q5 directly match the Task 4.1 description to collect their requirements (Q2), to help them define their important problems (Q3) and to lay the foundation for the roadmap (Q4 in terms of capabilities, Q5 in terms

[1] The survey was pre-tested by KAU (feedback on 4.04.2019), TUD (feedback on 4.04.2019), FBK (Third party of UNITN in the light of sending it to EIT Digital partners) and external participants (feedback organised by UPS-IRIT).
[2] https://ec.europa.eu/eusurvey/

of technologies). For keeping interviews short and focussed, the questions were restricted to this set. The instrument of structured interviews allowed us to gather consistent and comparable data and to reduce biases that could potentially be introduced by the different interviewers that were involved. Moreover, structured interviews were faster to execute and evaluate than unstructured or semi-structured interviews, which also motivated our choice.

The scope of the interviews was the same as the survey questions. Both focused on the different verticals to describe (1) three cybersecurity requirements that the vertical will need to meet in the future, (2) up to three cybersecurity-related capabilities that need to be developed, (3) what technologies need to be developed or deployed.

In total, 42 interviews were conducted by the WP 4.1 partners from May until the beginning of June 2019. The distribution of expertise of the interviewees was as follows (where the number in brackets provides the number of interviewees that indicated expertise for that specific area): Open Banking Security (5), Supply chain Security (7), Privacy-preserving Identity Management (10), Security Incident Reporting (11), Medical Data Exchange (8), Maritime Cybersecurity (4), Smart Cities (14) and 3 had general Cyber Security expertise. As it can be noted, several of the interviewees indicated more than one area of expertise.

The interviewees were recruited via personal contact networks of the partners and received an invitation letter explaining the objectives and set up of the interviews together with an informed consent form to be signed (see Annex). The interview set-up was positively reviewed and approved by one of the Ethical Advisors at Karlstad University. According to the Swedish Ethical Review Act, no further ethical review by the national research board was required, as no sensitive data (i.e., no special categories of data) were collected and there were no other ethical issues apparent either. The interviewees were specifically instructed not to provide any information in their answers, which could include any sensitive personal information.

Two types of interviews were implemented: (i) asynchronous and (ii) synchronous ones. In asynchronous interviews, the interview form was sent to the experts who filled it in and send it back along with their consent form.

Synchronous interviews were conducted in person or on the phone and took on average 20-30 minutes, as follows. The interviewer participated in the interview, usually together with one or two assisting researchers. All of them took notes. If the interviewees consented, the interview was voice recorded, which allowed to later go back to the interview session recordings for comparing or verifying the notes with them. In a first round, all participating researchers were writing down the main responses and key finding from the interviews based on their notes and after cross-checking with the audio recordings in separate documents. Some of the interviewees also provided written answers before the interview, which were then complemented based on the notes and audio recordings. In a second round, the interviewers combined all results and findings for a specific application area (vertical) from all note takers and all interviews into one document. Proposed corrections, revisions and interpretations in the second round were discussed among the team of interviewer and assistants and cross-checked with the audio recordings in a third round.

Requirements and key findings were elicited not only based on the interview notes and audio- recordings, but the survey answers were assigned to the respective application area and were also considered for eliciting

requirements and findings. An analysis was conducted jointly in discussions or meetings by the team of interviewer and assisting researchers that all attended the interviews.

The notes were then summarized in terms of key findings (see Annex).

2.3 Brainstorming workshops

Several brainstorming sessions were also organised as part of this task, in order to elicit input from local stakeholders. In order to prepare the ground for the future hub of community expertise to be piloted by CyberSec4Europe, it was decided to hold such workshops in Toulouse. Three such workshops were organised, as follows. On April 4, 2019, at the Ocssimore association (the association incubating the hub), with 11 participants present. On May 16, 2019, at the Ocssimore association, with 9 participants present. On June 6, 2019, at the UPS-IRIT partner, with 21 participants present.

The latter was a one-day brainstorming workshop, to which all WP4 partners representing all verticals were invited (and not only T4.1 participants), along with several members of the local ecosystem[3]. At this workshop, all the results from the interviews and the survey were summarized by Task 4.1 partners and then discussed with the participants. These discussions provided further relevant references and complementing information for filling gaps of relevant problems and approaches that need to be considered as well for the roadmap. In particular, the presence of the other WP4 partners allowed for a good understanding of how the current deliverable would best serve the tasks related to the WP4 roadmapping that is going to be crafted in the remainder of the project. The agenda of this brainstorming workshop is included in the Annex.

These three brainstorming workshops established an increased sense of awareness of stakeholders about the importance of defining their requirements related to the verticals. Consequently, they enhanced the practical technical content of such requirements, with real-world use-cases. In addition, the collaborative work done for the definition of the needs of the verticals during the workshops contributed to the establishment of a community in quest of finding solutions. This has immensely benefitted the structuring of the aforementioned hub of community expertise in Toulouse, that is being developed in WP2.

The overall results of the survey, interviews and the workshops were finally analysed and summarised by the task partners. They are presented in the following section.

3 The end-users' perspective

CyberSecurity4Europe is a pilot for a Cybersecurity Competence Network that will address a considerable set of issues in the cybersecurity domain. In order to test these cybersecurity challenges, several demonstration cases have been selected within the vertical sectors of digital infrastructure, finance, government, smart cities, health and medicine and maritime transportation. The goal is to define these

[3] Organisations that were present included AD'OCC, ATOS, BSC, CNRS, Continental, Cyblex Technologies, Engineering, FORTH, IBP, iBP-BPCE, IMS Networks, IRIT, IUT Blagnac, Karlstad University, Lyra Network, NEC Laboratories Europe GmbH, Orange CyberDefense , Silicom, Trust in Digital Life, Universidad de Murcia (UMU), University of Malaga, University of Piraeus Research Center, UPS.

demonstration cases in these specific verticals or sectors in such a way that they identify the common research and technologies developed in WP3.

Once the verticals chosen, the needs and challenges for them were elaborated by taking into consideration the opinions and views of the main stakeholders involved in each of the verticals. This analysis will lead to a detailed roadmap for CyberSec4Europe, taking into account the specific requirements of each vertical. This is the main objective of WP4 and of this deliverable. Thus, in this section the basis for the development of a common research and innovation roadmap will be set up. This will enable an innovative and multidisciplinary research on cybersecurity with the aim of reducing fragmentation in the different research communities addressing cybersecurity research within Europe.

In order to elaborate the basis for the roadmap, the methodology described in Section 2, above, was followed. This section summarizes the recommendations elicited from the stakeholders and synthetizes them in terms of challenges, requirements, technologies, and other measures to be addressed. In order to identify these key findings, the results of the online survey and of the interviews have been analysed as follows.

The responses provided for the online survey and at the interviews were collected and synthesised by project partners, and then presented and thoroughly discussed at the brainstorming workshop in June 2019. At the end of this process the responses were divided according to the vertical identified by each respondent and, for each vertical, the responses were examined to extract the key changes and capabilities that the respondents had recommended.

The recommended key changes and capabilities were then included below, in the relevant sub-section of this section, describing the corresponding vertical. Priority was given to changes and capabilities that were clearly in scope of this deliverable and had support from different respondents. Items whose support stemmed from several verticals were finally included in the next section, further below, which outlines common challenges, common requirements, and common technologies.

Accordingly, in the remainder of this section, for each vertical, a short summary of the requirements for the vertical, as described in D5.1, is included. This is then followed by the description of the identified challenges, the capabilities that are thought to be needed in order to overcome the challenges, what are the envisaged technologies that are thought to enable the capacities that are needed, and a few accompanying measures that would support the verticals alongside the envisaged technologies.

3.1 Open Banking

The Payment Services Directive 2 (PSD2)[4] has applied since the 12th of January 2016 and EU countries have had to implement it in national law by the 13th of January 2018. In short, it enables bank customers, both consumers and businesses, to use third-party providers to manage their finances. In the near future,

[4] https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366

consumers may be using Facebook[5] or Google[6] to pay their bills, making peer-to-peer transfers and analyse their spending, while still having their money safely placed in their current bank account. Banks, however, are obligated to provide these third-party providers access to their customers' accounts through open APIs (Application Program Interfaces). This will enable third-parties to build financial services on top of banks' data and infrastructure.

Consequently, banks will no longer only be competing against banks, but against everyone offering financial services. PSD2 will fundamentally change the payments value chain, what business models are profitable, and customer expectations. Through the directive, the European Commission aims to improve innovation, reinforce consumer protection and improve the security of internet payments and account access within the EU and EEA (European Economic Area).[7]

PSD2 introduces the following two new payment services provided by new actors.

- **Payment Initiation Service Providers (PISPs)[8]** will initiate online payments to third parties on behalf of the payers. These entities, which do not necessarily have a relationship with the payers' banks and are called Account Service Payment Service Providers (ASPSPs), shall access to the online account of the payers. P2P transfer and bill payment are PISP services likely to be seen when PSD2 is implemented.
- **Account Information Service Providers (AISPs)[9]** are able to give users a consolidated view of all their payment accounts even if they are managed by multiple ASPSPs.

In addition, PSD2 poses substantial economic challenges for the banking sector. In particular, IT costs are expected to increase due to new security requirements and the opening of APIs. Customers are entitled to a high level of security in mobile banking, but the new actors raise new security issues. For example, a bank customer may give a PISP full access to their online bank accounts to initiate payments. If so, the provider would also have access to all the bank information associated with the user. Since no formal relationship with the ASPSP is required, it makes the protection of customers complicated for the banks. In addition, in this example AISPs would have access to all incoming and outgoing payments in order to provide a consolidated view of the customer's bank accounts. As a consequence, AISPs will gain access to sensitive information data such as rent and salary or insurance and health insurance payments. The task of the banks to protect the privacy of their customers becomes much more complicated in such a situation. Finally, it would be very difficult for users to understand what is happening to their data, where it is being saved and what their rights are. Nor it is clear with whom the responsibility would lie in the case of any data loss.

3.1.1 Summary of findings and recommendations from D5.1

The demonstration case described in D5.1 investigates four different scenarios:

[5] Facebook.com
[6] Google.com
[7] https://www.evry.com/en/news/articles/psd2-the-directive-that-will-change-banking-as-we-know-it/
[8] See https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366
[9] Idem

- Privacy Preserving Verifiable Credentials
- An Open Banking Sensitive Data Sharing Network
- An Open Banking API Architecture
- Improving Financial Settlements

Each one of these addresses security concerns that have arisen as a result of the highly disruptive digital transformation in banking and financial services, from both the coming into force of new regulations as well as the introduction of new technologies. It could be said that Open Banking is just about data, and all that matters is how you use it. In particular, while the GDPR is intended to protect citizens' data, PSD2 is designed to remove the barriers to accessing bank information and the treasure trove of sensitive financial data contained therein. The four use cases reflect in one way or another the concerns arising from the emerging landscape of financial services about protecting access to and the potential loss of sensitive financial data.

Deliverable D5.1 describes the requirements for the CyberSec4Europe demonstration case entitled Open Banking. It first provides a high-level overview of the demonstration case and its goals, followed by a description of the actors involved. It then provides more detailed functional requirements featuring use cases, followed by a description of non-functional requirements. It also reports relevant constraints and assumptions to be considered while implementing the demonstration case. Finally, it discusses essential components for an adequate governance of the exposed services and the functional characteristics that could support the evolution towards Open Banking for open financial services.

In particular, a shared map of the macro-components and functionalities for the Open API was developed in D5.1. The map, which is reproduced below for the sake of completeness, is designed as a model to support API exposure with a view to openness. It is mentioned here, because it represents a useful starting point for moving towards future scenarios, but, as stressed in D5.1, it must be understood as a necessary but not sufficient condition for Open Banking, since the technological, infrastructural and architectural adaptation must in any case be accompanied by a broader rethinking of the organizational aspects, governance paradigms and business logic support models.

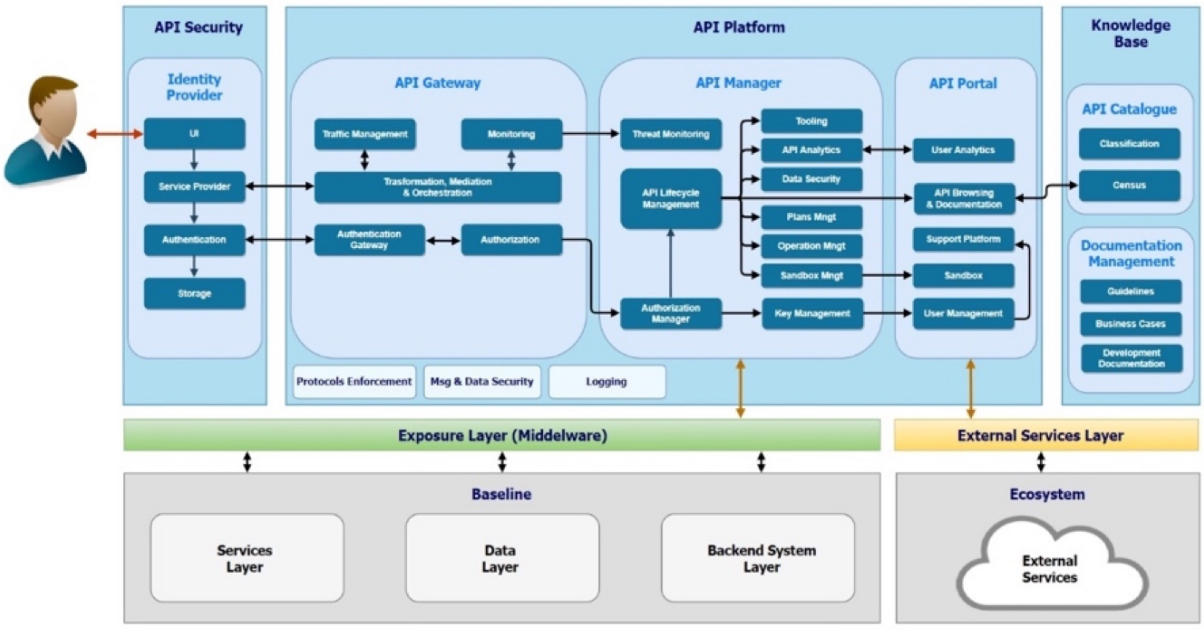


Figure 1: Map of the macro-components and functionalities for the Open API

3.1.2 Important problems and challenges for the mid- and long-term

The presence of the banking sector as a major business vertical in the Cybersec4Europe project is justified by three critical issues that today require both a significant change in the practice of security and the construction of technological innovations in this area.

- Firstly, threats are increasingly professional and repeatable. For example, between 2015 and 2016, the number of phishing sites targeting the Banques Populaires in France increased by a factor of 21[10]. In 2019, such attacks, particularly leveraging human weaknesses (users, customers, employees, and collaborators at partners and service providers), continue to succeed, as the degree of completion of these false communications is ever higher. Notably, the attacks demonstrate the allocation of high skills and large resources, against which any company is not prepared to fight alone. In addition, the industrialisation effort on the side of the attackers', in order to offer complete "starter kits" targeting any bank, allow the malicious actors to quickly reuse their modus operandi, from one bank to another, without significant effort and without being tracked.
- Secondly, the evolution of consumer banking toward ever more real time transactions will limit the ability of banking players to efficiently react in the event of proven fraud. Today, the co-creation and co-design of an "Open Security" approach federating the whole banking ecosystem, to make it globally aware and informed of any fraud attack in real time, is therefore a necessity.
- Thirdly, banking information systems architectures have been deeply remodelled, now focusing on APIs as critical business components. This revolution was fuelled by the establishment of the supremacy of mobile devices as the preferred interface to consume banking services and is accelerated by the PSD2 regulation, that aims to generate a great innovation dynamic benefiting the

[10] Source: Partner iBP

banking industry and the security of its services. If it is true that the design and the development of business APIs is now mature, thanks to the standards widely adopted by the developers' community, it is also verified that the "API-sation" of a banking information system creates organisational and methodological impacts that go beyond pure software development, introducing new security issues. For example, the development of the business applications consuming these APIs can now be externalized to innovative third parties, with benefits for "time to market" and banking innovation, but also resulting in an increased attack surface. Therefore, these new issues require a complete transformation in the provision of business services.

These three critical issues point to the following main challenges faced in the mid- and long-term:

- Fostering the adoption of a global vision of API system security that is both multi-stakeholder and multi-organization.
- Designing solutions to effectively detect fraudulent consumptions of an API, in a perspective in which core banking players no longer control the developed business applications, their use-cases, or the design of their internal security.

An additional significant problem is that the banking industry, like any other, must (re)position itself in the age of the data economy. Against a backdrop where banks have demonstrated their ability to be a trusted third party on their perimeter, namely the financial data of their customers, the GDPR creates opportunities to develop strategies for the fair use of personal data. To grasp such opportunities, however, the existence of a mechanism of user identification/authentication is fundamental. Such a mechanism, which is not necessarily restricted to historical banking services, should enable the development of new use-cases around the exchange of personal data, by working with other industries that also hold personal data (health, e-commerce, transport, ...).

The challenge is then three-fold, as follows:

- Innovating on new use-cases with high added value for the end-user.
- Innovating in the confidentiality of exchanges, because this would encourage wide adoption by end-users and maintain the value of personal data in the long term.
- Giving the users total control over the uses that will be made of their data, by producing identity management that is self-governing and allows individuals to own and manage their digital identity.

3.1.3 Requirements in capabilities

The following is a first list of fundamental capabilities that are needed in view of addressing the challenges described above.

- **A strong ecosystem of exchange of critical information** between Open Banking actors for the fight against bank fraud:
  - Exchanges need to be anonymised to encourage the widespread adoption of the sharing practice
  - Exchanged data must be desensitised, without compromising their business value

- New business models and partnerships allowing to create services that strengthen the trust in online transactions on the basis of such exchanges.
- Community datasets that can better train Artificial Intelligence systems to detect fraud and threat, exploiting such exchanges.

- The establishment of a **maturity model of business security** associated to the “API-sation" of an information system:
  - A methodological framework for the secure development of APIs whose efficiency is proven by practical experience.
  - The consumption of APIs by a large and uncontrolled customer ecosystem must be controlled.
  - Good practices that effectively address the issues of governance of APIs security within a company need to be shared.

- **A transversal digital identity platform for banking players**, and more broadly for all industries processing personal data of their customers/users, focused on the end-user:
  - Exchange protocols that guarantee the confidentiality of the data exchanged.
  - An architecture that respects by design the privacy of end-users and that gives them full control over their data and data usage.
  - Governance processes of the ecosystem of data providers (enrolment, trust, revocation, ...).
  - A self-sufficient ecosystem to implement, along with fully aware end-users, highly valued business use-cases.
  - New business models and partnerships.

3.1.4 Technologies sought

Several new technologies can contribute to establishing the capabilities described above. The following is a first list that should be researched already in the framework of Cybersec4Europe, but preferably more broadly.

- Concerning the need for the exchange and sharing of critical information in the fight against fraud:
  - Techniques for **desensitization of critical data** that are more efficient than current hash techniques.
  - Exchange algorithms that guarantee **anonymity**, e.g. Diffie-Hellman-like.
  - **Hybrid encryption technologies** that mix traditional encryption and post-quantum encryption and are specified for the banking sector.
  - **Community exchange platforms** such as a Malware Information Sharing Platform (MISP), that could ensure support in adequacy with real time requests.
  - **Hybrid decision systems** that effectively combine both business rules and machine learning, in order to detect and react in real time.

- Regarding the security of the API-sation of information systems:
  - **A governance framework** for security of systems based on business APIs.
  - **Artificial intelligence** systems able to profile API consumers in order to identify and fight against fraudulent consumptions, and to improve the experience of legitimate users

— **Smart decision-making systems** that continuously adapt security policies according to the observed APIs' consumptions.

- Regarding the digital identity platform:
  — **Protocols based on web standards**, such as FIDO CTAP2 and W3C's Web Authentication and Verifiable Credentials[11], and on trusted intermediaries (blockchain, Public Key Infrastructures – PKIs, ...), that guarantee the confidentiality, quality, and integrity of the data exchanged.
  — **Zero-knowledge-proof algorithms** and other tools that are adapted to a personal information exchange without transfer of the underlying data
  — Technologies able to secure the process of enrolment of an end-user / data provider.
  — Security technologies meant to create user experiences that encourage end-user adoption and trust.

3.1.5 Further measures

The following are the most salient non-technological measures that would need action in order to promote cybersecurity in the Open Banking environment.

- Adoption of an agreement from the competent authorities (one example being France's ACPR[12]) to allow the exchange of sensitive information (IBAN[13], KYC[14], ...) between banking actors for fraud concerns.
- European-wide communication campaigns (advertisement campaigns, organisation of dedicated events, production of good practices guides, etc.) to encourage end-users to modify their behaviour in the field of personal data management.
- Explore the definition and subsequent certification of the concept of sectorial cybersecurity expertise. This is a technical expertise in cybersecurity (pentesting, secure development, security architecture ...) associated with an expertise of its application in a particular economic sector (banking, transport, health etc.).
- European-led efforts aiming to homologate, at the level of the governance of the Web, the extensions/integration of standard protocols (ex: FIDO CTAP2 and W3C's Web Authentication and Verifiable Credentials) that will be proposed by the research community, as described above.
- Foster the definition of business models allowing to fairly share the added value produced by proposed innovations, facilitating the federation of all the expected partners.

[11] The Web Authentication (also known as WebAuthn) specification is hosted at W3C (World Wide Web Consortium) while the Client-to-Authenticator Protocol 2 (CTAP2) specification is hosted at the FIDO (Fast IDentity Online) Alliance.

[12] Prudential Control and Resolution Authority
[13] International Bank Account Number.
[14] Know your customer (KYC) is the process of a business verifying the identity of its clients and assessing their suitability, along with the potential risks of illegal intentions towards the business relationship. The term is also used to refer to the bank regulations and anti-money laundering regulations which govern these activities.

3.2 Supply Chain Security Assurance

The Supply Chain is nowadays considered one of the most extended and oldest verticals, which has gone through four different industrial generations[15,16,17], as can also be noted in Figure 2 and described as follows:

- ***1st Industrial Revolution***. This first generation began in the latter half of the 18th century with the mechanization starting mainly in the textile industry. Throughout this generation, traditional artisans were replaced by workers who manufactured products with the assistance of water or steam powered machinery as indicated in Figure 2. This industrial advance extended into other critical areas such as transportation and communication.
- ***2nd Industrial Revolution***. It started at the end of the 19th century and the beginning of the 20th century. This industrial generation was characterized by (i) the enormous technological deployment (e.g., electrification), (ii) the advances in the organization and management during the manufacturing processes, and (iii) the mass production (e.g., through assembly lines and interchangeable parts). To increase the productivity, Taylor's "Principles of Scientific Management" were applied to modern shop-floor practices in the context of a manufacturing organization[18].
- ***3rd Industrial Revolution*** - also known as the Digital Revolution. This generation started in the latter half of the 20th century, in which ICT (Information and Communications Technology) technologies and the "Internet" were adapted to the environment to improve the production processes (in terms of quality and reliability) and the speed up their delivery. This technological change introduced the need for the manufacturing, automation with robots, Remote Terminal Units (RTUs) or Programmable Logic Controllers (PLCs).
- ***4th Industrial Revolution*** - also known as the Industry 4.0[19], and currently in transition process and under way. It aims to digitalize all manufacturing processes to optimize the well use of resources and improve the production and distribution processes, allowing end-users (customers) to interact in the process and customize their own products or services.

  The idea behind this is to try to converge the new IT (information technologies) into the existing OT (operational technologies), allowing to create connected and complex IT-OT environments. In

[15] Waidner, M., & Kasper, M. (2016). Security in industrie 4.0 - challenges and solutions for the fourth industrial revolution. *2016 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 1303–1308. https://doi.org/10.3850/9783981537079

[16] Chen, B., Wan, J., Shu, L., Li, P., Mukherjee, M., & Yin, B. (2017). Smart Factory of Industry 4.0: Key Technologies, Application Case, and Challenges. *IEEE Access*, *6*, 6505–6519. https://doi.org/10.1109/ACCESS.2017.2783682.

[17] ENISA. (2018). *Good Practices for Security of Internet of Things in the context of Smart Manufacturing*. https://doi.org/10.2824/851384.

[18] J. Prince Vijai, G.S.R. Somayaji, R.J.R. Swamy, Padmanabha Aital, (2017) "Relevance of F.W. Taylor's principles to modern shop-floor practices: A benchmarking work study", Benchmarking: An International Journal, Vol. 24 Issue: 2, pp.445-466, https://doi.org/10.1108/BIJ-02-2015-0019.

[19] George Paes, The Significance of Industry 4.0 to Manufacturing History, Technology, and Business Transformation, Optessa, https://www.optessa.com/blog/industry-4-0-history-technology-business-transformation/, Sept 2018, last access in June 2019.

this sense, emerging technologies, such as Cyber Physical Systems (CPS), Industrial Internet of Things (IIoT), Artificial Intelligence, Big Data, Analytics or Cloud/Fog/Edge Computing or virtualization have already been considered as reference technologies to be largely integrated in the different sections of the value chain.

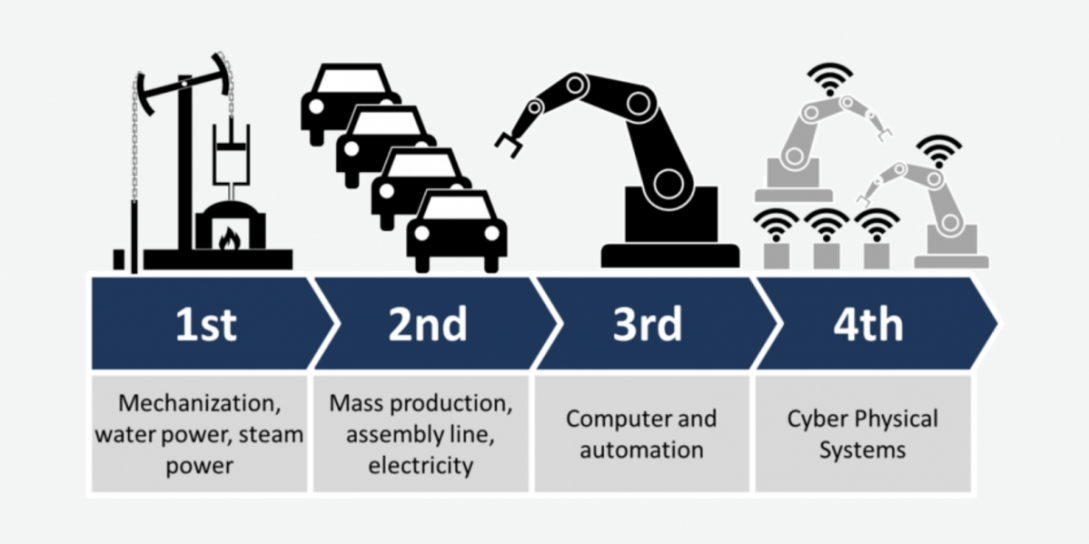


Figure 2: Transition through the four Industrial Revolution Generations

Both this document and the rest of documents to be prepared in this project will mainly be focused on the fourth industrial revolution in order to study the impact of the new technologies within the sector, the benefits that they could foster, and the multiple security problems that they bring in the future.

3.2.1 Summary of findings and recommendations from D5.1

Supply Chain Security Assurance corresponds to one of the use cases included in D5.1. The proposal of this use case is to provide a secure blueprint for generic supply chain solutions, permitting integral digitalization and optimization of all the processes and transactions involved in the value chain. With this, customized services, significant production costs and trusted participation of new stakeholders (such as end consumers, suppliers, manufactures, government agencies, providers, etc.) are expected to arise in this new industrial context, in which a set of technologies must also be part of the process to create advanced and collaborative manufacturing ecosystems. In this case, information technologies (IT) adapt to the existing operational infrastructures (operational technologies – OT) not only to incur to complex IT-OT-based network infrastructures, but also to add functional capacities to audit and establish accountability measures. For this reason, the demonstrator will work under a distributed ledger technology (DLT).

Indeed, the rapid emergence and adaptation of the new information technologies and the multiple interactions of parts, may root unforeseen or drastic risks in the new IT-OT domains, that may consequently lead changes in the final service/product. Moreover, due to the (inter)-dependencies entre infrastructures, any conflict in the operational processes may also affect the quality of critical services of other critical infrastructures, such as power grid systems. The optimal construction and disposal of critical elements

validated through large testing processes and auditing, are therefore fundamental to make sure the safety-critical of other critical infrastructures.

Given this, the demonstrator, defined in D5.1 and related to the Supply Chain Security Assurance, aims to contribute to effective control measures to guarantee quality and accountability in the entire value chain; i.e., starting from the suppliers to the end consumer. Through distributed ledgers it is possible to trace movements of parts, components and goods, and verify the compliance of standards and regulatory frameworks. Namely, the idea is to find a way to provide audit and accountability mechanism capable of avoiding possible counterfeit in the transactions, fraud or unforeseen changes or errors. To address all these current challenges, two further main use cases within supply chain security assurance have also been identified in D5.1: A supply chain for retail, and a compliance and accountability in distributed manufacturing system. Both scenarios mainly focus on characterizing and implementing a critical scenario related to the energy sector, and particularly, on the construction of power transformers to efficiently distribute energy to end consumers (see Figure 3).

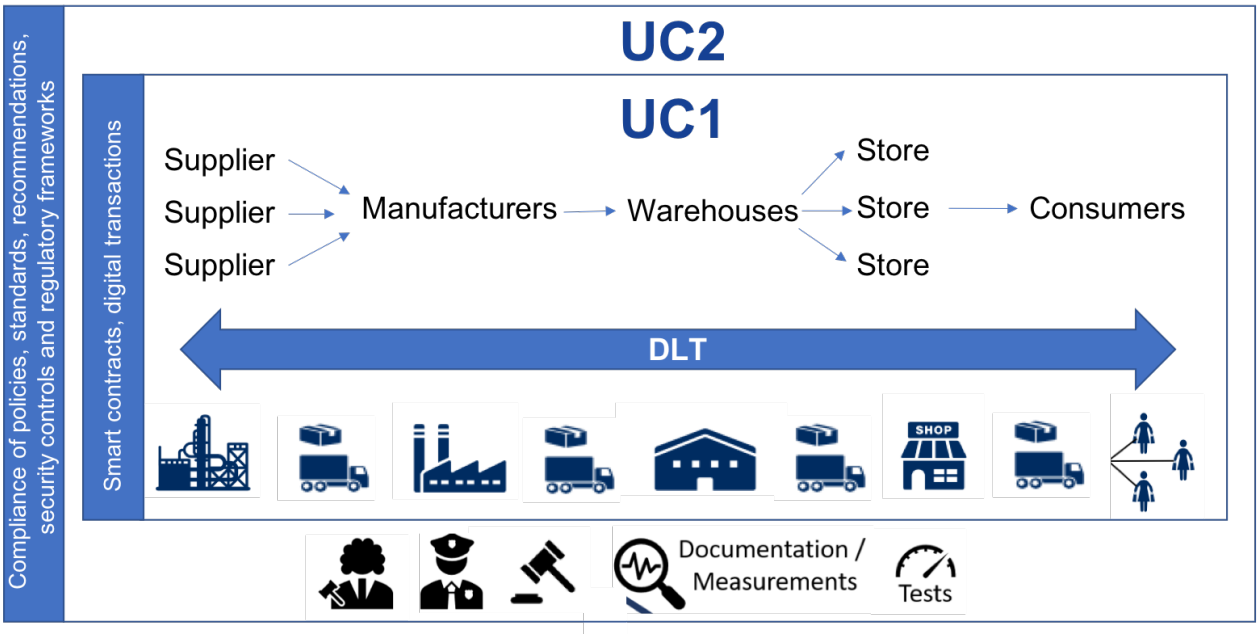


Figure 3: Use cases within supply chain security assurance

Through these specific use cases, a set security and privacy services are considered, covering the following research areas:

- traceability of the operational processes through trustable collaborative environments;
- the protection and access to the private data through the use of a set of minimal security services based on traditional security and privacy mechanisms; and
- the compliance of regulatory frameworks to establish quality in the products/services and accountability in the process. This also means to implement mechanisms related to audit, validation, electronic signatures and testing.

Therefore, this process can also entail to: (i) increase security controls through verified processes, (ii) improve certification processes under regulatory frameworks, standards and authorities, and (iii) prove the validity of the own regulatory frameworks in the value chain.

3.2.2 Important problems and challenges for the mid- and long-term

Supply chain is one of the main business verticals within the Cybersec4Europe project, mainly due to its critical nature in the manufacturing processes and delivery. This aspect was also underlined by vertical stakeholders, which identified several important problems within the sector; all of them described as follows:

- First, there is a special need now to adapt the new technologies (IT-OT) and remodel the manufacturing processes, accepting the inclusion and interaction of new stakeholders such as customers. This fact, however, adds the need to keep the security and safety levels in acceptable states, establishing, for example: resilience mechanisms, regulatory frameworks, exhaustive validation processes, auditing, and accountability.
- Second, the number of threats is becoming more notable, probably due to the use of the new technologies, and the business extension through the Internet. According to the analysis done by the USA's ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) in their last annual report[20], the sector of manufacturing is one of most targeted. In 2013 started to be reported the first incidents, rising to 15% of recorded incidents (38 incidents of 259), 27% in 2014 (65 incidents of 265), 33% in 2015 (97 incidents of 295), 22% in 2016 (63 incidents of 290) and 3% in 2017 (5 incidents of 149) – without being reported the annual document for 2017 yet.

These two critical issues point to the following main challenges faced in the mid- and long-term:

- Establish **dynamic risk assessment** at the supplier side. The number of risks and threats in these new IT-OT environments add new security risks, mainly caused by technological convergence. Thus, suppliers should be selected based on a systematic security evaluation, which is both risk-based and business driven; and in this way, guarantee a major control over their own environment.
- Add **protection at all the levels and authentication**. The new technological trends in the industry and the inclusion of new actors such as customers, force scientists to consider new security challenges to protect devices, their communications and systems. For example, at the hardware level, it is fundamental to protect intelligence and the edge processing of devices ("security hardware"), their connections and messaging control, as well as data storage considering the use of the new technologies (e.g., Cloud). Regarding authentication, the protection of the identity of users and access to the diverse critical devices is also essential. In this case, authentication must be subject to cryptography-based advanced methods to make sure the "encryption" of the access to devices and the protection of identities.
- Propose reliable and dynamic **event management mechanisms, prevention and detection**. The complexity of the new industries – comprising the technological diversity, the multitude of interactions and the diverse stakeholders – do not contribute in the accurate management of events.

[20] Industrial Control Systems Cyber Emergency Response Team, https://ics-cert.us-cert.gov, last access in June 2019.

Any supply chain must be able to dynamically and accurately manage events, and detect and prevent anomalous states in optimal times, e.g., through the implementation of specific and specialized mechanisms such as Security Information and Event Management (SIEM) systems.

- Include **assurance measures through verification and compliance with regulation frameworks**. Supply chain operations are critical by themselves, and they should comply with all the processes and regulations required for their well performance and security.
- Establish **standardization and certification measures**. There are not enough standardization and certification mechanisms in these types of critical infrastructures; and it is still necessary to harmonize approaches toward cybersecurity with cooperation across Europe.
- Make sure **trustworthiness and resilience of operations and services** in acceptable states and at all time. It is essential in a critical infrastructure of this type to ensure that all elements are permanently connected. All elements in the value chain and their connections must be "safe" to preserve the *integrity* of the product or the service, and this procedure can also comprise the need to preserve confidentiality and integrity of industrial data in hostile environments under sophisticated cyber-attacks.
- Keep **operational performance** and establish measures that help control the complexity of the system. The implicit complexities of the new IT-OT environments and the need to incorporate security measures, add new operational challenges related to the "availability". Any approach proposed must be optimized to ensure the availability of processes, resources and data streams when they are demanded.
- Extend **technological and security culture within the supply chain operations**. There exists an especial lack of knowledge and understanding of the well use of both the available technologies and the current policies. Namely, there are not enough security specialists with dual understanding and knowledge of technologies and policies.
- Establish **trust** between suppliers and customers. Suppliers should properly be audited (using, for example, the blockchain technology), and clients should be protected applying diverse control measures. It is necessary to avoid real cases such as the case Wipro – an Indian IT provider was compromised and all of its customers were impacted[21].

Summarising, the challenges in mid- and long-term are the followings:

- Innovation in event management platforms as well as in topics related to prevention and detection, considering all the possible risks in the sector.
- Deployment of protection measures in all the levels (hardware, software, communication, storage) and authentication to protect the access to critical resources.
- Provision of auditing measures and security controls to reduce risks in the customer's side.
- Innovation in resilience measures to keep the operations in high states 24/7 even in anomalous or hostile situations.
- Establishment of regulatory frameworks, standards, validation measures and certification.

[21] KrebsonSecurity. (2019), *Experts: Breach at IT Outsourcing Giant Wipro, Krebs on Security*, https://krebsonsecurity.com/2019/04/experts-breach-at-it-outsourcing-giant-wipro/ , last access in June 2019.

- Training and knowledge of the well use of technological resources (either IT and OT) and policies, further establishing same security awareness criteria and prerequisites in all Europe.

3.2.3 Requirements in capabilities

Supply chain is a complex and critical infrastructure that requires addressing diverse cybersecurity issues. To carry out safe and secure ``Supply Chain´´ operations, several capabilities are still needed. According to the stakeholders and the multiple tools (the workshop, interviews and the survey) established to collect information from them, the most important needed requirements are as follows:

- **Traceability, procurement and accountability**:
  - The idea is to be able to explain the origin of the components and the trust level, the ownership of elements/parts of the supply chain, and the active management of its stakeholders. In this sense, transparency mechanisms in all this operational process therefore becomes key to make sure traceability of actions and states within this context, and establish accountability.
- **Notification and multi-language management**:
  - Aligned with the previous point, it is also essential to provide notification capacities to adequately inform about anomalous events or status, considering the hierarchical structure/organization of all the value chain -- this implicitly entails to understand or manage multiple languages for notification.
- **Governance and assurance**:
  - Apart from applying regulations in safety matter, it is also necessary to (i) consider the gradual/self-adaptive implementation of effective, harmonized and lightweight security metrics, formal methods and controls to avoid exposing the underlying system and its own processes to vulnerabilities; and (ii) be capable of applying policies according to security requirements (i.e., "*that all the products around us, must comply with the security that the manufacturer says they have*"), and designing guidelines for the best practices of the industry.
  - For assurance, it is fundamental to make proofs of penetration testing in devices to discover vulnerabilities, and provide methods and tools that work at the interchangeable format and are feasible across Europe.
- **Standardization and certification:**
  - Enforcement of standardization, certification and homologation tools implies the development and deployment of a framework of standards and certification.
- **Resilience** through recovery measures 24/7, and working in optimal times.
- **Cyber-crisis management**.
- Provide a **suitable hardware upgrade** to accommodate future software components.
- **Post-quantum cryptography** to be prepared to possible changes in the future.
- **Defensive tools**:
  - To manage: (i) availability, integrity and confidentiality of operations, services and data; (ii) secure access; and (iii) unforeseen events or anomalous states as stated in previous section, involves incorporating defensive tools by defect.

- **Security awareness through** education and training:
  - Through interviews, stakeholders have underlined the need to provide more education on security risks and limitations of modern technologies (e.g., accessibility modes). In this case, education must cover all aspect of cybersecurity: governance, offensive measures, defence, operational security, etc., and under a global European awareness program on cybersecurity.
- **European cybersecurity agency**, which must be independent with respect to all national governments.

3.2.4 Technologies sought

The technologies needed to address the challenges above, not surprisingly, fall under the following categories:

- **Distributed Ledger Technology (DLT)** - e.g., blockchain - as also detailed in the use cases of supply chain of the deliverable D5.1 (see Section 3.2.1). Through this technology is possible to provide an auditing and accountability mechanism that allow to establish responsibilities and transparency in the entire value chain.
- **Cryptography** to protect identities and access. For example, homomorphic cryptography could be key to set trust with providers.
- **Strong authentication and authorization systems**.
- Usage of **big data, machine learning and artificial intelligence** techniques and technologies for the extraction of patterns in data and the identification of abnormal behaviours.
- **Internet of Things** applied in the supply chain must be an area where standards and certification have to be further developed.
- **Lightweight formal techniques** for ensuring security. The idea would be to modify the past approaches such as "typed assembly languages" and "proof carrying code". They have been developed so as to overcome some of the difficulties of checking software obtained from other developers.

3.2.5 Further measures

The following are the most salient non-technological measures that would need action in order to promote cybersecurity in the supply chain environment.

- Definition of policies and standards, and/or exploration of the use of existing ones. For example, one of the stakeholders recommended applying: **DO-178C**[22] (Software Considerations in Airborne Systems and Equipment Certification) focused on the software development and lifecycle process. The standard is based on 10 objectives:

[22] RTCA. (2011). *RTCA DO-178: Software Considerations in Airborne Systems and Equipment Certification.* https://standards.globalspec.com/std/1459138/RTCA%20DO-178, last access in June 2019.

- *Software Planning Process*;
- *Software Development Processes*;
- *Verification of Outputs of Software Requirements Process*;
- *Verification of Outputs of Software Design Process*;
- *Verification of Outputs of Software Coding & Integration Processes*;
- *Testing of Outputs of Integration Process*;
- *Verification of Verification Process Results*;
- *Software Configuration Management Process*;
- *Software Quality Assurance Process*;
- *Certification Liaison Process*.

- As stated above, standards and certification mechanisms must be developed when new technologies are being adapted (e.g., IoT). Apart from this, existing technologies (IT-OT) and components belonging to the own value chain (e.g., components, parts or machinery) must also be validated following formal engineering processes for their certification.
- Integrated safety systems with embedded **redundancy** mechanisms.
- Application of **free tools** (i.e., open sources mechanisms).
- Security awareness through large and reliable education and training programs.

3.3 Privacy-Preserving Identity Management

Privacy-Preserving Identity Management systems allow users to manage their personal data while interacting with service providers in a privacy-friendly way. The traditional realization of privacy-preserving identity management relies on the existence of a trusted third party to enable the communication between the interacting entities. Hence, traditional identity management systems do not integrate data minimization principle neither provide usability to end users.

3.3.1 Summary of findings and recommendations from D5.1

In this direction, the privacy-preserving identity management demonstration case has the objective to enable an identity infrastructure to fulfil the need for strong privacy-preserving authentication with a distributed and scalable platform for privacy-preserving self-sovereign identity management, which will be show-cased in the educational sector. The goal is to develop a highly efficient, scalable, and user-friendly identity management solution providing formal security and privacy guarantees to all parties based on state-of-the-art in privacy-preserving cryptography.

The Privacy-Preserving Identity Management demonstrator, introduced in D5.1 aims to provide a blueprint of the security and privacy challenges that hamper the adoption of privacy and usability in the current Identity Management solutions and identify mechanisms relevant to comply with privacy requirements of identity management systems. Namely, the objective is to develop a highly efficient and scalable identity management solution supporting security, privacy and usability guarantees to all parties. For this, the inclusion of (i) security and privacy recommendations, (ii) usability requirements, (iii) legal and regulatory requirements or (iv) operational requirements is paramount. In particular, the following recommendations are identified:

- **Authentication:** Authentication protocols are essential to mutually authenticate the components in any communication.
- **Unlinkability:** This requirement must serve users to decide which specific actions about them should be provable unlinkable to each other.
- **Anonymity**: The identity of the users must not be disclosed. Here pseudonymity is an anonymity with accountability trade-off.
- **Efficiency**: As an essential usability requirement, the deployed solutions should be highly efficient. (In particular, as required by D5.1: "the time needed for the cryptographic operations and necessary communication when receiving or presenting a credential should not exceed 1000ms, even when stored on a commodity smart card").
- **Transparency**: Guaranteeing transparency is important in helping users understand who knows what about them, how their data is being used, or how long it is held.
- **Scalability**: Identity management is a very demanding area in respect to scalability and performance aspects.
- **General Data Protection Regulation,** concerning the protection of personal data must be respected.

3.3.2 Important problems and challenges for the mid- and long-term

In the following sections we summarise the main problems identified from the interviews, the survey, and the CS4E stakeholder workshop regarding the *Privacy-Preserving Identity Management* area:

- The need to construct the Identity Management **(IDM) (in a strong privacy-preserving and easy to use** approach
  - The core challenge is to develop IDM solutions that satisfy all the following requirements at the same time:
    - strong privacy protection & authentication
    - no single point of failure or trust
    - usability, i.e. choice to be privacy-preserving and should be easy to use).
  - Most technologies that already exist satisfy only two out of the three requirements above. For instance, current privacy-preserving IDM solutions developed by the research community, such as Idemix , provide strong privacy, but are too complex, not easy to use, as they require different user actions to obtain and handle credentials, which users will not be able to easily understand and handle.
- Another core requirement would be to simplify privacy-preserving IDMs
  - Avoid trying to fit all the features in the same system. In particular, existing IDM solutions in practice lack strong and end-to-end authentication, which should be the main goal. Examples of good trade-off solutions are Cloudflare, Privacy Pass or ABC (attribute-based credentials) for the cloud (i.e., the approach taken by the CREDENTIAL project), where an intermediary in the cloud run everything on behalf of the user with good-enough privacy guarantees.
- A more general cyber security requirement is the need for **systematic security work**
  - At the supplier side, systematic security work, which is both risks based and business driven, is a key criterion (to have control over your own environment).

- **Bridging the gap between policy & technology**
  - Being capable of breaking down policy documents to actual security requirements, controls, and technical implementation (converting the theory to real world scenarios).
- **Take a step back from the theory and identify practical requirements**
  - While good theoretical solutions have been proposed by the research community, practical solutions addressing real-world needs have to be made available and usable for users. Such solutions should be efficient with good enough privacy guarantees which are simple and understandable.
- The concrete problem of looking for **more distributed privacy-preserving systems**
  - For instance, where trust is distributed in a single sign on;
- A way to **manage strong authentication keys for the end users**
  - Usable key management so that key holders can be securely authenticated;
- The need to **have good implementations**
  - There are many good solutions from research on papers but they have not yet been implemented in practice.
- **Knowledge gap**
  - There are insufficient security specialists available with dual understanding and knowledge of technologies and policies.
- **Lack of criteria for good security architectures**
  - Lack of metrics for security solutions as well as methods on how to achieve them in the first place.
- The need for **better mechanisms to hide and/or manage complexity**
- **Lack of transparency for data subjects**
  - Lack of clear security and privacy strategies in regards to the handling of the data subjects' personal identities.
- **Cross-border unification and interoperability**

3.3.3 Requirements in capabilities

The following cybersecurity-related capabilities need to be developed:

- Raising awareness is key, in particular awareness of non-technical people to understand what the online privacy problems and threats are, what and how everything works. There is the need for education and training in privacy-preserving crypto, which is often counter-intuitive and thus hard to believe and hard to understand by managers or policy makers. Such decision makers need to understand what is possible with "crypto-magic".
- Secure implementations of PET (privacy enhancing technologies) crypto – PET cryptographic systems are mostly designed by mathematicians, but are often not or not well implemented by software developers. In particular, vulnerabilities of devices need to be considered as well.
- Policy interventions are needed – The GDPR is important since it creates demand and interest in PETs and Data Protection by Design. There should be pressure from policy intervention - for example, for today's public transport systems often cheap mobile phone based, privacy-invasive solutions are in use, which allow user tracking, even though practical PETs could be used for enhancing privacy. Policy intervention could in such cases require privacy-preserving identity management solutions.

- Research and decisions in regards to what is a proper implementations of the GDPR is needed.
- There is a need for open-source, which provide PET implementations in good quality and are easy-to-use tools for developers.
- There is a need for addressing security awareness issues by a broad security training and education efforts. Currently, a good security mindset does not exist in all sectors. While for certain areas in the banking sector there is a high level of security awareness, it is much lower in production environments, even though cybersecurity is equally important there.
- It is necessary to introduce educational measures, and means for improving security culture in order to increase trust in IDM technologies.

3.3.4 Technologies sought

The following technologies need to be developed or deployed:

- First of all, adoption of existing cryptographic privacy-enhancing technologies is important. Cloudflare and Privacy Pass solution are good example to use in some other fields. There is an insufficient use of existing technologies rather than a lack of privacy-enhancing solutions.
- Reusable Open Source implementations of PETs and privacy-preserving crypto blocks are needed, which can be easily adopted in current identity management systems.
- Research is needed on taxonomies & architectures for privacy-preserving identity management systems. In particular, for IoT environments with restricted devices, there is a need to develop usable, more decentralized, distributed IDM technologies, where the handling of credentials may be outsourced to a potentially trusted intermediary.
- Distributed, decentralised architectures for privacy preserving IDM need to be developed.
- Usable solutions that can help users to remember and handle cryptographic keys, including secure backup and recovery keys.
- Enabling privacy-preserving, transparent advertising, profiling and analytics is also an important research objective. First, it needs to be analysed which data are really needed to be stored by the service provider and how much linkability is needed in order to give helpful suggestions to customers (e.g., which movie to watch).
- Decentralized authorization mechanisms as well as certification and validation services. Here, blockchain-based solutions, which can also enhance transparency are recommended.

3.3.5 Further measures

- Educational and training programmes for raising security awareness for non-technical people need to be developed.
- Furthermore, there is a need for multidisciplinary projects considering also the economic aspects for achieving economically viable solutions.

3.4 Incident Reporting

The environment of the digital single market and its transformation into a set of highly interconnected systems has led regulators to identify critical areas that require particular attention. Indeed, the analysis of all the actors involved in a cyberattack scenario has of course highlighted the magnitude of its impact but above all has shown that not only does the cyber-risk cross national borders, but also sectoral borders, resulting in potentially dramatic systemic risks. It is therefore important to adopt a holistic vision and promote a collaborative approach in order to improve, in particular, the cyber-resilience of the actors concerned. This requires increased preparation and awareness in the area of cybersecurity.

3.4.1 Summary of findings and recommendations from D5.1

Work Package 5 is demonstrating manners by which incidents can be reported in accordance with the different procedures and methods specified by the relevant regulatory bodies. In D5.1, it is proposed that the demonstrator specifically supports the bidirectional sharing of cybersecurity information to enable a centralized or decentralized approach, i.e. a peer-to-peer approach.

The resulting prototype developed in WP5 will cover (i) the sharing of reliable information, including secure and efficient protocols for information exchange, analysis of large amounts of cybersecurity data and quantitative risk assessment, (ii) the application of machine learning and other AI (Artificial Intelligence) techniques to prevent attacks and threats, but also to assist decision-making and improve incident response, secure and confidential, efficient and possible storage of information, using distributed mechanisms, blockchains and interfaces useful for designing and managing electronic security procedures.

3.4.2 Important problems and challenges for the mid- and long-term

The main problems and challenges identified by the vertical stakeholders are:

- Lack of harmonised procedures
    - The current EU legal framework already provides for the need to comply with the obligation for Incident Reporting to the various supervisory authorities by respecting the relevant impact assessment criteria and thresholds. However, the timetable, all data, and means of communication are defined by each authority at European and national levels. Therefore, the overall incident reporting process is fragmented and must be managed according to the critical path of incident management itself. There is, hence, a crucial need for harmonisation of procedures across Europe.

- Prove the efficiency of AI in cybersecurity events detection and incident responses

— There are currently many solutions based on AI. Most of the time, they are black boxes. Today, there is a growing desire to have access to the algorithms and methods used to better understand how they work.

- Access to the information
  - — Get a European referential of incident typology,
  - — Offer a centralized European CERT (Computer Emergency Response Team), open for all, with open-data APIs (Application Programming Interfaces) at least for TLP (Traffic Light Protocol) “Green” data sharing
  - — Propose a standardised and coordinated cybersecurity communication cooperation that will pave the way towards a public and private collaboration to reach the common goal of an enhanced cyber resilience,
  - — Identify available and adapted tools for enhancing the preparedness of small and medium enterprises to face cybersecurity incidents and respond to them adequately.

- Facilitating the collection of incident and/or data leak
  - — Have a Single-stop shop approach. Today the multiplicity of authorities to whom incidents must be reported appears to weaken the proper collection and dissemination of these reports,
  - — Merge the roles of "information creator" and "information user" to promote a richer exchange of information such as the signing of a virus to qualify it in relation to a profession or reporting the use of an IBAN (International Bank Account Number) in financial fraud.

- Train people to manage security incidents
  - — Understand what constitutes a security incident, and what is not considered a security incident (e.g. spam, etc.).
  - — Identify and correctly react to security incidents.

- Improve the economic model of CERT
  - — Today, the economic model for sharing incident reports is based on a pricing system that is proportional to the wealth of information provided. This restricts the use of a full service to those who can pay for it.
  - — SMEs (Small and Medium Enterprises) should be supported, financially and from an organizational point of view (like a EU grant).

3.4.3 Requirements in capabilities

The main stakeholder's expectations are:

- Harmonisation of procedures
    - Most economic players need standardised and coordinated cooperation in Europe in order to be able to meet their incident reporting obligations in line with the different procedures/methods specified by regulators.
    - Such harmonisation should pave the way for public and private cooperation to achieve a common objective: to improve cyber-resistance in Europe and beyond the EU's borders.

- Trustworthy use cases and data sets
    - This aims at benchmarking AI algorithms to demonstrate how results are performed. This should be based on a reproducible methodology which will help to overcome the lack of clear engineering principles and explanations on how to comply with good practices. The main objective is to provide assurance that the information given is trustworthy.
    - This should also provide assurances explaining which security controls should be implemented and why. This is important because many defence techniques are based on black box machine learning techniques.
    - This should help to identify vulnerabilities at the software architecture level. Current vulnerability assessment tools mainly identify security bugs rather than architectural flaws.

- Develop a training strategy for having
    - Educational background in proper engineering discipline and authority and responsibility for engineers.
    - A generation of professionals who master both the security of systems but also understand how cybersecurity affects the business in many other aspects is much needed.
    - More expertise about: cybersecurity governance, technical specializations about malware analysis and network security.

- Platforms for
    - Testing technologies for Incident Reporting, tools & methodologies for the identification of the impact perimeter of an incident, tools and methods for the quantification of the potential or real impact of an incident to determine the overall severity of the critical event.
    - Defining a common incident taxonomy taking into account all applicable regulatory requirements.

3.4.4 Technologies sought

The technologies expected by this vertical's stakeholders summarize the requirements described above.

Their aim is to develop the coordination, financing and support of efforts to accelerate the emergence of an advanced, innovative, dynamic, and integrated cyber security ecosystem that reaps the benefits of basic and advanced technologies. They should also ensure the dissemination of basic and advanced technologies to all economic sectors, critical and non-critical, and by all stakeholders (from large industries to SMEs, from public authorities to NGOs[23]) so that European cyber defence is strengthened, large European vertical industries are transformed in a secure and resilient way and data are protected in accordance with the GDPR while feeding the data economy.

The technologies sought are as follows.

- Open source platform for incident reporting to share data, use cases and results of AI algorithm benchmarking.
    - Maintained by a European service
    - Accessible to all companies
    - It must be able to provide tools and services to deploy and manage resilient and trustworthy services, without compromising their usability, accessibility and functional properties.
    - Accessible to citizens and companies.

- Open source platform dedicated to GDPR incidents
    - Compared to GDPR Enforcement Tracker site[24] which contains a list and overview of fines and penalties which data protection authorities within the EU have imposed under the EU General Data Protection Regulation, this platform should focus on the types of incidents and the processes to be implemented to avoid and/or overcome them.

[23] Non-Governmental Organization
[24] http://www.enforcementtracker.com/

3.4.5 Further measures

In order to develop and maintain a high level of awareness in cybersecurity in our society, the following is the most important non-technical measure that should be taken according to our stakeholders:

- All the economic consequences of cyber incidents suffered by industries, services, administrations, and citizens, which would have been identified during the week in Europe should be collected and disseminated to CERT subscribers and to general news organisations.

3.5 Maritime Transport

The Maritime transport vertical is a representative example of a collaborative and complicated process that involves domestic and international transportation, communications and information technology, warehouse management, order and inventory control, materials handling and import/export facilitation, among others.

The maritime transport services include various interactions and tasks among the various entities engaged (stakeholders and actors) having different goals and requirements. In particular it includes a number of interactions and tasks that involve several physical (docking of the ship, stevedoring, loading, unloading, storage, transportation, inspection, etc) and cyber (pre-arrival notifications, customs clearance documentation management, declarations to the International Ship and Port Facility Security, etc) operations, interconnections, and assets.

3.5.1 Summary of findings and recommendations from D5.1

Obviously, the maritime ecosystem is characterized by significant (inter)dependencies among the involved actors. Thus, one needs to treat internal, external and diffused cyberthreats for the entire maritime ecosystem. In this context, D5.1 identified the need to contribute to the effective protection of the maritime transport that arises from the interconnections and interdependencies of a set of maritime entities, such as port authorities, ministries, maritime companies, ship industry, customs agencies, and maritime/ insurance companies, with other transport critical information infrastructures (CIIs), like airports, and even other CIIs, like energy and telecommunication networks). Therefore, there is an emerging need for innovative approaches that facilitate the identification, analysis, assessment, and mitigation of the organization-wise and interdependent cyber threats, vulnerabilities, and risks.

The challenge for the demonstrator in this area, as described in D5.1, is to implement targeted security services that will provide security for various critical maritime transport services, covering (i) the threat and risk management, (ii) the trust and key management services, (iii) the security of the communications in respect to the trust and key management services, and (iv) the software hardening of critical systems.

3.5.2 Important problems and challenges for the mid- and long-term

The main problems identified by the vertical stakeholders are:

- Deploy systems that follow the **resilience-by-design** principle
  - — Maritime operations are critical. Long-time failure of normal operations may lead to catastrophic results, especially for island regions. Reducing failures by building resilient systems seems to be the challenge that needs to be faced.

- Understand the continuously evolving **threat landscape** of the maritime sector (and transport sector in general)
  - — Although threats (and threat models) are relatively understood in digital domains (such as the domain of telecommunications and the Internet), threat models in maritime operations are very little understood.
    - Who is the adversary? What are their motives?
    - What do the adversaries want? Money? Ransom? Fame? Terrorism? Protest? Other?
    - At which part of the chain of operations will they choose to attack?
- Understand the cyber and physical **dependencies** with other systems or sectors and the relevant security risks.
  - — Maritime systems do not operate in isolation. How do they depend on other systems? What are these other systems? What is the weakest link there?
- **Security culture** within the maritime operations
  - — Ports and maritime supply chain providers are relatively new to the cybersecurity culture. Some of them may not be aware of emerging and interdependent cybersecurity threats, may not be prepared for catastrophic cybersecurity attacks, and may not perform regular risk assessments
- **Lack of targeted standards and methodologies**.
  - — Lack of specific tools or methodologies implemented for the specific analysis or assessment of maritime risks and their cascading effects. The existing risk management methodologies do not adequately take into account the cyber nature of the ports and the security requirements of the business processes associated with the maritime supply chains, which are nowadays ICT enabled and therefore severely dependent on intentional and unintentional compromise of CIIs.
- **Lack of information sharing**
  - — Port authorities, maritime supply chain providers, governments, and public authorities may be reluctant to share cybersecurity-relevant information. Private undertakings, as well, may be reluctant to share information on their cyber vulnerabilities and resulting losses for fear of compromising sensitive business information, risking their reputation or risking breaching data protection rules. Trust needs to be strengthened for public-private

partnerships to underpin wider cooperation and sharing of information across a greater number of sectors.

- **Hybrid attacks**
  - Ships are complex entities that can be subject to hybrid attacks that combine digital and physical systems. For example, attackers might collect information about the systems of a ship, trigger an attack in the digital world that will cripple a defence system and then launch an attack in the physical world through piracy or other means. Such hybrid attacks are extremely difficult to defend against.

3.5.3 Requirements in capabilities

Some of the most popular capabilities that are required for maritime transport in the future include:

- **Resilience** – robustness – fast systems recovery
  - As explained above, maritime systems need to operate 24/7 and be resilient to attacks. Prolonged disruptions of operations may have dire consequences for the population: no water and no fresh food in some cases.
- **Safeguarding** sensitive **data** and ensuring **data integrity**
  - Data integrity and confidentiality appear in several verticals. Indeed, in a world that depends on data, data integrity is a high priority for correct operations.
- **Availability and robustness against cyberattacks**
  - Very related to resilience, availability is a key requirement to ensure continuity of operations
- **Ability to adapt** to novel security threats
  - This is probably one of the toughest. The main difficulty stems from the word "novel". This means that this "novel" security threat is previously unknown: it is new. The defences needed to deal with it are not in place. And to make matters worse, it will take a few more days (or even weeks in some cases) before software patches become available.
- **Understanding** of cybersecurity
  - Although similar to the above, this is a bit more on the technical side. It is not just to understand "what is coming to our way", but also "how this attack actually works; how will it penetrate the systems; and how to identify the vulnerable systems".
- **Hardening** of software and systems
  - This is another tough one. Hardening is an ingenious approach to defend against what is not known. It is like saying "I do not know what is going to hit us, but to be on the safe side I will bolt down the windows". Same thing with computers: executables are going to be "fortified" and "hardened" so as to withstand the attack.

3.5.4 Technologies sought

The technologies needed to address the challenges above fall under the following categories:

- New methods are required that combine active approaches which are used to detect and analyse **anomalous activities** and attacks in real-time with reactive approaches that deals with the analysis

of the underlying infrastructure to assess an incident in order to provide a more holistic and integrated approach to incident handling.

- Usage of **big data, and machine learning and other artificial intelligence** techniques and technologies for the extraction of patterns in data and the identification of abnormal behaviours.
- Novel techniques for ensuring the **secure distribution and storage of all incident related artefacts** in order to protect them from unauthorized deletion, tampering, and revision.
- Integration of state-of-the-art elements for **risk prediction** related to the occurrence of threats, sensor/platform allocation, and communications
- Development of innovative **decision support systems for maritime security** involving different communities; integrating of decision support tools in operational environments (i.e. in legacy systems); research efforts in artificial intelligence applicable to security decision support systems.
- Adaptive and Dynamic **Threat Modelling and Risk Assessment/Management** (Targeted for Maritime)
- **Trust Management** systems that are distributed and resilient so that they can support secure communications
- **Authentication** Systems that provide a trusted identify in a world that consists of agents distributed all over the globe.
- **Security Hardening** for critical maritime systems

3.5.5 Further measures

In order to increase the likelihood that the technologies described above are adopted, accompanying measures were also recommended, as follows.

- **Awareness** among the relevant actors.
  - It is not surprising to see this. Awareness is usually the best line of defence. Fortunately, from a technical point of view, this is not difficult to develop.
- The compliance of all maritime supply chain providers with the security related standards (e.g. ISO28001) needs to become obligatory so information sharing can be accelerated. With a view of the Cybersecurity Package the maritime sector can benefit towards enhancing its cybersecurity in various ways:
  - Build cooperation between ENISA and the maritime stakeholders (e.g. IMO – the International Maritime Organization) to establish a maritime Information Sharing and Analysis Centres (ISACs) sharing best practices and guidance to all maritime actors on available tools, procedures, as well as getting guidance on how to address regulatory issues related to information sharing.
  - The NIS (Network and Information Systems) directive embraces the ports CIIs in order to establish an open, safe and secure cyberspace, highly contributing to coordinated prevention, detection and mitigation of risks enabling mutual assistance amongst the national competent maritime authorities. Synergies among the main actors (IMO, EMSA – the European Maritime Safety Agency, DGs MOVE, MARE, and CONNECT, and ENISA) need to be built in order to implement the NIS directive, as well as the USA's Strengthening

Cybersecurity Information Sharing and Coordination in Our Ports Act of 2015[25], in the ports CIIs, and a broad group of companies or trade associations of the maritime and logistics supply chain.

- Maritime Security Products need to be **certified** in order to overcome security maritime market fragmentation and at the same time strengthen the competitiveness of the EU maritime industry.
- Accelerate EU **maritime digital market**.
  - Identify existing innovative EU cyber products and innovative prototypes that can meet maritime needs. Bring the two communities (ICT developers and maritime integrators) together to upgrade existing cyber products and prototypes to meet maritime requirements. Avoid double-spending by strengthening the prospects of EU civilian and military maritime industrial markets; by shaping, implementing and coordinating industrial, military and civilian maritime cybersecurity and cyber defence research and efforts (e.g. programs, activities, funds).
- Build **collaboration** with public and private entities to develop **centres for cyber-security incident handling training** targeting general and maritime-specific security needs where simulation and exercise platforms will facilitate skills development.
  - Close the cyber skills gap with hands-on risk assessments, virtual simulation of industrial attacks and incidents targeting the maritime and international supply chain digital ecosystem. Extensively using cyber-ranges can help the maritime stakeholders to improve their understanding in handling complex attacks and incidents and improve preparedness and resilience in the maritime sector. This will involve realistic evidence-based experiments and "capture the flag" exercises with cyber defence and attack teams pitted against each other. EU and NATO (North-Atlantic Treaty Organisation) collaborate in common cyber exercises. ENISA (with its new mandate) is expanding the practical training efforts to all Member States engaging their military and civilian stakeholders.

3.6 Medical Data Exchange

Processing information efficiently is vital to the healthcare provider in order to suitably address patient care, advance the operational process and meet the changing regulatory mandates. And thus, the *Medical Data Exchange* vertical in CyberSec4Europe has the objective to enable a trustworthy exchange of sensitive data between several players who have different aims and claims.

3.6.1 Summary of findings and recommendations from D5.1

The main objective of the Medical Data Exchange demonstration as defined in D5.1 is to integrate and validate the research outcomes on the cyber-security and sensitive and personal data protection for medical

[25] https://www.congress.gov/bill/114th-congress/house-bill/3878

data sharing in a realistic environment (the Partner DAWEX' Data Exchange Marketplace). For achieving this, the following sub goals are defined:

- Enhance the multi-lateral trust among stakeholders generating and consuming data in the medical business sector (including pharmaceutical companies, hospitals and health tech companies as data providers, the Data Exchange Marketplace and laboratories and health research projects as data consumers);
- Improve the data marketplace exchange platform trustworthiness, and finally
- Generate new business opportunities.

3.6.2 Important problems and challenges for the mid- and long-term

The following are the cybersecurity challenges that the area of Medical Data Exchange needs to meet in the future.

- Obtaining consent and enforcing data subject rights in compliance with the GDPR
  - Today, many organisations handling medical data are not well prepared to process, collect and store personal data in a GDPR compliant way.
- Technical security measures are not updated
  - In case of the need to store a high amount of data (e.g., genetic data) companies should store these in the cloud. There are no clear or appropriate security measures for companies on how they should transfer such data.
- Exchange data between cooperating companies
  - Companies located in different countries have different rules and regulations on how medical data should be exchanged.
- Enhancing interoperability and data re-used through secure data governance.

Furthermore, more general cybersecurity challenges for this area were also mentioned:

- **Provide End-to-End encryption** and integrating data into electronic health records for data collected from heterogeneous sources and systems (IoT devices, monitoring systems, lab results and images)
- Difficulty to **implement access control, logging and Intrusion Detection Systems** in health care
  - There is a trade-off between patient safety and privacy, it is a challenge to define and enforce data accesses by medical personnel following the least privilege principle and to automatically analyse logs.
- Lacking of secure and usable authentication process
  - The GDPR implicitly requires 2-factor authentication, which is difficult to implement in practice and not even supported by some vendors.
- Trust in eHealth systems

- Many incidents on how patient information is mis-handled have been reported in the media (such as the recent data breach with the 1177 eHealth service in Sweden[26]) which have challenged trust.

- Creating security and privacy awareness
  - There is a need for technical people to understand legal rules (e.g., in regard to consent and data subject rights). They need to understand how to enforce the consent in an easy and legally compliant way.
- Implementing requirements from NIS Directive in an appropriate manner.

As Cybersecurity-related problems that need to be solved in order to meet the requirements, the following problems were mentioned:

- For the storage and processing of the medical data, it is not clear what appropriate/adequate security mean in different contexts.
  - For instance, the security and data protection by design requirements of the GDPR can be met if data outsourced to the cloud are anonymized or pseudonymised. However, there is not a clear way and rule for companies to achieve secure anonymization or pseudonymisation, and hence, companies should be helped in this direction;
- There is a lack of standardisation on how the data are exchanged between the national contact points in different countries;
  - Guidelines, standards and frameworks for medical data usage and storage exist, like the NIST (the National Institute of Standards and Technology in the USA) framework for clinical data exchange[27], FHIR (Fast Healthcare Interoperability Resources) Standard for exchanging electronic health records[28], and the Commission Recommendation on a European Electronic Health Record exchange format (C(2019)800) of 6 February 2019). While there are centralized rules for the exchange of genetic data in Europe and the USA (National Institutes of Health Genomic Data Sharing Policy[29]), there are no such rules for health data in general yet.

3.6.3 Requirements in capabilities

According to the responses of the stakeholders some of the most popular requirements and capabilities include:

- Awareness
  - Non-technical people should also understand the risks and basic threats of data breaches. As sometimes the personnel do not understand that they are invading the patients' privacy

[26] For more information about the 1177 data breach, see for instance: https://www.bbc.com/news/technology-47292887
[27] https://www.nist.gov/itl/ssd/clinical-data-exchange
[28] https://www.hl7.org/fhir/
[29]https://osp.od.nih.gov/wp-content/uploads/NIH_GDS_Policy.pdf

by doing things like keeping the doors unlocked, not logging out of accounts, or chatting about patients' data on a WhatsApp[30] group

- Improve competence level
  - Especially for vendors and developers in cybersecurity, they should increase their knowledge in secure coding, privacy by design and privacy by default. Moreover, security competence and awareness need to be increased at management level;
- Conduct more research
  - This is a need to understand more why it is very difficult to implement cybersecurity in healthcare. And the research should not only focus on the technology needed but also on the non-technical organizational security perspective.
- A sustainable and systematic approach to Cybersecurity as well as Information Security Management Systems needs to be implemented in Health Care.
  - Implement appropriate security controls, conduct evaluations, educate personnel and implement follow-up measures.

3.6.4 Technologies sought

Technologies that need to be developed or deployed in order to address the challenges above:

- **Secure and Easy-to-Use Authentication/Authorization Systems** need to be deployed and Authentication/Authorization policies need to be developed. Improving the secure authentication based on multiple factors is necessary. While SIQS[31]-based cards and two-factor authentication have been implemented in some systems, many password-based systems are still in use;
- **Architecture for keeping personal data updated**. This is especially a challenge for genetic data processing. Today, we only know at about 1% of what genetic data means and how it can be interpreted. New interpretations of genetic data and conclusions drawn from it can constantly change requiring an update of the patient's medical profile;
- **Crypto solutions on both data at rest and data in transfer.** Moreover, the development of crypto solutions for allowing the analyses on encrypted data needed;
- **Patient record systems need to be improved**, as the current systems do not look on privacy and security of information exchange;
- In general, **improved technical solutions for usable multi factor authentications**, Single Sign-On, Intrusion Detection Systems, role/context-based access control need to be developed for health care;
- Moreover, the need for a **health-care dedicated blockchain/ledger**, which would provide a patient-centred solution for increasing transparency of data processing.

[30] Whatsapp.com
[31] Self-Initializing Quadratic Sieve

3.6.5 Further measures

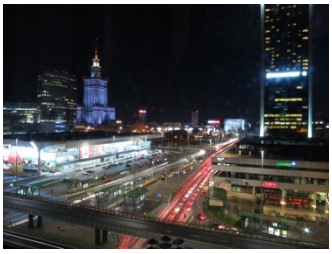
Measures that could be further developed to improve the Medical Data Exchange are as follows:

- Companies need to build their own **architecture for storing huge and sensitive data** in a secure way.
- More government regulations
    - More regulations from the government could generally provide help. GDPR is a good example on a regulation that puts more pressure to improve the security and privacy of health care systems.
- Standardization and regulations for cloud service providers
    - Certifications for cloud service providers within the healthcare system is needed. It should be required that all cloud providers string data of a certain information class/risk need to be certified according to certain requirements.
- There is a need for trustworthy systems and products, but also the trustworthiness of all stakeholders involved needs to be guaranteed.
    - Security metrics are needed for measuring the achieved level of security and privacy of controls, and thus the level of "trustworthiness".
- There is a need for a secure development process for both networks and systems, based on Data Protection by Design (as already required by the GDPR) and Security by Design.

3.7 Smart Cities

Over the past few years an increasing amount of automation has started to permeate everyday environments: from regulating the water in large scale facilities to regulating the temperature in ordinary homes, smart devices have started to proliferate and will contribute to do so in the future. As these sensors and actuators monitor and control significant parts of everyday life, they are bound to be considered by cyber attackers as an attack target. To address this challenge, smart cities will be forced to implement the necessary mechanisms so as to offer a safe and secure environment to their citizens.

3.7.1 Summary of findings and recommendations from D5.1



The Smart Cities demonstrator has to operate in a complex environment where Local Public Administrations (LPAs) need to adopt tools to protect themselves from cyber-attacks in privacy and security. Such attacks can happen at the individual level (such as citizens and civil servants) and at the organizational level (such as Public Authorities and Third Parties). The two levels will need different kinds of tools as follows:

- At an individual level:
    - A Social Driven Vulnerability Assessment, that may simulate one of the most dangerous attack strategies (called Social Engineering) performed by attackers against people (both

employee and citizens) in order to convince them to reveal personal and sensitive information.
  - An assessment tool for people about phishing emails, the goal being to assess their capability to identify phishing emails.
  - An entire training platform that may facilitate Organizations (not only LPAs) to manage and assign specific training plans to people (both citizens and employees), in order to improve cyber-threats awareness and knowledge on how to defend themselves from an "on-going threat reality".
- At an organizational level: a Risk Assessment Tool, the aim of which is to help Risk managers, CEOs[32] and LPAs to obtain a full detailed report based on discovered vulnerabilities and estimated economic impacts. The carried-out goal is not only to give a predictive analysis of the possible attacks and impacts that an organization may suffer, but also to give a detailed plan of mitigation actions (both soft and hard) which need to be implemented in order to minimize risks.

The work in WP5 has identified two major goals:

- To setup and put into operation a **consent-based infrastructure** to support sensor and other urban data platform and infrastructure for **personal data exchange** and reuse in public services, in compliance with GDPR.
- To setup an **Open Innovation cycle** that will drive city stakeholders from cybersecurity risks and needs assessment to the identification of the related solutions (i.e., cybersecurity services): Setup cyber-security risk assessment tools and social engineering penetration testing tools.

3.7.2 Important problems and challenges for the mid- and long-term

The stakeholders identified the following main problems and challenges for the Smart Cities vertical.

- Federation of **trust** among all involved stakeholders
  - Building a federation of trust is a major challenge that needs to be addressed. Some market players (such as Google and Facebook) have already moved very fast into this direction providing seamless authentication, authorization, and trust across a wide variety of platforms.
- **Physical Tampering**
  - Smart devices may be deployed in an open or even hostile environment where complete strangers may have physical access to them. Indeed, these strangers, which can even be attackers, may touch a device, may open a device, may distort the device, etc. Such physical access may adversely impact the security of the device and the integrity of its operation. To make matters worse such tampering may also affect the security and safety of those who depend on the operation of the device.
- **Social Engineering**

[32] Chief Executive Officer

- Surrounded by millions of smart gadgets in a smart city, ordinary citizens may fall victims to social engineering. Attackers may now easily impersonate practically any organization in the city (from the water supply to the garbage collector) and phish for passwords and valuable information.

- **Interfaces with Legacy Systems**
  - Interfacing legacy systems with digital ones, may open new attack opportunities to such legacy systems which were safe due to their isolation from the digital world.
- **Change the operation model from emergency to prevention**.
  - Sometimes the mode of operation is based on emergency: put out a fire, handle a surge in the traffic, etc. Using big data analytics, the model may change from emergency to prevention.
- **Secure access to data** at the edge
  - Securing data in highly guarded data centres does not seem extremely difficult. Securing data collected from or stored at sensors that are deployed in isolation, which could be subject to all kinds of attacks, from tampering to vandalism, is a challenge that needs to be addressed.
- **Risk Management – Assessment**
  - Systems in Smart Cities will be used 24/7 by ordinary, non tech-savvy people. To make sure that the systems perform as expected extensive risk assessment and management needs to be performed.
- **Blindly trust in the holder of the data** which may even be the government
  - This may turn out to be the biggest challenge for the era of big data. How do you trust the holder of the data? How can the holder of the data prove that they are trustworthy? How can people verify that data holders do not betray their trust? How do people that the digital world they build will not become a panopticon that will be used against them?

3.7.3 Requirements in capabilities

Smart Cities is a rising application area. To be able to provide a safe and secure Smart Cities operations environment, several capabilities are needed. According to the feedback received, the most important needed requirements are:

- **Education** and **training**. Stakeholders mentioned education, cyber-ranges, campaigns, awareness etc. Interestingly, they called for "top management **awareness**" about the cybersecurity risks. They also called for privacy **awareness** among ordinary people – people who say "I do not care about companies exploiting my data".
- **Privacy** policies and rules as a capability need to be developed. Indeed, Smart Cities may turn out to be a huge Big Brother who will monitor all activities. To avoid the dystopia of 1984, one needs

not only privacy-preserving technologies, but also privacy policies and rules that will enforce the protection and preservation of privacy of citizens as they move around in a Smart City environment.

- **SMEs capacity to react to cyber-attacks.** It is expected that several of the functions provided by Smart Cities will be consumed by (or provided by) SMEs**.**
- **Security by design.** This includes verification, validation, etc. This is a requirement that crops up often.
- **Security metrics.** This is a very important requirement – scientists need to get better at measuring security.
- **Data traceability.** Be able to explain where each piece of data comes from and how it arrived to its current state.
- **Resilient Services** and Infrastructures
- **Enable citizens to have control** over the use and haring of their data. Allow for user-centric infrastructures.

3.7.4 Technologies sought

Some of the technologies that will be needed to support the Smart Cities of the future include:

- **Security/privacy labels**. This is an "easy-to-understand" label about how much security or privacy a device or an application provides. One might think of it as the "energy consumption" labels in home appliances. For example, a security/privacy label of "A" means good level of security/privacy protection, a security/privacy label of "B" means fair level of security/privacy protection, and a privacy label of "C" means bad level of security/privacy protection. The hope is that this will be a simple way to communicate to consumers which devices respect their privacy and which devices do not.
- Standards and interfaces to enable the **opening of public data** to the entire EU so as to build cross country e-services.
- **Privacy enhancing technologies**. This is a very broad area which, however, is desperately needed, as several of the data will be personal data, or will help to uncover personal information.[33]
- **Distributed ledgers** (like blockchain). Trust and provenance are requirements that appear often in the Smart Cities vertical. Distributed ledgers or other similar technologies (e.g., secure logging) need to be developed to solve the problem at the scale (size of data and number of transactions per second) required.
- **Simple authentication mechanisms for citizens.**

3.7.5 Further measures

Some of the further measures that have been mentioned include:

[33] For example, the electric consumption of a house may seem to contain no personal data at all. However, such data can be used to deduce when the occupants of the house are at home, what are their daily/weekly patterns, etc.

- Appropriate **education** in **secure coding** and secure software development. Education, training, and capacity building are among the top priorities.
- Development of national and regional **cybersecurity centres**. This is a very interesting approach that may significantly improve the state of cybersecurity. Although there exist some relevant centres, in the form of CERTs or report offices, very little effort has been dedicated to creating a concerted approach in this area.
- **Liability**. Some problems just cannot be solved by technology alone. In such cases, legal and policy interventions may

4 Commonalities among the Verticals

This section illuminates the common points that have emerged in at least two Verticals. Such commonalities give a clear entry avenue where to prioritize policy design that is meant to foster research on specific areas. In case further prioritisation would be needed, then a finer study about the broader impact of each of such commonalities should be performed. As we have done in the previous section, we will group the commonalities in terms of challenges, requirements, and technologies.

4.1 Common Challenges for the Mid and Long Term

- **Trust.** Depending on the vertical, the need for trust is conceived in different ways. Thus, in the case of Smart cities, federation of trust is the challenge, building trust in other verticals or trusting the data holder in the smart cities vertical. The establishment of trust is essential for information sharing in any vertical although it is highlighted as important for maritime transport and supply chain.
- **Privacy and Identity Management**. The challenge of privacy is manifold. Depending on the vertical, however, most of them consider the achievement of privacy as a key challenge. Thus, for medical data exchange the main concern is, apart for how data is treated, the need to be compliant with the GDPR, whereas in the Online Banking case the stakeholders refer to confidentiality and proper identity management as a key point. Also, in this sense, for the Privacy preserving Identity management, the highlighted challenge is the combination of some requirements: strong privacy, trustworthiness and usability.
- **Authentication**. All the verticals consider the need for authentication as a challenge, however, very related to identity management. Of special relevance is the difficulty to implement usable authentication, access control and logging in health care. The implementation of usable two factors authentication implicitly required by the GDPR for accessing special categories of data is a special challenge in health care systems, for instance.
- **Resilience.** This challenge is especially important in verticals that are critical, such as the Maritime Transport or Supply Chain. In these cases, building resilient systems becomes essential as a failure in any operation might lead to disastrous effects. In particular, the term *resilience by design* is considered as a key challenge.
- **Threat landscape or detection of fraud.** The first term is used in maritime transport and for online banking scenarios the latter, however, they refer to the same idea. In this vertical, stakeholders highlight the need to consider hybrid attacks as specific for them. A related challenge is considered by the Supply Chain vertical as *event management, prevention and detection.* In the same direction, the stakeholders for the Privacy-preserving Identity management vertical highlight the need for

more effective security controls that avoid them to be exposed to vulnerabilities. In the case of smart cities social engineering might be a source of attacks for smart devices.

- **Training and cybersecurity culture.** This is horizontal challenge for all the verticals. In general, all the stakeholders agree on the lack of cybersecurity professionals to be hired by companies. In the same direction for some verticals, such as the maritime transport one, this challenge is addressed as security culture in new cybersecurity threats that might arise.
- **Standardization and certification.** Supply chain and maritime, medical data exchange need standardization of methodologies. Certification for cloud providers is also needed.

Besides the challenges listed above, the specific ones for each scenario are well explained in Section 3.

4.2 Common Requirements

By analysing the requirements specified for each of the verticals in Section 3 we can observe that some of them are common to all or most of them.

- **Education and training.** This is a requirement that has been considered as essential by all the stakeholders inquired for all the verticals. Then, for each of the verticals there are some specific professional profiles with specific knowledge that are needed. Thus, for instance, in the privacy-preserving identity management or secure data exchange verticals the required professionals should have specific knowledge on how to deal with the requirements of the GDPR.
- **Raising cybersecurity awareness** is slightly related to the previous one, not only in terms of education but in terms of making non-technical users aware of the cybersecurity risks that they might face in the respective verticals. However, it seems that cybersecurity awareness is at a higher level in the online banking scenario.
- **Certification and standardization.** The need for having certified projects or using standard tools or technologies is considered by all the verticals. Thus, for example, the online banking vertical mentions as a requirement the need for a transversal digital identity platform or the development of protocols using web standards. Or for medical data exchange it is mandatory that the cloud providers are certified in the field of health care.
- **Resilience.** All the verticals highlight the need for resilience as a requirement that must be met in all the cases. Thus, this requirement is especially important in supply chain, maritime transport and smart cities. In online banking, the requirement is considered as 'smart decision-making' systems that are able to adapt or in smart cities the requirement is specified in terms of capacity of SMEs to react to cyber-attacks as well as to specific resilient services and infrastructures.
- **Security and privacy by design.** Some verticals mention this requirement as such, however, it includes aspects such as verification and validation that are considered for all the verticals.
- **Data exchange and information sharing.** This requirement is very related to security and privacy by design and might involve also some notions of trust. Also, regulations that are GDPR compliant is related to the information sharing aspect.

4.3 Common Technologies Sought

In order to achieve the requirements identified in Section 4.2, the stakeholders mentioned the following technologies as most needed.

- **Encryption and cryptography techniques.** The use of technologies that provide encrypted identities is of paramount importance for dealing with the identities of the actors involved in the verticals.
- **Distributed Ledgers (e.g., blockchain).** These technologies seem to be the preferred ones to achieve the requirements listed above in smart cities, maritime transport, online banking, etc., where the scale of data per second in increasing.
- **Strong authentication and authorization mechanisms.** These technologies are required for all the verticals and all of them suggest to have them as simple as possible to make them usable for regular citizens, when needed.
- **Trust management.** Trust management systems should be distributed and resilient so the exchange of data in all the verticals can be done in a successful way and we can guarantee integrity of the data.
- **Artificial Intelligence or Big Data.** These techniques will be useful for extracting data and the identification of abnormal behaviours, for example in the cases of supply chain, maritime transport or smart cities.

5 Conclusion

This document presented deliverable "D4.1 - Requirements Analysis from Vertical Stakeholders", becoming the basis for the roadmap to be developed in the remaining of Work Package 4.

For all Verticals, requirements for future research were elicited from the project's stakeholders, as well as from other players that have direct and specific interests into, or interact with, such vertical ecosystems. The methodology that was used in the elicitation process, described in Section 2, facilitated the collection of important problems and challenges for the mid- and long-term in each of the Verticals. Such a landscape then induced requirements in capabilities, technologies, and other related measures that are going to be needed to address those problems and challenges in future. Importantly, such requirements were put in perspective against the findings and recommendations produced by WP5 in D5.1.

The main take-aways from the identification of the commonalities among the Verticals' requirements are as follows.

- **Common challenges**: Trust, privacy and identity management, authentication, resilience, threats identification and fraud detection, capacity building that include the development of a cybersecurity culture, and the establishment of standards and certification frameworks.

- **Common requirements**: Education, training, cybersecurity awareness campaigns, certified projects, widening the use of standard tools and technologies, resilient systems, security and privacy by design, and an environment where data are exchanged and information is shared in volumes much larger than today.

- **Common technologies**: Encryption and cryptography techniques, distributed ledger technologies, strong authentication and authorisation mechanisms, trust management, tools based on Big Data, and Artificial Intelligence.

Therefore, it can be concluded that CyberSec4Europe's stakeholders envision resilient systems, infrastructures, and societies as their common objective. It emerges from this task as a whole that their needs will only be fulfilled by an environment that wisely encompasses regulation, incentives, structural reorganisations, and capacity building, along with research and deployment of new technologies.

As said above, the results shown in this deliverable will now serve as foundation for WP4's roadmap, which will be developed in the course of the whole project. In addition, they also provide feedback to Task 3.1, for the methodology definition on research topics to be pursued in future, and to WP5, for the integration of these mid- and long-term considerations into its demonstrators. Such a full integration into the project output is a guarantee that the demands of the project's stakeholders will be at the forefront of CyberSec4Europe's works.

6 Annex

Table of contents in this Annex

Material used to question stakeholders

Interview request letter

Short Interviews for Eliciting Stakeholder Requirements for a CyberSecurity Roadmap

We want to ask you as an important stakeholder in the area of Cyber Security to participate in a telco interview for eliciting both cybersecurity requirements in your area of activities for the EU H2020 project CyberSec4Europe.

CyberSec4Europe is one of the pilots funded by the European Union to explore common European Cybersecurity Research & Innovation Roadmaps beyond 2020 and European cybersecurity strategies for industry. Mariya Gabriel, Commissioner for Digital Economy and Society, said: "*These projects will assist the EU in defining, testing and establishing the governance model of a European Cybersecurity Competence Network of cybersecurity centres of excellence.*" The competence centre is supposed to become the main body that would manage EU financial resources dedicated to cybersecurity research under the two proposed programmes – Digital Europe and Horizon Europe – within the next multiannual financial framework, for 2021-2027.

For more Information, see:

http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2019)635518

Your expert opinion is of utmost importance for correctly shaping the European cybersecurity landscape of the future.

Participation is completely voluntarily with the participant's consent. Data will be collected and processed in compliance with the EU General Data Protection Regulation (GDPR) and no sensitive personal data will be asked or processed. The study should take not more than 15-20 minutes.

Please contact us by email, telephone or in person if you could like to participate, so that we could schedule a time for the Interview

Contact persons:

Interview form

(All questions are voluntary):

Profession/Role:…….

Organisation:…….

Gender:…….

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange
- ☐ Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

Q5: For your selected area describe some technologies that need to be developed-deployed
(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

Privacy Policy & Consent Form for Stakeholder Interviews

Introduction:

CyberSec4Europe is one of the pilot projects funded by the European Union (H2020) to explore common European Cybersecurity Research & Innovation Roadmaps beyond 2020 and European cybersecurity strategies for industry.
This survey will help CyberSec4Europe to analyses the problem space and to elicit cybersecurity requirements in your area of activities for developing a common Research and Innovation Roadmap Competence Network.

What data will be collected and for what purposes? Who will process your data?

With your consent, Karlstad University (KAU) as the data controller will collect and process the following data:

- Contact data (name, email)
- demographic data (type profession, type organization, role, gender)
- Your area of expertise

in addition to your interview answers in regard to Cyber Security problems and requirements.
Moreover, the interview session may be voice-recorded if you consent. In addition, a list matching your name with a pseudonym will be created for the purpose of pseudonymisation of all data collected for this interview.

All data will be kept confidential, stored safely, transcribed, and pseudonymised.
Your data will be used for the sole research purpose of collecting stakeholders' opinions on the requirements.
Interview results will be reported in project deliverables and research papers in anonymised form.

How will your data be processed?

All your data *including the notes and any recordings that we take* will be kept confidential, stored safely in a locked filing cabinet or on a secured partition of a computer hard drive, transcribed, pseudonymised as soon as possible and deleted after the archiving period of 10 years (required by KAU for all original research data for preventing/detecting research fraud). The list matching your names to pseudonyms will be kept separately from all other collected data at a secure place.
Data processing and handling will be done by KAU and in compliance with the EU General Data Protection Regulation (GDPR). The data will also be shared with other CyberSecurity4Europe project partners, which are all located in Europe. At no time, your name or any other information that may directly identify you will be used when reporting the results, unless you explicitly agree to be quoted for specific statements.

Voluntary Participation & Your Rights:

Participation in this test is **completely voluntary**. You are free to leave or end the interview at any point without explanations. If you withdraw, we will delete your data and therefore destroy any notes in which you are represented. You can also exercise your data subject rights to access, rectification, deletion or blocking of your data according to the GDPR without any costs – data deletion is however only possible up to the time that the results of the interview analyses will be published in anonymized form.

Contact:

If you have questions, concerns or if you want to exercise your rights, please contact:

Data controller:

Contact persons:

You can provide your consent by signing and ticking the respective boxes below:

[ ] I agree to participate in the interview for the CYBERSEC4EUROPE project and to provide the data for the purposes and under the conditions stated above.

_____

Participant's Signature, Place & Date

[ ] I agree to the audio recording of the interview session.

_____

Participant's Signature, Place & Date

Survey form

CyberSec4Europe - **European Network of Centres of Cybersecurity Expertise.**

Fields marked with * are mandatory.

EUROPEAN NETWORK OF CENTRES OF CYBERSECURITY EXPERTISE.

YOUR OPINION MATTERS

Introduction

Who We Are

CyberSec4Europe is one of the pilots funded by the European Commission to explore common European Cybersecurity Research & Innovation Roadmaps beyond 2020 and European cybersecurity strategies for industry.
Mariya Gabriel, Commissioner for Digital Economy and Society, said: "These projects will assist the EU in defining, testing and establishing the governance model of a European Cybersecurity Competence Network of cybersecurity centres of excellence."
The competence centre is supposed to become the main body that would manage EU financial resources dedicated to cybersecurity research under the two proposed programmes – Digital Europe and Horizon Europe – within the next multiannual financial framework, for 2021-2027.

More info: http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2019)635518

Why We Ask You

This survey will elicit both cybersecurity requirements in your area of activities and suggestions about governance models for the Competence Network.
Your expert opinion is of utmost importance for correctly shaping the European cybersecurity landscape of the future.

1

Privacy Policy & Consent

Participation in this survey is completely voluntary. Your data will be used for the sole research purpose of collecting stakeholders' opinions on cybersecurity requirements and the governance of the network of cybersecurity centers.
Such opinions would not be attributed personally to you along the "Opinion on Anonymisation Techniques" WP216 05/2014 by Article 29 Working Party and will be reported as overall findings described in scientific reports (e.g. deliverables to the European Union).

See the full provacy policy in PDF:
CS4E_Interview-_Full_privacy_policy.pdf

☐ * I agree to the survey

Information about the respondent

Country

- ○ Austria
- ○ Belgium
- ○ Bulgaria
- ○ Croatia
- ○ Cyprus
- ○ Czech Republic
- ○ Denmark
- ○ Estonia
- ○ Finland
- ○ France
- ○ Germany
- ○ Greece
- ○ Hungary
- ○ Ireland
- ○ Italy
- ○ Latvia
- ○ Lithuania
- ○ Luxembourg
- ○ Malta
- ○ Netherlands
- ○ Poland
- ○ Portugal
- ○ Romania
- ○ Slovak Republic
- ○ Slovenia
- ○ Spain

2

- Sweden
- United Kingdom
- Other

If other please specify

*You are employed in:

- Industry
- Academy
- European Agency
- National Agency
- European Regulator
- National Regulator
- Law Enforcement
- Standardization Body
- Other

Other (please specify):

*What is your area of work?

at least 1 choice(s)

The following sectors are taken from the statistical classification of economic activities in the European Community (NACE). They will be used to associate your response to the different stakeholders communities.

Agriculture, Forestry, Fishing
Mining, Quarrying, and Oil and Gas Extraction
Utilities (electricity, gas and water supply, waste management, etc.)
Construction
Manufacturing
Wholesale Trade
Retail Trade
Transportation and Warehousing
Information and communication
Finance and Insurance
Real Estate and Rental and Leasing
Professional, Scientific, and Technical Services
Management of Companies and Enterprises
Administrative and Support Services
Education
Health Care and Social Assistance
Arts, Entertainment, and Recreation
Accommodation and Food Services
Public Administration

Defense
International organizations
Other

Other (please specify)

What is your position?

- ☐ President/CEO/Member of Board
- ☐ Senior administrator/head of department
- ☐ Manager/professor/head of group
- ☐ Officer/Researcher/Administrator/Member of Staff
- ☐ Consultant/self-employed/
- ☐ Other

Other (please specify)

* Are you directly involved in one of the EU pilot projects launched to prepare the European Cybersecurity Competence Network?

- ○ Yes
- ○ No

* Are you involved in CyberSec4Europe?

4

- Yes
- No

* Which of the following verticals of the pilots is your specific area of expertise:

at least 1 choice(s)

- Finance and E-Commerce
- Supply Chain Security Assurance
- Privacy-preserving Identity Management
- Incident Reporting
- Maritime Transport
- e-Health and Medical Data Exchange
- Smart Cities

* Which of the following Cybersecurity Vertical Sectors is your specific area of expertise?

- Energy
- Financial
- Health/Medicine
- Digital Infrastructure
- Transportation
- Public Safety
- Defense
- Space

Main goal

What Europe should achieve as an overall goal in cybersecurity?

*

In your specific area of expertise, what is the key cybersecurity situation that must change (e.g. better resilience, transparency, trustworthiness, security metrics...)? If possible, explain also the motivations behind your indications.

The European Cybersecurity Competence Network will have to indentify its key priorities to drive the cybersecurity technological agenda and access to cybersecurity expertise.

Capabilities

* In your area, what key capabilities are required by systems, people, institutions, etc, to achieve that change?

The Competence Centre and its Network will become the main implementation mechanism for activities in support to Member States and the cybersecurity industry (including deployment, investments and research) in the 2021-2027 period.

What is needed to achieve the capabilities you just mentioned?

	Not Essential	Of Minor Importance	Of Major Importance	Essential
Novel Technologies	○	○	○	○
New professional or academic skills	○	○	○	○
Policy interventions (regulations and fines)	○	○	○	○
New Certification and Audit procedures	○	○	○	○
New or improved technical standards	○	○	○	○
Other	○	○	○	○

Other (please specify):

* Please describe some specific technologies or technical standards that you have in mind

6

* Please describe some specific organisational measures (e.g. skill sets, regulation, liability) that you think are important

Decision Makers in the Network

The upcoming regulations of the European Cybersecurity Competence Network of cybersecurity centres establish that the main European centre will be governed by the European Commission and the Member States. However, the participants to Advisory Committee and the Individual National Centres are not yet defined. The purpose of the Pilots is to suggest the European Commission on their composition and their decision making process.

* Who should be the key players in the *European Cybersecurity Competence Network of cybersecurity centres of excellence* to achieve those capabilities?

between 1 and 8 choices

- ☐ European Commission
- ☐ ENISA (European Network and Information Security Agency)
- ☐ National cybersecurity agencies
- ☐ Other national Government Representatives
- ☐ Industry
- ☐ Academia
- ☐ Industry associations
- ☐ Consumer associations
- ☐ Data Protection Authorities
- ☐ Computer Emergency Response Teams (CERTs, CSIRTs)
- ☐ Formal standards and/or certification organizations (e.g., ISO, ITU)
- ☐ Community standards and/or certification organizations (e.g., IETF)
- ☐ Community professional organizations (e.g., NANOG, community around RIRs like the RIPE NCC)
- ☐ Open Source software communities (e.g., the Linux foundation or the community around FOSDEM)
- ☐ Hacker communities (e.g., the German CCC or members of European Hackerspaces)
- ☐ Other

If other please specify:

* In your expert opinion, what should be the key role of the entities you have selected above in the *Network* ? (Decision making on Financial allocation, advisory to Member States, etc.)

The Competence Centre and its Network will become the main implementation mechanism for activities in support to Member States and the cybersecurity industry (including financial distribution of EU funds, deployment and research) in the 2021-2027 period.

What type of accreditation process would be appropriate for those players in the *Network* ?

What do you think should be the relationship between ENISA (European Network and Information Security Agency) and the *Network*?

Has your national legislation given a coordination role on cybersecurity to a national agency?

- YES
- NO

If yes: what do you think should be its relationship with the *Network*?

Any Other Issue

8

What additional information you would like to give us and that we forgot to ask for?

Would you like to/prefer to be interviewed in person? (If YES, please live your contact details below).

- Yes
- No

More information on the interview session:

CS4E- Interview information.pdf

Name

Email

9

Collection of responses

Interview forms

Profession/Role <Anonymized>

Organisation <Anonymized>

Gender <Anonymized>

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity

X Medical Data Exchange

- ☐ Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

- People need to trust the services that share the data.
- Data exchange applications and systems should be easy to use for people.
- Interoperability about the data is also critical since there are thousands of medical devices and services that need to speak to each other

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

- The first problem is the secure storage of medical data. Many cyber-attacks now go after medical data.
- The second problem is the security of the IoT and medical devices that generate the data.

- The third one is the data privacy technologies that need to be applied before sharing the data. In many regulations and jurisdictions, data needs to be anonymised before shared.

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed
(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

- End-to-end encryption,
- better standards and policies for security hardening of medical devices,
- education and training of the personnel,
- scalable data privacy technologies

Q5: For your selected area describe some technologies that need to be developed-deployed
(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

- Security auditing profiles for medical devices,
- advanced data privacy technologies like homomorphic encryption

Profession/Role: <Anonymized>

Organisation: <Anonymized>

Gender: <Anonymized>

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ **Maritime Cybersecurity**
- ☐ Medical Data Exchange
- ☐ Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

- Resilience against both cyber and physical threats, that includes: (a) robustness (critical systems should continue to provide a minimum service level during or after an unwanted event) and (b) fast system recovery.
- Availability, since this is closely related to resilience.
- Ability to quickly identify and to adapt to novel security threats (such as cascading threats and indirect attack paths that may exploit the increased connectivity of modern maritime systems)

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

- Deploy systems that follow the resilience-by-design principle
- Understand the continuously evolving threat landscape of the maritime sector (and transport sector in general)
- Understand the cyber and physical dependencies with other systems or sectors and the relevant security risks.

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

- Cybersecurity awareness of the involved actors
- Novel cybersecurity technologies following the resilience-by-design principle

Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

- Adaptive and dynamic threat modelling and risk assessment methodologies specifically tailored to the needs of the transport sector.
- Distributed and resilient trust management systems/platforms to support secure communications.
- Security hardening for critical maritime systems.

Profession/Role:……

Organisation:……

Gender:……

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange
- ☐ Smart Cities and IoT
- ☐

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

- Hardening and resilience of the ports' and maritime in general critical infrastructures to any kind of cyber-attack
- Safeguarding sensitive data and ensuring data integrity
- Ensuring the robustness of the maritime ICT infrastructures against cyber attacks.
- Improving the security and protection of maritime information systems from cyber-crime and cyber-terrorism
- Ensuring all aspects of integrity, trust and liability in ports' and maritime operations

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

- **Security culture within the maritime operations**: Ports and maritime supply chain providers do not have a mature cybersecurity culture. Most EU commercial ports do not adopt "Good ICT supply chain security and are not aware of emerging and interdependent cybersecurity threats and are not prepared for catastrophic cybersecurity attacks. They do not perform regular risk assessments and they do not have incident handling strategies.
- **Lack of targeted standards and methodologies**: lack of specific tools or methodologies implemented for the specific analysis or assessment of maritime risks and their cascading effects. The existing risk management methodologies do not adequately take into account the cyber nature of the ports and the security requirements of the business processes associated with supply chains,

which are nowadays ICT enabled and therefore severely dependent on intentional and unintentional compromise of CIIs.

- **Information sharing**: Port authorities, maritime supply chain providers, governments and public authorities are reluctant to share cybersecurity-relevant information for fear of losing their reputation or of compromising commercial, enterprise or national security and competitiveness. Private undertakings are reluctant to share information on their cyber vulnerabilities and resulting losses for fear of compromising sensitive business information, risking their reputation or risking breaching data protection rules. Trust needs to be strengthened for public-private partnerships to underpin wider cooperation and sharing of information across a greater number of sectors.
- **Certification**: Certification plays a critical role in increasing trust and security in products and services that are crucial for the digital single market. At the moment, a number of different security certification schemes for ICT products exist in the EU. For example, currently smart meter producers need to undergo separate certification processes in France, UK and Germany. While these initiatives prove the importance of certification, there is an increasing risk of creating fragmentation and barriers in the single market.
- **Economic Crisis: A stumbling block to maritime security**: Maritime's activities were severely affected by the most recent economic crisis. Personnel is reducing and no budget is foreseen, in order to increase the security team of the maritime operators and authorities. In particular, they are not willing to finance the security enhancements of their companies.

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

- Maritime Organizations (e.g. IMO, EMSA, ENISA, IPCSA, DGMARE) may contribute towards security awareness raising by giving presentations during various events, offering security seminars, certification courses and summer schools. Furthermore, they may use their dissemination tools (e.g. Newsletters, magazines, newspapers, social media) to inform the maritime world about emerging security threats. The insurance companies and auditors may be the main drivers in the campaign of maritime security awareness by enforcing maritime providers to comply with existing cyber and supply chain security standards (e.g. ISO28000, ISO28001, ISO27001, ISO27005), directives (e.g. NIS, GDPS) and guidelines (IMO cybersecurity guidelines)
- The compliance of all maritime supply chain providers with the security related standards (e.g. ISO28001) need to become obligatory so information sharing can be accelerated.
  With a view of the Cybersecurity Package the maritime sector can benefit towards enhancing its cybersecurity in various ways:
  - ✓ Build cooperation between ENISA and the maritime stakeholders (e.g. IMO) to establish a maritime Information Sharing and Analysis Centres (ISACs) sharing best practices and guidance to all maritime actors on available tools, procedures, as well as getting guidance on how to address regulatory issues related to information sharing.
  - ✓ NIS directive embrace the ports CIIs in order to establish an open, safe and secure cyberspace, highly contributing to coordinated prevention, detection and mitigation of risks enabling mutual assistance amongst the national competent maritime authorities. Synergies among the main actors (IMO, EMSA, DGMOVE, DGMARE, DGCONNECT, ENISA) need to be built in order to implement the CIIP and NIS directives as well as the

USA, 2016H.R.3878 in the ports CIIS, and a broad group of companies or trade associations of the maritime and logistics supply chain

- Maritime Security Products need to be certified for overcoming security maritime market fragmentation and strengthening the competitiveness of the EU maritime industry.
- Build collaboration with public and private entities to develop centres for cyber-security incident handling training targeting general and maritime-specific security needs where simulation and exercise platforms will facilitate skills development. Close the cyber skills gap with hands-on risk assessments, virtual simulation of industrial attacks and incidents targeting the maritime and international supply chain digital ecosystem. Extensively using cyber-ranges (Internet-scale simulation environments-e.g. In this context, targeted training methodologies and modelling/visualization tools can help the maritime stakeholders to improve their understanding in handling complex attacks and incidents and improve preparedness and resilience in the maritime sector. This will involve realistic evidence based experiments and "capture the flag" exercises with cyber defense and attack teams pitted against each other. EU and NATO collaborate in common cyber exercises. ENISA (with its new mandate) is expanding the practical training efforts to all Member States engaging their military and civilian stakeholders.
- Develop common civilian-military maritime security centre. In Communication JOIN(2017) 450 "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"[34], the Commission announced the intention to create a cybersecurity competence network with a European Cybersecurity Research and Competence Centre. Civilian and military maritime research entities should become part of the EU network to jointly carry out research solving civilian and military cyber defence challenges (e.g. develop defensive strategies for upcoming Artificial Intelligent attacks). Build a cyber defence cluster of expertise within the European Cyber Security Network of Excellence involving military and civilian actors in order to develop common Research agendas in the common areas of interest (e.g. training, innovation, certification, procurement).
- Accelerate EU maritime digital market. Identify existing innovative EU cyber products and innovative prototypes that can meet maritime needs. Bring the two communities (ICT developers and maritime integrators) together to upgrade existing cyber products and prototypes to meet maritime requirements. Avoid double-spending by strengthening the prospects of EU civilian and military maritime industrial markets; by shaping, implementing and coordinating industrial, military and civilian maritime cybersecurity and cyber defence research and efforts (e.g. programs, activities, funds).
- Harmonise military-civilian maritime certification efforts. Assess military maritime security certification schema against civilian certification schema for cyber security and cyber defence. Reach consensus on certification requirements based on civilian and military usage; for the development of common Protection Profiles (PPs) for the EU cybersecurity and cyber defence products covering various dimensions e.g. privacy, security, transparency, interoperability, accountability, liability and compliance with EU directives. Encourage both communities (military and civilian) of manufacturers, developers and integrators to adopt the culture of sharing responsibilities for security by performing common conformance testing.

[34] http://ec.europa.eu/transparency/regdoc/?fuseaction=list&coteId=10101&version=ALL

- Strengthen and expand the Digital Single Market (DSM). Maritime cyber security and cyber defence markets need to be considered as part of the Digital Single Market (DSM) and need to be treated as such. The Commission efforts strengthen the conditions for an open and competitive cyber market in Europe; help companies operate across borders and help Member States get best value for money in their procurements. These efforts have high impact in the facilitation and enlargement of the DSM.

Q5: For your selected area describe some technologies that need to be developed-deployed
(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

- New methods required that combine active approaches which are used to detect and analyze anomaly activities and attacks in real-time with reactive approaches that deals with the analysis of the underlying infrastructure to assess an incident in order to provide a more holistic and integrated approach to incident handling.
- Usage of big data, machine learning and artificial intelligence techniques and technologies for the extraction of patterns in data and the identification of abnormal behaviors.
- Novel techniques for ensuring the secure distribution and storage of all incident related artefacts in order to protect them from unauthorized deletion, tampering, and revision.
- Integration of state-of-the-art elements for risk prediction related to the occurrence of threats, sensor/platform allocation, and communications
- Methodologies from the tactical to the strategic level to maximise the effectiveness of assessment for decision making.
- Development of innovative decision support systems for maritime security involving different communities; integrating of decision support tools in operational environments (i.e. in legacy systems); research efforts in artificial intelligence applicable to security decision support systems.
- War games methodologies supported by tools to test scenarios and conflict situations to support the decision making process in the maritime domain.

Profession/Role <Anonymized>

Organisation <Anonymized>

Gender <Anonymized>

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity

- ☐ Medical Data Exchange
- X Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

- I can vouch for the importance of trust in the govenment and user friendly public e-services.
- Opening public data to allow startups/developers to build apps whilst maintaining trust is a balance that is tough to achieve (ex. Kivra app in Sweden).

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

- In Sweden, mobile ID is used to access public sector services and third party apps. A problem that might emerge in the future in Sweden is blindly trusting the government and how the data are handled.

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

- Transparency and decentralisation.

Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

- Opening public data in EU to build cross-country e-services (ex. OOP) is step 1.

Profession/Role: Researcher

Organisation: Engineering Ingegneria Informatica SpA

Gender:Male

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity

- ☐ Medical Data Exchange
- ✓ Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.
(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

- ensure data traceability
- ensure trust of citizens in digital public services
- ensure a simple and trusty communication between citizens and the Public Administration

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements
(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

- definition of a clear procedure for data collection and management
- provision of a simple and secure authentication mechanism for citizens

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

- education and training (to increase skill of citizens)

Q5: For your selected area describe some technologies that need to be developed-deployed
(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

- blockchain
- authentication/authorization systems

Profession/Role: Researcher

Organisation:Engineering Ingegneria Informatica S.p.A.

Gender: Male

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting

- Maritime Cybersecurity
- Medical Data Exchange
- Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

1. Situational awareness
2. Sharing of information: One of the big security gaps is poor information sharing
3. A greater coordination between the operators of the public security forces and all the actors that affect the functioning of the city itself, namely those who manage transport, multi-utilities, telecommunications, but also public administration, hospitals, schools and large companies

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

1. Responsiveness: the subjects involved must warn the right people, in the right place in the city.
2. Analytics: It is essential to analyze the data collected, because this is the only way to understand how the city works
3. Public Administrations should change the way they consider and plan the safety of their citizens, moving from the culture of emergency to one of prevention, without having to intervene unprepared and at the last minute to try to save what is possible.

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

Today the mobile is represented by smartphones, but in the future screens will be used connected to glasses with augmented reality, flanked by broadband and other technologies.

Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

1. Machine learning for automatic vehicles to protect data and secure the driving
2. Blockchain in public administration

Profession/Role:…….

Organisation:…….

Gender:…….

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange
- ☐ Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

- Hardening and resilience of the ports' and maritime in general critical infrastructures to any kind of cyber-attack
- Safeguarding sensitive data and ensuring data integrity
- Ensuring the robustness of the maritime ICT infrastructures against cyber attacks.
- Improving the security and protection of maritime information systems from cyber-crime and cyber-terrorism
- Ensuring all aspects of integrity, trust and liability in ports' and maritime operations

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authenticatin, etc.).

- **Security culture within the maritime operations**: Ports and maritime supply chain providers do not have a mature cybersecurity culture. Most EU commercial ports do not adopt "Good ICT supply chain security and are not aware of emerging and interdependent cybersecurity threats and

are not prepared for catastrophic cybersecurity attacks. They do not perform regular risk assessments and they do not have incident handling strategies.

- **Lack of targeted standards and methodologies**: lack of specific tools or methodologies implemented for the specific analysis or assessment of maritime risks and their cascading effects. The existing risk management methodologies do not adequately take into account the cyber nature of the ports and the security requirements of the business processes associated with supply chains, which are nowadays ICT enabled and therefore severely dependent on intentional and unintentional compromise of CIIs.
- **Information sharing**: Port authorities, maritime supply chain providers, governments and public authorities are reluctant to share cybersecurity-relevant information for fear of losing their reputation or of compromising commercial, enterprise or national security and competitiveness. Private undertakings are reluctant to share information on their cyber vulnerabilities and resulting losses for fear of compromising sensitive business information, risking their reputation or risking breaching data protection rules. Trust needs to be strengthened for public-private partnerships to underpin wider cooperation and sharing of information across a greater number of sectors.
- **Certification**: Certification plays a critical role in increasing trust and security in products and services that are crucial for the digital single market. At the moment, a number of different security certification schemes for ICT products exist in the EU. For example, currently smart meter producers need to undergo separate certification processes in France, UK and Germany. While these initiatives prove the importance of certification, there is an increasing risk of creating fragmentation and barriers in the single market.
- **Economic Crisis: A stumbling block to maritime security**: Maritime's activities were severely affected by the most recent economic crisis. Personnel is reducing and no budget is foreseen, in order to increase the security team of the maritime operators and authorities. In particular, they are not willing to finance the security enhancements of their companies.

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

- Maritime Organizations (e.g. IMO, EMSA, ENISA, IPCSA, DGMARE) may contribute towards security awareness raising by giving presentations during various events, offering security seminars, certification courses and summer schools. Furthermore, they may use their dissemination tools (e.g. Newsletters, magazines, newspapers, social media) to inform the maritime world about emerging security threats. The insurance companies and auditors may be the main drivers in the campaign of maritime security awareness by enforcing maritime providers to comply with existing cyber and supply chain security standards (e.g. ISO28000, ISO28001, ISO27001, ISO27005), directives (e.g. NIS, GDPS) and guidelines (IMO cybersecurity guidelines)
- The compliance of all maritime supply chain providers with the security related standards (e.g. ISO28001) need to become obligatory so information sharing can be accelerated.
  With a view of the Cybersecurity Package the maritime sector can benefit towards enhancing its cybersecurity in various ways:
  - ✓ Build cooperation between ENISA and the maritime stakeholders (e.g. IMO) to establish a maritime Information Sharing and Analysis Centres (ISACs) sharing best practices and

guidance to all maritime actors on available tools, procedures, as well as getting guidance on how to address regulatory issues related to information sharing.

- ✓ NIS directive embrace the ports CIIs in order to establish an open, safe and secure cyberspace, highly contributing to coordinated prevention, detection and mitigation of risks enabling mutual assistance amongst the national competent maritime authorities. Synergies among the main actors (IMO, EMSA, DGMOVE, DGMARE, DGCONNECT, ENISA) need to be built in order to implement the CIIP and NIS directives as well as the USA, 2016H.R.3878 in the ports CIIS, and a broad group of companies or trade associations of the maritime and logistics supply chain

- Maritime Security Products need to be certified for overcoming security maritime market fragmentation and strengthening the competitiveness of the EU maritime industry.
- Build collaboration with public and private entities to develop centres for cyber-security incident handling training targeting general and maritime-specific security needs where simulation and exercise platforms will facilitate skills development. Close the cyber skills gap with hands-on risk assessments, virtual simulation of industrial attacks and incidents targeting the maritime and international supply chain digital ecosystem. Extensively using cyber-ranges (Internet-scale simulation environments-e.g. In this context, targeted training methodologies and modelling/visualization tools can help the maritime stakeholders to improve their understanding in handling complex attacks and incidents and improve preparedness and resilience in the maritime sector. This will involve realistic evidence based experiments and "capture the flag" exercises with cyber defense and attack teams pitted against each other. EU and NATO collaborate in common cyber exercises. ENISA (with its new mandate) is expanding the practical training efforts to all Member States engaging their military and civilian stakeholders.
- Develop common civilian-military maritime security centre. In Communication JOIN(2017) 450 "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"[35], the Commission announced the intention to create a cybersecurity competence network with a European Cybersecurity Research and Competence Centre. Civilian and military maritime research entities should become part of the EU network to jointly carry out research solving civilian and military cyber defence challenges (e.g. develop defensive strategies for upcoming Artificial Intelligent attacks). Build a cyber defence cluster of expertise within the European Cyber Security Network of Excellence involving military and civilian actors in order to develop common Research agendas in the common areas of interest (e.g. training, innovation, certification, procurement).
- Accelerate EU maritime digital market. Identify existing innovative EU cyber products and innovative prototypes that can meet maritime needs. Bring the two communities (ICT developers and maritime integrators) together to upgrade existing cyber products and prototypes to meet maritime requirements. Avoid double-spending by strengthening the prospects of EU civilian and military maritime industrial markets; by shaping, implementing and coordinating industrial, military and civilian maritime cybersecurity and cyber defence research and efforts (e.g. programs, activities, funds).
- Harmonise military-civilian maritime certification efforts. Assess military maritime security certification schema against civilian certification schema for cyber security and cyber defence.

[35] http://ec.europa.eu/transparency/regdoc/?fuseaction=list&coteId=10101&version=ALL

Reach consensus on certification requirements based on civilian and military usage; for the development of common Protection Profiles (PPs) for the EU cybersecurity and cyber defence products covering various dimensions e.g. privacy, security, transparency, interoperability, accountability, liability and compliance with EU directives. Encourage both communities (military and civilian) of manufacturers, developers and integrators to adopt the culture of sharing responsibilities for security by performing common conformance testing.

- Strengthen and expand the Digital Single Market (DSM). Maritime cyber security and cyber defence markets need to be considered as part of the Digital Single Market (DSM) and need to be treated as such. The Commission efforts strengthen the conditions for an open and competitive cyber market in Europe; help companies operate across borders and help Member States get best value for money in their procurements. These efforts have high impact in the facilitation and enlargement of the DSM.

Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

- New methods required that combine active approaches which are used to detect and analyze anomaly activities and attacks in real-time with reactive approaches that deals with the analysis of the underlying infrastructure to assess an incident in order to provide a more holistic and integrated approach to incident handling.
- Usage of big data, machine learning and artificial intelligence techniques and technologies for the extraction of patterns in data and the identification of abnormal behaviors.
- Novel techniques for ensuring the secure distribution and storage of all incident related artefacts in order to protect them from unauthorized deletion, tampering, and revision.
- Integration of state-of-the-art elements for risk prediction related to the occurrence of threats, sensor/platform allocation, and communications
- Methodologies from the tactical to the strategic level to maximise the effectiveness of assessment for decision making.
- Development of innovative decision support systems for maritime security involving different communities; integrating of decision support tools in operational environments (i.e. in legacy systems); research efforts in artificial intelligence applicable to security decision support systems.
- War games methodologies supported by tools to test scenarios and conflict situations to support the decision making process in the maritime domain.

Profession/Role: Senior Researcher

Organisation: Engineering Ingegneria Informatica

Gender: Female

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange
- ✓ **Smart Cities and IoT**

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

- To gain citizen' trust, e.g. by creating transparent policies around IoT data privacy and data use.
- To rationalize varied security protocols: each connected device/object may have different rules or standards for providing access, some weaker than others.

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

- The lack of common standards and policies (e.g. in governing the functioning of IoT devices: some have minimal security protocols).
- Many new devices and systems being deployed in Smart Cities, but often without adequate testing and assessment strategies to identify and mitigate the cyber risks.
- Many Smart Cities have no action plans and procedures for responding to possible cyber attacks.

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

- To develop cyber competencies and awareness program: especially the public sector often lacks workforce with the technical know-how on cyber security
- To provide useful guidelines for policy makers and city managers.

Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

- Data analytics, machine learning and artificial intelligence can help identify threats before cyber attacks occur and can increase responsiveness

Blockchain technology can offer secure, self-sovereign and trusted identities e.g. to certify IoT devices on the network

Profession/Role: Senior Researcher…

Organisation:…Engineering Ingegneria Informatica S.p.A…….

Gender:…Male…….

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange
- ✓ Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

- Allow individuals to have control over the use and sharing of their data
- Support the easy development of application in compliance with security and privacy regulations
- Ensure interoperability and integration of Cybersecurity solutions with existing legacy systems
- Ensure usability and user experience and reduce digital divide.

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

- Data encryption techniques
- Data control usage techniques and Data provenance
- Audit Logging

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

- Standardizations and Policies
- Education and Tranings

Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

- Blockchain
- Privacy Enhancing Technologies
- Data Sovereignity

Profession/Role:……Senior

Organisation:…CSEC…….

Gender:…Male…….

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange
- ☐ Smart Cities and IoT

The areas do not really match but i guess that IoT is the closest?

That's one of all the things we do and tell me what's not a thing and connected to the internet.

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc)

We need more young people with a deeper and more holistic technical knowledge of how computers and computer systems are designed and constructed from circuit level up to application level in combination whit the most common vulnerability and their causes and how they can be avoided. The education today is in many cases to shallow and high level.

There needs to be a deeper knowledge/understanding on how security solutions and economy are connected. What protection doctrine will be the best given the recourses and technology that they require and the recourses (including what skills people need) and technology that are available and economically reasonable. In other words what doctrine will give us best possible results both in security and the cost for products and services.

Society today is highly dependent of a few vendors of IT components. This leads to a chain of monocultures in many solutions. The consequence of this is that if one of the components break, this will make many solutions insecure in one sweep. There is a need for knowledge about the consequences for society with these monocultures and how they can be avoided.

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

There education in the area needs to be reformed to give higher technical depth. Maybe we need a new form of engineers that are educated in the same model as medical doctors i.e. a 5 years basic education followed by a period as a general practitioner and then some years of specialist education.

There needs to be more interdisciplinary research so that we understand what security doctrines we have and what the consequences of them are in terms of security, recourses and economy. And we need to do research in how monocultures impact the information security in society and how they can be avoided or what to do about them.

Profession/Role:…Data Unit Manager
Security…….

Organisation:……IT Infrastructure
Supplier…….

Gender:……Male…….

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- √Supply chain Security
- √Privacy-preserving Identity Management
- √Security Incident Reporting
- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange
- √Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.
(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

1) Systematic Security work, which is both risk based and business driven, at the supplier side is a key criteria (To have control over your own environment)
2) Bridging the gap between policy & technology: Being capable of breaking down policy documents to actual security requirements, controls, and technical implementation. (Converting the theory to real world scenarios)
3) Need for far more effective security control in practice, which do not expose us to vulnerabilities.

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements
(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

1) Need for multidisciplinary projects and a holistic security approach, considering both technical and economic aspects for achieving secure and economically viable solutions.
2) Knowledge gap, not enough security specialists available with dual understanding and knowledge of technologies and policies.
3) Lack of criteria and metrics for good security architectures and security solutions as well as for methods how to achieve them in the first place.

4) Better mechanisms to hide and/or manage complexity.

-

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

1) Internal or broader public of specialist education on security challenges. There are a lot of security programs that are however still missing some subjects. More education on security risks and limitations of modern technologies is needed.
2) Security awareness issues to be addressed by security training/eductaion: Currently, a good security mindset does not exist in all sectors. While for instances in the banking sector there is a high mindset, it is much lower in production environments, even though cyversecurity is equally important there.
3) Law makers should make more effort to address the problems above via regulations

Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

1) Authentications and authorization systems are the main challenge
2) Ways of dealing with security for legacy systems.
3) There is insufficient use of existing technologies and not insufficient technologies. There should be a correct use and deployment of the existing technologies

Profession/Role: IT-Security Manager

Organisation: Region Värmland

Gender: Male

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity
- ✓ Medical Data Exchange
- ☐ Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.
(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

As the healthcare industry is not in pair with other sectors I have difficulty to see new requirements, as I think it is important to start with the base before going too much forward, hence these are not new requirements, but they still need to be fulfilled better:

Access control: More strict access control, following principles of least privilege, removing privileges no longer needed.

Today most organisations have an access model where all personnel can access all patients. According Patientdatalagen (PDL) personnel are only allowed to access patient if they are involved in the patient's treatment.

This is not a new requirement, but the healthcare side is behind in this area and are relaying on log control, to fill the gap of what is possible and what is allowed. This is not enough according to Datainspektionen.

(Health Care personnel is not very interested to promote more access restrictions and take patient privacy as a reason).

How to solve this is difficult and one prerequisite is that the business works more process oriented, this could hopefully make the need of access more predictable.

Logging: More efficient logging, that is automatic and intelligent.

Today most organisations have an access model where all personnel can access all patients. According Patientdatalagen (PDL) personnel are only allowed to access patient if they are involved in the patient's treatment.

This is not a new requirement, but the healthcare side is behind in this area and are relaying on log control, to fill the gap of what is possible and what is allowed.

Most organisations do this in a random fashion and the result is not very efficient. This is not enough according to Datainspektionen.

SIEM tools are starting to be used but the development of use cases and reports is today cumbersome, and it goes slowly forward. AI is likely to be adapted in this field.

SIEM in practice mainly target outsider attacks that are easy to detect. However, insider attacks violating the least privilege principle in health care are difficult to detect, e.g. if a doctor from a department other than the one treating the patient was allowed to look into a patient file or not. No best practice solutions for SIEM in eHealth exist yet.

Authentication: Easy and secure ways to authenticate

Today's methods for authentication is not fast and easy enough and are perceived as cumbersome by the healthcare personnel.

Due to this fact it is common that the personnel finding ways to avoid reauthentication, e.g. by sharing login, not login out, etc.

Patient DataLagen requires Multi Factor Authentication, but this is not always used by organisations and in many cases, it is not even supported by the vendor.

Two factor authentication is widely used but not everywhere due to the fact that some systems still do not support it or personnel does not accept it.

A single sign on environment is needed with easy login and easy logout.

However, there are also problems with legacy systems.

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

Access control:

It is difficult to predict which patients a user (healthcare personnel) needs to access. A more process-oriented workflow would help to identify departments, personnel roles and patient groups to be used for modelling access control.

Logging:

It is in many cases quite easy to define which use cases that are not allowed but how to implement them in a SIEM as more difficult and in many cases the data needed is lacking. The process is slow and cumbersome.

The way of implementing use case needs to be simpler and more efficient.

Example of use case that is easy to define but difficult to build: It is not allowed to open a neighbour's journal, unless you are involved the treatment of that person.

Authentication:

The authentication needs to be secure, but easy to use.

The system vendors need to support better methods for authentication.

The workplace for healthcare personnel consists of many different components e.g. different devices and different systems. The authentication solutions need to be standardised in order to work more seamless for the personnel and for example support SSO.

The different components need to consider and support the complete workflow of healthcare and each component need to be built to fit into the big picture and not as in isolated item.

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

Vendors needs to be better in cybersecurity in general and needs be better at secure coding, privacy by design and privacy by default.

More education about cybersecurity for engineers. Engineers only think of system functionality or other quality terms such as performance but usually not of security. There is especially a lack of competence at the vendor's part, as vendors often do not understand the issue, even though the GDPR has helped to improve the situation.

GDPR helps vendors to focus more on security issues especially (PBD)

Standardisation and regulations concerning certification for cloud service providers within healthcare is needed. *For example, it should be required that all providers of a certain information class / risk class need to be certified according certain requirements.*

Today many organisations put a lot of time, effort and money trying to decide if a service is legal and secure to use or not. In many cases the analysis is not correct due to lack of competence.

Also, legislation concerning cloud services needs to be clarified, especially how to relate to EU external legislation e.g. Cloud Act, causes concerns and is an obstacle for digitalisation.

In practice, there is a need for a checklist with requirements for using a cloud service. Cloud provides need to provide good information for working out a data processing agreement. It is however more difficult to follow-up and check whether the agreement is followed. Therefore, it is good to have 3rd party certifications and re-certifications to check that the checklist/requirements are fulfilled.

Secure, fast and easy authentication

Needs to fit into the overall workflow.

-

Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

Again, I think it's more about maturity in the security field, more processes and people, but of course technology helps.

AI for log-analysis

That can make use case implementation easier or even automated. Products exist in the generic case for cybersecurity (anomaly detection) and needs to be adopted for this special case.

Authentication

Secure, easy, fast. Needs to fit into the overall workflow.

Many different use cases, e.g. personal/shared desktop, shared mobile device, personnel in surgery clothes, etc.

Profession: Professor– specialized on Health Informatics & Information Security

Organization: University

Gender: Female

Q1. Select which of the following application areas is closer to your line of expertise

Medical Data Exchange

Q2. For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

1. The main requirement would be creating trust in in eHealth systems medical data exchange. Many incidents many incidents on how patient information is mis- handled have been reported in the media (such as 1177), which have challenged trust.
2. Secondly, there are governmental requirement to be implemented, e.g. from the NIS Directive, which will play an important role in future. Here, the problem is how to implement the requirements in an appropriate way.

3. Thirdly, there are requirements from the public that is getting a higher awareness regarding security and privacy in medical data exchange. In that sense, GDPR has helped increase public awareness.

Q3. For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements.

The first thing would be the increased knowledge on security. There is a need to increase competence and knowledge at all levels: In particular, security competence and awareness of the security needs to be increased at management level.

Moreover, there is a need for a secure development process for both networks and systems, based on Privacy by Design (as already required by the GDPR) and Security by Design.

In addition, a sustainable and systematic approach to Cybersecurity as well as Information Security Management Systems need to be implemented in Health Care. Yet, security issues are rather addressed ad hoc than systematically. For a systematic approach, we should first know do a risk-assessment for the information to be processed, classify then information, then implement appropriate security controls, conduct evaluations, educate personnel and implement follow-up measures.

Q4. For your selected area describe up to three cybersecurity-related capabilities that need to be developed

1. Education and trainings on all levels and, with a focus on the management side of healthcare system that need to take decisions.
2. Research is needed to understand why Cybersecurity is so hard to implement in health care? Not only research on technology is needed, but also research on the non-technical, organizational security perspective.
3. Maybe more regulations from the governments are required. GDPR is a good example of a regulation that has put much pressure.

Q5. For your selected area describe some technologies that need to be developed-deployed

- Authentication/Authorization policies. Improved the secure authentication based on multiple factors needed Example: SIQS cards, two-factor authentication, has been implemented in some systems. However, still many password-based systems are in use.
- Crypto solutions on both data at rest and data in transfer. Moreover, the development of crypto solutions for allowing the analyses on encrypted data needed.
- Patient record systems need to be improved, as the current systems do not look on privacy and security of information exchange.

Profession: Software Engineer

Organization: Italian Software company dealing with eHealth applications

Gender: Female

Q1. Select which of the following application areas is closer to your line of expertise

Medical Data Exchange

Q2. For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(1) Obtaining consent and enforcing data subject rights in compliance with the GDPR. Most companies processing personal data are not prepared to collect and store data in a GDPR compliant way allowing to enforce data subject rights
(2) Technical security measures if high amount of data (eg for genetic data) needs to be stored in the cloud. Not clear for companies what appropriate security measure are.
(3) Data exchange between cooperating companies that have different rules and regulations.

Q3. For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements.

The first thing would be the need to help technical people to understand the legal rules. They need to understand how to enforce the consent in an easy way and legally compliant way.

Next for the store and process of the medical data, it is not clear what appropriate/adequate security mean in different contexts. For instance: the regulation asks for the anonymization of the data in cloud, but there is not a clear way how to anonymize it. Companies should be helped in this direction.

Other than that, in the context of the exchange of data, there is a lack of standardization how the data is exchanged between the national contact points in different countries. It is essential to find a way to standardize the communication between the national contact points.

Q4. For your selected area describe up to three cybersecurity-related capabilities that need to be developed

4. Training of non-technical people about the risks and basic threats for data breaches. Even that we have the GDPR with special protection needs for sensitive data, sometimes the personnel do not understand that they are endangering patients' privacy (Keeping the doors unlocked and not logging out accounts, or chatting about patients' data on a whatsapp group).
5. Understand more about the countermeasures that need to be applied to protect the data (ordinary developers might not understand the latest technologies for implementing security policies).

• Q5. For your selected area describe some technologies that need to be developed-deployed

- Authentication/Authorization need to be deployed
- Architecture for outsourcing sensitive data in a safe way without compromising it.
- Architecture for keeping personal data updated. This is especially a challenge for genetic data processing. Right now we only know at about 1% of what genetic data means and how it can be interpreted. New interpretations of genetic data and conclusions in drawn from it can constantly change requiring an update of the patient's medical profile..

Profession: Scientist

Organization: AIT

Gender: Male

Q1. Select which of the following application areas is closer to your line of expertise

Privacy-preserving identity management

Q2. For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

The main requirement would be to simplify privacy-preserving IDMS, and not try to fit all the features in the same system. Current privacy-preserving IDM solutions developed by the research community, such as Idemix that are user-controlled, are too complex and require different user action to obtain and handle credentials, which users will not be able to easily understand and handle. Also, running Idemix on smart devices poses challenges.

On the other hand, existing IDM solutions in practice lack strong and end-to-end authentication, which should be the main goal.

We should step back from theory and rather address practical requirements that make suitable trade-offs, which are efficient with good enough privacy guarantees, simple and understandable. Examples of good trade-off solutions are Cloudflare, Privacy Pass or ABC for the cloud (ie, the approach taken by the CREDENTIAL project), where an intermediary in the cloud run everything on behalf of the user with good-enough privacy guarantees..

Q3. For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements.

The most essential one would be to take a step back from the theory and to identify practical requirements.

Then, solutions addressing real-world needs have to be made available and usable for users.

Q4. For your selected area describe up to three cybersecurity-related capabilities that need to be developed

1. Raising awareness is key, in particular awareness of non-technical people to understand what the online privacy problems and threats are, what and how everything works.
2. In addition, there should be pressure from policy intervention. For example, for today's public transport systems often cheap mobile phone based, privacy-invasive solutions are in use, which allow user tracking, even though practical PETs could be used for enhancing privacy. Policy intervention could in such cases require privacy-preserving identity management solutions.
3. There is a need for open-source, which provide PET implementations in good quality and are easy-to-use tools for developers

Q5. For your selected area describe some technologies that need to be developed-deployed

1. Adoption of cryptographic privacy-enhancing technologies.
2. Cloudflare & Privacy Pass solution are good example to use in some other fields.
3. Reusable Open Source implementations of PETs and privacy- preserving crypto blocks are needed, which can be easily be adopted in current identity management systems.
4. Research is needed on taxonomies & architectures for privacy-preserving identity management systems. In particular, for IoT environments with restricted devices, there is a need to develop usable, more decentralized, distributed idm technologies, where the handling of credentials may be outsourced to a potentially trusted intermediary.

Profession/Role: Cryptography Researcher

Organisation: Large company Research

Gender: Female

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- √ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange
- ☐ Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

There is a need to construct the IDM in a strong privacy-preserving and easy to use. The core challenge is to satisfy all the following requirements at the same time:

- *strong privacy protection & authentication*
- *no single point of failure or trust*
- *usability, ie choice to be privacy-preserving and should be easy to use).*

Most technologies that already exist satisfy only two out of the three requirements above. For instance, identity mixer (Idemix) provides strong privacy but it is not easy to use and one still needs to trust third parties (IdP or revocation/escrow agent), which is a trade off.

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

1) ***Looking for a more distributed privacy-preserving systems (Distribute the trust in single sign on)***
2) ***Find a (usable) way to manage strong authentication keys for the end users that can be memorised***
3) ***Having good implementation (There a lot of good solution from research on papers but they are not implemented in practice yet)***

Interview Form

(All questions are voluntary):

Profession/Role: Faculty Manager (Service support to academic product delivery)

Organisation: Stellenbosch University

Gender: Male

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☒ Supply chain Security
- ☒ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange
- ☐ Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

Staff access to cyber services: 1) access to internet; 2) access to secure core information and training platforms; 3) access to secure administration systems for production and financial administration.

Protect data storage and retrieval process to prevent unauthorized access.

Access for authorized personnel to network storage while off-site.

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

Integrated authentication of single user profile for various access points.

On site vs Cloud based storage blend.

Imbedded encryption for point to point users accessing sensitive and personal information.

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

Hardware upgrade of existing port IT network to accommodate appropriate software.

Training for users and network administrators to manage accessibility.

Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

Authentication system for physical access to facilities as well as login verification.

Integrated safety systems with imbedded redundancies.

System security training on use of systems and protection of accessed data.

Profession/Role: INFORMATION SECURITY OFFICER

Organisation: Anonymised

Gender: MALE

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management

X Security Incident Reporting

- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange
- ☐ Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

- Inclusion of the security culture to the engineering of products and services (in our case specifically of the railway sector)
- IoT identity.
- Industrialization of security protection (automation on identification of ongoing threats and their response and mitigation).

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

- Framework for standardization of products and services for the railway sector
- Improvement of the training of Cybersecurity professionals
- Inclusion of cybersecurity and privacy by default and by design

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

- Training
- Resilience
- Alignment with the current national and railway sector legislation.

Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

- Situational awareness
- Threat hunting
- Improvement of the intelligence of Cybersecurity that includes the continuity use and generation of IOCs.

Profession/Role: R&D and Innovation

Organisation: BEIA Consult International

Gender: Male

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security

- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange
- x Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.
(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

In the area of Smart Cities it is important to get data securely in near real time and enable automated actions

Also, in Smart Cities it is important to certify that data from sensors is not being manipulated

In the area of IoT it is important to enable people to share the data in a traceable and transparent way

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements
(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

In Smart Cities one such problem is to ensure quality of service for time critical applications and in the same time end to end encryption

Another problem to solve is integrity of data, maybe using blockchain

In IoT one problem would be to have a marketplace where you can manage your personal data.

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed
(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

For smart cities test beds using real time cloud processing should be developed.

Also, blockchain or quantum capabilities should be developed

Furthermore, a IoT marketplace should be developed.

Q5: For your selected area describe some technologies that need to be developed-deployed
(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

Blockchain, multi-actor marketplace, quantum security

Interview Form

(All questions are voluntary):

Profession/Role:……CFO…….
Organisation:……OCEANIC MARINE SERVICES…….
Gender:……FEMALE…….

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange
- ☐ Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

Reply

Satellite and radio communication
The specification of the satellite link should be considered when establishing the requirements for onboard network protection.

Wireless access control
Wireless access to networks on the ship should be limited to appropriate authorized devices and secured using a strong encryption key, which is changed regularly.

Malware detection
Scanning software that can automatically detect and address the presence of malware in systems onboard should be regularly updated.

Secure configuration for hardware and software
Only senior officers should be given administrator profiles, so that they can control the set up and disabling of normal user profiles. User profiles should be restricted to only allow the computers, workstations or servers to be used for the purposes, for which they are required. User profiles should not allow the user to alter the systems or install and execute new programs.

Email and web browser protection
Email communication between ship and shore is a vital part of a ship's operation

Data recovery capability
Data recovery capability is the ability to restore a system and/or data from a secure copy or image, thereby allowing the restoration of a clean system. Essential information and software-adequate backup facilities should be available to help ensure recovery following a cyber incident.

Application software security
Safety and security updates should be provided to onboard systems.

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements
(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

Reply

IoT threats
Insecure web interfaces and data transfers, insufficient authentication methods, and a lack of consumer security knowledge leave users open to attacks.

Serverless Apps Vulnerability – Cloud-based services
Customer information is particularly at risk when users access your application off-server — or locally — on their device. On-server, when the data is stored in the cloud rather than the user's device, you have control over that information and the security that surrounds it.

Ransomware
Threats take a computer, and sometimes even entire networks, as hostage. Often, all the files and data previously stored on a system become inaccessible until the victim (i.e. someone in the workplace) hands over a ransom fee, typically paid in cryptocurrency like bitcoin.

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

Reply

- Conduct frequent cyber risk assessments.
- Implement sensible data security safeguards and monitoring systems: Use data encryption, multi-factor authentication, or a disaster recovery as a service solution.
- Create a framework for ongoing threat management, operational oversight, risk management, and regular reviews of contracting businesses with whom you've partnered; document plans to handle threats and mitigate the impact of attacks with a data backup solution in place
- Continuous training of users.

Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

Reply

- Hardware authentication. The inadequacies of usernames and passwords are well known. Thus, a more secure form of authentication is needed.
- User-behavior analytics. The technology uses big data analytics to identify anomalous behavior by a user.
- Data loss prevention. A key to data loss prevention is technologies such as encryption and tokenization.
- Deep learning on artificial intelligence and machine learning.
- The cloud, such as virtualized security hardware, virtualized firewalls, and virtualized intrusion detection and prevention systems.

Profession/Role: Researcher

Organisation: NuCypher Inc.

Gender: Male

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management ←
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange
- ☐ Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

- Foster trust and adoption of privacy-preserving technologies
- Increases citizens' control over their data
- Reduce centralization of personal data storage

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

- Improved user experience for privacy-preserving technologies
- Prevalence of end-to-end encryption solutions as a default
- Secure data sharing and processing over encrypted data

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

- Increase public awareness in threats to their own privacy
- Stringent regulations on privacy protection

Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

- Improved proxy re-encryption schemes (e.g., collusion-resistance)
- Efficient fully-homomorphic encryption

Profession/Role: Communications and Marketing

Organisation: Global Cyber Alliance

Gender: male

Q1: Select which of the following application areas is closer to your line of expertise:

- **Open Banking Security**
- ~~Supply chain Security~~
- ~~Privacy-preserving Identity Management~~
- **Security Incident Reporting**
- ~~Maritime Cybersecurity~~
- ~~Medical Data Exchange~~
- ~~Smart Cities and IoT~~

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

In both areas, the management of private data will be a key concern.

For Open Banking Security, the exploitation of private data will become a business engine for new developments (big data, aggregation of data, modelling, customised advertising, CRM, human-machine interaction…), but also a profitable target for fraudsters and e-criminals.

In that sense, we could name several cybersecurity requirements, such as cloud-computing protection, sound encryption techniques, new strong-authentication techniques, biometric data protection, social-engineering prevention techniques…

In the field of Security Incident Reporting, those data will need to be properly protected (with an adequate understanding of policies such as GDPR) so that the restrictions to their management do not hinder an efficient exchange of information or the capabilities of both the authorities and the corporations to fight e-crime activities.

This will require the development of automated trust-building technologies (most surely, based on a combination of blockchain and encrypted-data analysis) and of new certification models. Also, the already high volume of data on incidents will increase, and good analysis techniques will become a must. Automated models according to the intelligence-cycle model will become a priority in the future.

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

For Open Banking Security:

- Private Data Protection (also against malicious big data or data aggregation techniques)
- Social Engineering Prevention and Awareness
- Multi-platform Security

For Security Incident Reporting:

- Automated Trust Building
- Securing Data Exchange
- New Analytics

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

For Open Banking Security:

- New approaches to data storage (Data Architecture, Encryption, Modular Access…)
- Education (at all levels: from the employees to the most vulnerable clients)
- Interoperability in Secure-By-Design approaches

For Security Incident Reporting:

- Multi-disciplinary approaches to trust-building (IT can't be the only solution)
- Development of techniques combining blockchain and encryption
- Education and research in data analytics (operators need to be upgraded to analysts)

Q5: For your selected area describe some technologies that need to be developed-deployed

For Open Banking Security:

- Proactive data protection techniques (for instance, automated data-leakage checking)
- Automation of the concept of humans-as-a-security-sensor
- Secure-design standards

For Security Incident Reporting:

- Multi-layer certification, fast vetting techniques
- New algorithms for data exchange (self-certified processes)
- Artificial Intelligence models for data analytics and visualisation

Profession/Role: Cybersecurity Research and Innovation

Organisation: Telefonica Digital España

Gender: Masculine

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange
- ☐ Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

- Improved two factor authentication mechanisms.
- Enhanced real-time security during navigation, both preventive and reactive.
- Robust post-quantum algorithms.

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

- Better non-intrusive mechanisms to help individuals to adopt security inadvertently.
- Raise awareness between users about the security risks and privacy concerns.
- Help researches with the necessary infrastructure and resources to let them work freely without pressure into complex scientific fields such as quantum cryptography.
-

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

- Improve machine learning and deep learning techniques to manage, in a unmanned way, real cybersecurity operations
- Better dialog between industry and academia in order to make effective transference of knowledge, and support that kind of actions at European level.
- Penalize mayor companies who mock about laws and user's rights regarding security and privacy of their private information such as Google or Facebook.

Q5: For your selected area describe some technologies that need to be developed-deployed
(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

- Post-quantum resistant technologies
- Unified IoT paradigm with real cybersecurity and privacy considerations.
- Private-Public global sandbox infrastructure ready to launch cybersecurity experiments to reproduce malicious activities and learn from them.

Profession/Role: Analyst

Organisation: European Border and Coast Guard (Frontex)

Gender: Male

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management

X Security Incident Reporting

- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange
- ☐ Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.
Far-reaching protection from intrusion by state and non-state actors to safeguard sensitive information (essential to facilitate information-sharing by security actors). Simple authentication for user and connectivity to other secure systems of cooperation partners.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

In particular the duration it requires to obtain national security clearances for the necessary personnel to maintain infrastructure etc is a challenge.

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

Crucially training for the safeguarding of the systems and correct use thereof.

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

Q5: For your selected area describe some technologies that need to be developed-deployed

I am unfortunately not competent in the exact nature of technologies that would best serve to secure the IT infrastructure to the extent that sensitive information can be safeguarded.

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

Profession/Role: R&D

Organisation: Schneider Electric

Gender: Male

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange
- ☐ Smart Cities and IoT (X) (Smart Grids)

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

- Secure access to the Smart Grid devices
- Secure communications between control center and field devices
- Event management
- Detection and prevention mechanisms for the substation

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements
(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

Legacy devices don`t allow security mechanisms

Real time (availability) is a must

OT environments with IT security problems

IT security mechanisms don't work in OT environments

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed
(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

Industrial protocols with secure profile

Detection-prevention security mechanisms in the field devices

IT security mechanisms adaptation to OT environment

Q5: For your selected area describe some technologies that need to be developed-deployed
(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

Include new technologies (blockchain, AI, bigdata, etc) in the Smart Grids

Profession/Role: Cyber Threat Intelligence

Organisation: MNEMO

Gender: Male

Q1: Select which of the following application areas is closer to your line of expertise:

Open Banking Security
Supply chain Security
Privacy-preserving Identity Management
X Security Incident Reporting
Maritime Cybersecurity

Medical Data Exchange
Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

- **Threat Hunting Team**: Have teams focused on threat hunting for the rapid and proactive identification of new threats.
- **Threat Intelligence Team**: Incident Response teams must have Threat Intelligence teams that are capable of developing possible potential attack scenarios for a group of cyber criminals and generate hypotheses about incidents that have already occurred.
- **Tools that allow automation**: Different types of tools which allow a series of actions to be carried out automatically, especially focused on the analysis parts of an incident.

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

- **Lack of qualified personnel**: There are not many people trained in Spain in Incident Response or Threat Intelligence issues.
- **More flexible Incident Response cycle**: The Incident Response cycle should be more operative to streamline the different activities carried out in it.

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

- **Intelligence**: The incident response analysts should know intelligence methodologies for intrusion analysis. Methodologies such as F3EAD, OODA Loop, Cyber Kill Chain and the diamond model. This will allow to attribute the different intrusions to possible countries and / or actors.
- **Investigation**s: Carry out research on tools that exist in the market and adapt them to the needs of an Incident Response Team so that the response times to an incident are as short as possible
- **Training in Threat Hunting**: Training in Threat Hunting with the aim of knowing the main characteristics of this modality when it comes to identifying possible indicators of commitment in a proactive manner.

Q5: For your selected area describe some technologies that need to be developed-deployed

- **Tools for extracting entities and the relationship** between them by similar characteristics would serve and facilitate the work of Incident Response teams when analyzing incidents.
- **Remote forensic analysis tool**, on equipment that is not located geographically in the same place where the incident response equipment is located.

Interview Form

(All questions are voluntary):

Profession/Role: Researcher / Lecturer

Organisation: Faculty of Military Science - Stellenbosch University

Gender: MALE

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☒ Maritime Cybersecurity
- ☐ Medical Data Exchange
- ☐ Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

① Education and training

② Members operating in and around the maritime domain will have to be trained on the threat and possible counter measures.

② Development of hard- + software to combat cyber threats.

③ the identification of persons | groups | organisations who are responsible for such threats.

- working groups
- establishment of international groups
- conferences | seminars

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

① The identification and bookmarking of the possible threats in the maritime domain. Formalising education/training.

② Better encryption of data in order to ensure safeguarding of data.

③ Better protection measures or protocols for hardware eg unmanned ships and submarines.

④ Also physical protection measures where unmanned equipment is in use.

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

1. Physical counter measures
2. Education / training carricula.
3. Research groups / think tanks focusing on the cyber maritime domain.
4. Governance structures on the highest level to the lowest. eg UN / AU / Regional / national.

Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

1. Maritime domain awareness systems - including integrated displays.
2. Training systems.
3. Satellite connectivity for data management.
4. Training on the use / abuse of algorythms.

Profession/Role:

Organisation: JTSEC Beyond IT Security S.L.

Gender: Male

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange
- ☐ Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

Security Awareness of the final user

SecDevOps

Cybersecurity Certifications

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

- Security Updates – Patch Deployment
- Security Awareness in the development

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

- Cybersecurity Certification Framework
- Cybersecurity Requirements by the Regulators

Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

Certified and secured platforms to allow quick and secure development of products

Profession/Role:……Security ……

Organisation:……INDRA……

Gender:……MALE……

Q1: Select which of the following application areas is closer to your line of expertise:

- ☒ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange
- ☐ Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

Maintaining secure credentials, applying Best practices to security governance and to Infrastructure, especially in third party cloud, and finally analyze security data from a threat intelligence perspective.

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

Improve access control with strong authentication and identity federation for the users

Improve the cybersecurity data analysis by means of Threat Intelligence

Improve the response to threats either internally or the way to communicate with other stakeholders or suppliers.

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

Training and awareness in an effective way, really focused on the person

Classification of information and gathering of data and sharing o geopolitical information to detect spear attack to our business.

Make security configurations a lot easier either for the technicians and for the regular user.

Q5: For your selected area describe some technologies that need to be developed-deployed
(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

- Situational awareness and training
- Blockchain technology
- A Unified

Profession/Role:

Organisation: Idfy Norge AS

Gender: Male

Q1: Select which of the following application areas is closer to your line of expertise:

X **Open Banking Security**

- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange
- ☐ Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.
(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

- For the area of Open Banking, it would be desirable to be able to create user-centric decoupled authentication flows, in the way that the user should not need to authenticate towards each and every bank to fetch and exchange data, but rather through a federated solution (using e.g. eIDAS notified electronic ID schemes trusted by all parties) outside of the bank itself. This would likely require a commonly recognized token scheme which is trusted by the different parties, e.g. with OpenID Connect/OAuth2 type of authentication/authorization flows. It is unclear as of today

which parti(es) could take such a role, but we believe that establishing such a solution could open many new possibilities within the Open Banking area.

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

- For the Open Banking area, we would have to solve the challenge of establishing a common scheme which can be trusted by all parties. I.e. one could use authentication schemes in the form of strong electronic IDs (as defined by eIDAS, e.g. eIDAS substantial and/or high assurance level), but an unsolved problem is to be able to perform the authentication part outside of the bank, but in a way that the bank (and all banks) still can recognize and trust

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

- Research into token exchange schemes, encryption, authentication/authorization and electronic signatures
- Policy interventions in order to further harmonize between regulations such as PSD2 and eIDAS (which probably ideally should be more closely linked than they seem to be today)

- ### Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

- Work would have to be done within the authentication/authorization field, in order to create a more harmonized solution building upon the concepts set out by e.g. the eIDAS regulation. Could it e.g. be possible to extend existing protocols (OAuth2/OpenID Connect) and link them to eIDAS concepts, to achieve the goal of decoupled authentication? Then extensions and new systems around the authentication/authorization parts would have to be developed, deployed and recognized by the different parties in the value chain (both eligible third parties and banks).

Profession/Role: Army Officer – Signals , Cybersecurity

Organisation:NATO

Gender:MALE

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange
- ☐ Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.
(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

- Link the Security Incident Reoprting with Cybersecurity Awareness Tools
- Produse Security Incident Reporting Repository and Registry to assess the incident and consider it as a stand alone incident or as a part of a serial of incidents related to a plan for a cyber attack
- Use Security Incident reporting to do vulnerablity assement , assess the need for reaccreditation of a CIS and identify the need for additional training for the personel dealing and using CIS.

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements
(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

- CIS Security Policy needs to be always updated and applied without any exception to all CIS in order to minimize the number CIS Security Incidents and mitigate the impact they will have to the Cybersecurity
- All CIS need to be accredited, audited and inspected no matter the availability of the necessary resourses to lower the risk for CIS Security Incidents which affect badly the Cybersecurity posture
- The "need to know" rule should be applied for the desimennation of sensitive information to minimize the number CIS Security Incidents and leackage of sensitive information in the Cyber domain.

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed
(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

Cyberdefence Situational Awareness Tool with Security Incident Reporting Registry

CIS Security Policy for the Cyberdomain Security Incidents

Q5: For your selected area describe some technologies that need to be developed-deployed
(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

Situational AwarenessTool

Multi Level Inforamtion Assurance CIS to follow the "need to know" rule

Profession/Role:……Cybersecurity …….

Organisation:……Vicomtech…….

Gender:……Male…….

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security

- Supply chain Security
- **Privacy-preserving Identity Management**
- Security Incident Reporting
- Maritime Cybersecurity
- **Medical Data Exchange**
- **Smart Cities and IoT**

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

PPIM

- That the systems I access allow me transparent access and stop using keys when possible
- How can I really know who has my data and what is doing with them?

MDE

- That my patient records are unified and accessible to any health professional, anywhere, both public and private.
- Never repeat a test because access to raw data captured is not available

SCIoT

- I do not want to feel watched or controlled
- I want to have all and accurate information to make the best decision at every moment

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

PPIM

- Achieve complete interoperability between identity systems, which follow very different technical standards
- Access information securely without destroying the business model of the organizations that use it

MDE

- The availability and integrity of data depend to a large extent on a format that is not globally standardized.
- The cost associated with obtaining the information cannot be ignored, so secure accounting tools must be used to guarantee correct operation.

SCIoT

- Systems allow capturing information that identifies people against their will.

- Some of the information you may need is not directly accessible to you, or you do not have the necessary permissions to access it.

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

PPIM

- Standardization and tools framework need to be developed to share a basic infrastructure.
- Interventions in the policy of access to data and education. Turn it over so that it is the user who stores who has been given information

MDE

- Research and education for citizens.
- The most accepted AAA systems are usually centralized, in this case a system shared by all those affected is convenient.

SCIoT

- Information management to guarantee the privacy requirements of each person
- Training and the ability to establish specific contracts to access information when necessary.

Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

PPIM

- Digital Identity Systems

MDE

- Authentication, Authorization and Accounting (AAA)
- Distributed Ledger Technology (DLT)

SCIoT

- Privacy Awareness
- Blockchain

Profession/Role:……Cyber Security Sales……..

Organisation:…DEKRA DTC…….

Gender:…….

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security → **X**
- ☐ Privacy-preserving Identity Management → **X**
- ☐ Security Incident Reporting → **X**
- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange → **X**
- ☐ Smart Cities and IoT → **X**

We cannot define only one area described. DEKRA DTC it is a company where we have accreditated labs where we can certificate all kind of products

The company is accredited under the CCRA terms in the Spanish and Turkish schemes for the latest Common Criteria version and also by the USA NIST Cryptographic Module Validation Program (CMVP) and the Japanese Cryptographic Module Validation Program (JCMVP) for FIPS 140-2 and ISO 19790 testing, respectively. It is also the only accredited evaluation facility to perform "Hardware Devices with Security Boxes" evaluations at the SOGIS technical domain in the Spanish Scheme.

So we can cover transversely all areas certificating the different elements in hardware or software comprising those different spaces.

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.
(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

In the different areas, we think the three more important points are:

• Assure all connected elements. All products with a kind of connection must be safe to preserve the integrity of the product and the security of people.

• To Accredit than all products deployed in cities, cars, and other elements comply with the security descriptions that they decide for the product and comply with the current regulations.

• To have encryption access to assure the identity of the users and protect access to the devices

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

Vulnerabilities in access to:

- Devices. In hardware matters, it is necessary to protect devices intelligence and the edge processing
- Communications. Protect the device initiated connections and messaging control.
- Data storage. Secure the cloud and the identification, authentication and encryption.

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

- Apply regulations in safety matter
- Make proofs of penetration testing in devices to discover vulnerabilities
- Mentalization that all the products around us, must comply with the security that the manufacturer says they have

Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

- Encrypted Access
- Strong authentication

Profession/Role:…Certification and Quality

Organisation:…Safelayer Secure Communications S.A

Gender:…….

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange
- ☐ Smart Cities and IoT

➔ Products on Public Key Infrastructure (PKI) and digital signature.

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

➔ Remove existing barriers to the cross-border use of electronic identification means used in the Member States to authenticate.
➔ Define a security framework for the use of qualified trust services (including issuance of qualified certificates, signatures, seals and time stamps)
➔ Define a security framework for the use of remote electronic signature, where the electronic signature creation environment is managed by a QTSP (Qualified Trust Service Provider).

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

➔ Relationship between the eIDAS Regulation and the EU Cyber Act.

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

➔ Definition of the certifications needed for the PKI (Public Key Infrastructure), Trust Services Providers, Time Stamp products and Digital Signature areas.

Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

Profession/Role: CyberSecurity Lab

Organisation: DEKRA

Gender:Male

Q1: Select which of the following application areas is closer to your line of expertise:

- ☐ Open Banking Security
- ☐ Supply chain Security
- ☐ Privacy-preserving Identity Management
- ☐ Security Incident Reporting
- ☐ Maritime Cybersecurity
- ☐ Medical Data Exchange

X Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

1 – Interoperability: Nowadays, several different approaches are used for developing IoT devices. Systems cannot communicate with each other. The need to define a new standard for data communication and share data across different platforms.

2 - Certification: Different certification schemes have been defined for IoT devices exists, some based in complex certification procedures like ISO 15408 (CC) or more basic like CTIA IoT Cybersecurity Test plan. In addition to this, security guidelines and best practices exists like GSMA IoT Security Guidelines, CSA IoT Security Controls or IoT Security Framework. However, there is no clear winner in this battle at the moment.

3 - Privacy: Irresponsive information usage by devices manufacturers could be a risk to the user data including health devices handling sensitive data.

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

1. Basic security issues: We have analyzed several IoT products manufactured by well know brands that have multiple basic vulnerabilities. We are not talking about complex attacks, it is about things like: hidden configuration pages, default passwords, vulnerable services, no encryption,... Some kind of certification or label for products should be put in place at least for covering a minimum set of tests. Maybe something like CTIA IoT Cybersecurity Test Plan.

2. Lack of standarization: each manufacturer is defining their own infrascture and platform without thinking in integrations or interoperability. In addition to this, IoT devices usually do not have any mechanism for identification and it is difficuly to include them in asset management tools.

3. Data privacy risks: Due to the firs point, there are several risks related to the way that data is storaged in IoT devices. When analyzing IoT devices usually only mobile application or cloud services are analyzed. However, hardware analysis (including firmware) should be included as well. Sensitive data could be stored physically in this kind of devices and it could be easily extracted sometimes. In addition to this, we have seen some low budget devices that usually are sending a lot of user data to chinese servers.

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

1. Education/Training: Not only to developers, for users as well. As mentioned previously, we have seen chinese low budget devices with multiple vulnerabilities that can be easily compromised by attackers.

2. Security Regulation: ENISA is working on defining some cybersecurity requirements at the moment. Some kind of testing should be required in order to use these kind of devices based on their capabilities, data processed and privacy requirements.

Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

1. (Semi) Automated tools for security testing: With these kind of tools, security tests will be performed easily even by manufacturers themselves. Some projects like FACT, OpenVAS and similar could help to enhance cybersecurity of IoT products in order to avoid basic vulnerabilities.

2. Threat Analysis Tools: At the end devices could be compromised. Having tools that could help developers to identify these attacks could avoid massive data exfiltration. Log and monitoring systems should be required for IoT devices in order to identify wrong behaviors.

Profession/Role:

Organisation: Private CSIRT

Gender : Male

Q1: Select which of the following application areas is closer to your line of expertise:

Security Incident Reporting

Q2: For your selected area describe up to three cybersecurity requirements that the area :
Training people what to do in case of security incident

Having the appropriate software for log correlation and having them well configured

Having the capabilities to reconstruct the network

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements will need to meet in the future.
Making people understand what is a security incident and what is not (spam, etc.)

Lack of investment in SIEM capabilities

Finding competent employees or companies

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed
Training people how to identify and react to security incident

Investment pre-crisis

Training in cyber crisis management

Q5: For your selected area describe some technologies that need to be developed-deployed
IA for log correlation

Profession/Role: CISO

Organisation: Hospital

Gender : Male

Q1: Select which of the following application areas is closer to your line of expertise:

Medical Data Exchange

Q2: For your selected area describe up to three cybersecurity requirements that the area :

Need of secured IoT devices in medical field : conception of components compliant with health security needs (HDS in France)

Security of medical images (high storage capacity needed, security complexity)

Sensibilisation of medical actors about risks and solutions

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements will need to meet in the future.

Integrated security in medical IoT

Easy-to-use authentication (through CPS cards)

Security awareness, about risks on medical data and medical infrastructures

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

- Security training and security integration for IoT suppliers and IoT security homologation or certification
- Platforms of Cybersecurity awareness training (and specific examples about risks on medical data and medical infrastructures)
- IoT homogenization (communication, encryption, etc.)

Q5: For your selected area describe some technologies that need to be developed-deployed

- IoT securization
- Awareness free platforms

Profession/Role: Consulting manager

Organisation: Cybersecurity Consulting

Gender : Male

Q1: Select which of the following application areas is closer to your line of expertise:
Through my work, I can work on several line of expertises. My main expertises are :

- Open Banking Security

- Supply chain Security

- Medical Data Exchange

Q2: For your selected area describe up to three cybersecurity requirements that the area :
Main requirements are :

- risk approach for each line of expertise, in order to address the relevant risks with the relevant solutions

- end-user awareness in each line of expertise : most of the time, the solutions deployed are not relevant as end-users don't understand why they must use them in their job ("we never had a problem...")

- homologation / certification for european cybersecurity experts in order for multi-country companies to identify relevant actors on an European level

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements will need to meet in the future.

- shared risk analysis methodology, compliant with most of the European countries prerequisites

- same security level and prerequisites in all Europe in order to be relevant on a collegial awareness platform

- "cheap" solutions for small company which can't have same budgets for cybersecurity

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

- "certification" or "homologation" of European Cyerbsecurity actors who could work on multi-country company

- global European awareness program on cybersecurity

- European cybersecurity agency, independent of all national governments

Q5: For your selected area describe some technologies that need to be developed-deployed

- free tools to help a risk approach for each actors

- security approach in project methodology and in computer schools

Profession/Role/ Consultant Expert Sénior

Organisation: Société SCASSI

Gender:… Male

Q1: Select which of the following application areas is closer to your line of expertise:

□□Open Banking Security
□□Supply chain Security
□□Privacy-preserving Identity Management
□□□Security Incident Reporting
□□Maritime Cybersecurity
□□Medical Data Exchange
□□Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

1 - The main requirement for incident response is the existence of event traceability
to explain the actions of the information system.
2 - Homogeneity of event logs
3 - Securing logs against deletion and modification

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

Not all systems necessarily generate event logs, it remains at the discretion of the administrator.
In an IOT environment, these logs are completely absent.
At the moment each event log has more or less its own proprietary recording format
without containing all the data essential to the representation of an event.

In order to ensure that the data collected can be presented before a court, it is necessary that they have the characteristic of non-repudiation.

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

In education/training on the creation of event logs with high semantic added value.
In the production of network monitoring tools, an AI-based correlation must be integrated.
The distribution of the network must make it possible to offer alternative and secure channels for information transmission and business continuity in degraded mode.

Q5: For your selected area describe some technologies that need to be developed6deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

Encryption and unalterable communication channel for the information system's survival channels.

Profession/Role:MEDICAL DOCTOR , FACULTY , RESEARCHER
Organisation:TOULOUSE university hospital
Gender:Male

Q1: Select which of the following application areas is closer to your line of expertise:

□□Open Banking Security
□□Supply chain Security
□□Privacy-preserving Identity Management
□□Security Incident Reporting
□□Maritime Cybersecurity
□□Medical Data Exchange
□□Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

1-GAIN PATIENT TRUST

- Electronic Health Record held by patient : DATA PORTABILITY
- encryption and cloud storage : LOCKERS & smart contracts

- ledger as a LIFELINE RECORD :
- ledger for smart contracts
- portable application giving to the patient the opportunity to administrate the use of his DATA

2-ENHANCE INTER OPERABILITY and DATA RE-USE through secured DATA GOVERNANCE

- ETHICAL by design : security can not be raised against patient rights
- SELF SERVICE of anonmized data
- Cloud managment and dashboard
- Cloud computing and analytics (A.I.)

3-CONSISTENCY , SECRECY and INVIOLABILITY

- consistency by CAP theorem , SECURITY by design , Access policy and document HASH
- SECRECY by encryption and smart lockers
- INVIOLABILITY and certification of E.H.R. : blockchain / ledgers

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

1-End to end encryption and melting in E.H.R.:

- from IOT
- from monitoring systems
- from lab results and imaging
- from very inhomogeneous sources and systems

2-Strong authentifications patient-firendly

- e;g; elderly

3-smart lockers Healthcare compliant in the cloud

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

1-European Union Council for cybersecurity and data exchange in healthcare

- rules the ecosystem
- regulatory trends
- monitoring the system
- make it possible through the E.U. borders
-

2-Healthcare-dedicated blockchain/ledger

- one for each patient : personal unique ID issue?
- replicated and distribuated through europe
- patient-centered where patient can administrate his own information.

3-E.U. secured Healthcare network or Database:

- based on ledger?
- Big Data COMPLIANT for ananymized data meaningful extraction (healthcare enhancement)
- A.I. development and related cybersecurity

Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

1-Helathcare dedictaed patient-centered Ledger / blockchain linked to personal digital lockers with encrypted documents

2-Simple identification software and ID verification for authentification , patient-friendly

3-Secured software /API for DATA administration by the patient himself
DATA transfert to primary care provider or trusted physician

- DATA anonymisation and transfert "on the go" for regulatory institution and public healthcare improvements
- SMART contracts through ledgers in order to get involved in medical research or pharmaceutical survey-SMART contracts for DATA monetization
- ETHICAL by design : give the total control of DATA to patient with hisghest security level possible

Profession/Role:...CYBERSECURITY EXPERT

Organisation:.....CONTINENTAL DIGITAL SERVICES

Gender:.....

Q1: Select which of the following application areas is closer to your line of expertise:

- € Open Banking Security
- € Supply chain Security
- € Privacy-preserving Identity Management
- € Security Incident Reporting
- € Maritime Cybersecurity
- € Medical Data Exchange
- € Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

Privacy

- Need to define efficient balance between end user privacy and capability to innovate

Incident reporting

- Officialize a European referential of incident typology
- Offer a centralized European CERT, open for all, with open-data APIs at least for TLP Green data sharing

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

Incident reporting

- The risk of penalty tends to refrain organizations from reporting the incidents they suffer
- The multiplicity of authorities to report incidents to is crippling the efficiency of reporting (eg in France : CNIL + ANSSI + Agence Nationale de Santé + ...) → need for a "guichet unique"

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

Privacy

And

Incident reporting

- International lobbying in order to align foreign regulations with European ones (eg "GDPR dissemination" ...) ; this would help European businesses in international competition

Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

Privacy

- Develop and offer public implementations of cryptographic algorithms such as homomorphism...
- Create a public platform operated by European authorities for identity provider (digital passport) and consent management (eg "France Connect" extended to European level and opened to private sector providers)
- Develop and certify a European MFA technology and devices

Profession/Role:.. .....

Organisation:.....LYRA.....

Gender:.....♂.....

Q1: Select which of the following application areas is closer to your line of expertise:

- [x] € Open Banking Security
- [ ] € Supply chain Security
- [ ] € Privacy-preserving Identity Management
- [ ] € Security Incident Reporting
- [ ] € Maritime Cybersecurity
- [ ] € Medical Data Exchange
- [ ] € Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

1) Safe User Experience

2) Gain customer's trust

3) High availability

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

1) Fraud Management

2) Strong Authentication

3) User privacy concerns vs security

(The most information about the customer you get, the most secure you are)

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed
(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

→ A strong Security Awareness Program:
- Education
- Cyber ranges

→ Technology Intelligence: Get hackers' newest technique to determine how to detect and block them

Q5: For your selected area describe some technologies that need to be developed-deployed
(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

→ Machine learning: "Know normal, Find Evil"

→ Biometry

Profession/Role/ ……

Organisation: ……

Gender:…….

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.
(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

Supply chain security :

The cybersecurity challenge of the supply chain is far beyong the energy sector. Most of the critical infrastructure and operator of essential services rely on supplier to configure, maintain and secure their IT (MSP/MSSP). The supplier could be the weakest link and used by an opponent to break into the system of their client. The trust between a supplier and the client should not only based on a contract. The supplier need to be **audit** and **control** to ensure that whole client are not at risk. We need to design a secure way to administrate critical infrastructure and operator of essential services with practical implementation and trusted relation between the supplier & the client. We must avoid in Europe case like Wipro : large indian information technology provider was compromised and all of the customer were impacted. https://krebsonsecurity.com/2019/04/experts-breach-at-it-outsourcing-giant-wipro/

Privacy-preserving Identity Management

Blockchain is a huge opportunity to create distributed database with **strong cryptographic properties** and public trusted content. It's also an opportunity to use proved cryptographic protocol and proved compiler. Smart contract should also be lead by **formal verification** so the blockchain could store high valuable item (medical, etc.).

Maritime Cybersecurity

The cybersecurity on boat is challenging because the boat do not have a reliable connection. So we need cybersecurity defense that could take decision instead of operator (SOC provider) according to the legislation and the safety constraint.

There is also a mutual relation between the security of a port and the boat. It's the same requirement than Supply Chain security.

Smart Cities

Protocol and technologies used in smart cities need to be unified and regulate. Each cities has one kind of operator with one kind of propritary protocol.

IoT

It think IoT is the most challenging subject of the whole list. Today's IoT system are limited to few device interconnected manually or enrolment process scale on a very small set. Tomorrow every device will be connected and more often locally connected (5G network). How to authenticate each of this device at scale ? The authentication must use strong cryptographic protocol. What is the identity of an IoT ? What is the responsibility of the owner about security ? The main requirement here is **security at scale.**

We need to enforce a regulation so the IoT follow a security development lifecycle. Today IoT device is poorly developed with economic objective in mind and is implemented by unqualified people. The IoT are more and more involved to process critical device with potentially physical impact.

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

IOT : Authentication at scale. Each time you add an IoT device, you increase the complexity of the authentication scheme.

⇨ Smart Cities would create more and more IoT and increase the need to authenticate at scale.

Blockchain : formally proved cryptographic protocol and certified compiler to produce the core infrastructure (the blockchain and the smartcontract)

IOT : secure development lifecycle for low energy device

IOT + Maritime Cybersecurity : patch management for device that could run 10 years (cars, washing machine, etc.) Experience show we are bad to keep device patched in long period of time.

Smart cities : energy efficient computing + security

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

For each item, we need :

- Regulation to set a framework. The framework must be built with both technical and non-technical people.
- More certified product that respond to this framework.
- Awareness so company would pay to get certified product. Awareness is an endless job so people to join the cause of cybersecurity.

We need more people trained to cybersecurity, IA won't work if you don't have the right people behind the computer. Education must cover all aspect of cybersecurity : governance, offensive, defense, operationnal security, etc.

CyberCrisis management.

Post-quantum cryptography. We do not know if human kind will create a quantum computer, we need to be prepared. Every new device or technology should be configured to use now such technology (quantum computer would be able to break current transaction / communication)

Q5: For your selected area describe some technologies that need to be developed6deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

High performance homomorphic cryptography is a key feature to set trust in cloud computing provider.

Profession/Role:.....

Organisation:.....CYBLEX TECHNOLOGIES.....

Gender:.....MALE.....

Q1: Select which of the following application areas is closer to your line of expertise:

- € Open Banking Security
- € Supply chain Security
- € Privacy-preserving Identity Management
- € Security Incident Reporting
- € Maritime Cybersecurity
- € Medical Data Exchange
- € Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.

(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.)

In the Security Incident Reporting, we need solutions that can demonstrate their efficiency to be trustfull. For example, there is a lot of solutions in the market that use AI but no one can demonstrate the percentage of false positive that it will reduce or the time that it will reduce incident investigation.

We also need to be able to share incident data, like IOC and CERT information but in a very simplier way and with trust. To that, we need to be able to give a feedback on shared informations to know if they are usefull or worthless.

Finaly, one of the most important is to be able to contact clients if there is a data leak with personnal data constated. A central solution, where people could subscribe and received in real time notifications about a data leak regarding there informations could be very usefull in an incident response process. This could reduce time and help european people to protect themself against identity thiefs

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements

(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).

For my first point, I think the efficiency of AI in cybersecurity events detection and incident response needs to be proved. Currently there is a lot of solutions but no one want to open algorhythms and methods of AI to assure and demonstrate what the solution is doing and. They assume that the solution is a black box and they just want the client and users to trust them. This is a big problem, because how do we know if the solution is telling the true if we don't know how it works and how it detect and response to incidents.

The problem that my second point explain is the access to the information. We have open source Threat Intelligence feed but the data are not update every day and this means a lack of accuracy and veracity. Also I think that in some way, IOC and incident informations should be public and provided by a state service.

Finaly, GDPR obliged organisation to inform when an incident and data leak occured. But it's very difficult to contact users and clients impacted by the incident. A public plateform where companies could notified clients and users would help.

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed

(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.)

Point 1: Explaining AI with the help of experts and the reasearch community. We also need to shared trustfully uses cases and datasets to benchmark algorhythms and give feedback about what carecteristic vector is needed to explain the AI results.

Point 2: A way to share, evaluate, grade ,etc. Threat Intelligence informations.

Point 3: A way to share the nature of an incident with the citizen and company and related to GDPR.

Q5: For your selected area describe some technologies that need to be developed-deployed

(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.)

Point 1: opensource plateform that could help to share data, use cases and benchmark's results of AI algorhythms.

Point 2: an improvement of MISP plateform maintained by a european service and that any company could access.

Point 3: a plateofem like MISP but dedicated to GDPR incidents with a easy way to access for the citizen and companies

Survey

Explanation of how to read the survey results that follow

The results of the survey were first integrated into an Excel table for easy reading. The first line shows the question asked. Each following line shows all answers from the same person. However, it was not possible to fill the 24 questions on one Word page and they are hence placed in three consecutive pages. Each series of answers is composed of an average of 7 responses.

1	2	3	4	5	6	7	8	9
Country	**If other please specify**	**You are employed in:**	**Other (please specify):**	**What is your area of work?**	**Other (please specify)**	**What is your position?**	**Other (please specify)**	**Are you directly involved in one of the EU pilot projects launched to prepare the European Cybersecurity Competence Network?**
		Academy		Professional, Scientific, and Technical Services		Manager/professor/head of group		
Sweden		Academy		Education		Manager/professor/head of group		Yes
Italy		Academy		Research and Higher Education		Senior administrator/head of department		Yes
Spain		Industry		Finance and Insurance		Manager/professor/head of group		No
Netherlands		Academy		Research and Higher Education		Officer/Researcher/Administrator/Member of Staff		Yes
France		Academy		Information and communication		Officer/Researcher/Administrator/Member of Staff		Yes
Greece		Academy		Research and Higher Education		Manager/professor/head of group		Yes
Germany		Academy		Research and Higher Education		Manager/professor/head of group		Yes
Germany		Academy		Research and Higher Education		Officer/Researcher/Administrator/Member of Staff		Yes

10	11	12	13	14	15	16	17	18
Are you involved in CyberSec4 Europe?	**Which of the following Cybersecurity Vertical Sectors is your main area of expertise?**	**If other, please specify:**	**Which of the following verticals of the pilots is your main area of expertise:**	**What Europe should achieve as an overall goal in cybersecurity?**	**In your specific area of expertise, what is the key cybersecurity situation that must change (e.g. better resilience, transparency, trustworthiness, security metrics...)? If possible, explain also the motivations behind your indications.**	**In your area, what key capabilities are required by systems, people, institutions, etc, to achieve that change?**	**What is needed to achieve the capabilities you just mentioned?: Novel Technologies**	**What is needed to achieve the capabilities you just mentioned?: New or improved technical standards**
			Incident Reporting	Ensuring best practices are actually followed.	Lack of clear engineering principles and adherence to best practices.	Educational background in proper engineering discipline and authority and responsibility for engineers.		
Yes	Health/Medicine		Privacy-preserving Identity Management	Better cooperation between expert ccnters?	Address Usable privacy and security, Address Human Factors	More research capabilities	Essential	
Yes			Finance and E-Commerce	Improve the ability of European citizens and companies to understand what they are doing. They can still do risky choices but at leats tehy should know what they are doing.	Better transparency	Better skills and risk perception.	Not Essential	Not Essential
				Trust	Trustworthiness in sharing on intelligence information and incidents	Knowledge of the industry user	Of Minor Importance	Of Minor Importance
No	Other	Governance		Unity of intent and action	Decision-making transparency Clear legal base	Better communication	Essential	Of Minor Importance
Yes			Supply Chain Security Assurance	Create policies and tools to ensure all cybersecurity stakes are covered, either by enforcing rules, imposing certification processes for critical domains and designing clear guidelines for the best practices of the industry. EU has to become independent regarding cybersecurity challenges from other countries, and thus ensure all players of its strategic industrial domains are protected and able to design safe technologies.	In my field of expertise, cybersecurity issues and most importantly safety requirements have to be accounted for at the design stages to ensure a no-risk behavior of the cyber-physical system.	Key capabilities in matter of certification rules enforcement and validation.	Of Major Importance	Of Major Importance
Yes			Privacy-preserving Identity Management	A harminonized, cross-border, cybersecurity and cyberdefense framework for all EU countries.	Transparency is, currently, lacking from many EU governmental sites as well as industrial partners. ICT systems are, by nature, of zero transparency, since the user cannot see <<under the hood>>, This jeopardizes EU citizens' trust towards EU ICT infrastructure and services.	Better security awareness levels and employment of expert (in ICT security and privacy) in key positions in EU institutions.	Of Minor Importance	Essential
Yes			Privacy-preserving Identity Management	Competitiveness with Asia and the US Protection of Eu citizens and companies against attacks from out-of-Europe General Standards Privacy and Data Protection	privacy and data protection clear information strategies	education better understanding privacy and it-security by design - build products, services, software including these from scratch	Of Minor Importance	Of Major Importance
Yes			Supply Chain Security Assurance		I am actually no expert in cybersecurity. I am working on the governance structure of the pilot. Sorry, I can't answer this.	I am actually no expert in cybersecurity. I am working on the governance structure of the pilot. Sorry, I can't answer this.		

19	20	21	22	23	24
What is needed to achieve the capabilities you just mentioned? : Other	**Other (please specify):**	**Please describe some specific technologies or technical standards that you have in mind, otherwise add N/A.**	**Please describe some specific organisational measures (e.g. skill sets, regulation, liability) that you think are important. Otherwise add N/A.**	**Should the Network and Centre push towards specialization of Member States and prioritize funding the development of different technologies in different Member States?**	**What additional information you would like to give us and that we forgot to ask for?**
		-	A requirement for engineers to sign of on projects and becoming liable in the process.		-
		Usable tools providing end users with better privacy controls, Testing techniques for usable security	Security & Privacy awareness programmes	No	
		NA	If you sell a software that is insecure you should be fined. in the same way as you cannot sell a toy with asbestos or you cannot sell food with pesticides. If we don't start putting fines on lack of quality there is never going to be an improvement (also because customers cannot tell the good product from the bad one).	No	
		N/A	Skills and end user experience	Yes	
		N/A	N/A	Only in special cases	
		DO-178C	Novel technologies (IoT) have to be pushed into cyberphysical systems and we need to adapt the technical standards to ensure cyberphysical rules are enforced properly	No	
		Identity management, especially federated schems that work in a cross-border manner as well as privacy preserving technologies.	Skills in ICT security and privacy are essential as well as installation of protection systems and software.	Yes	Let's wish us good luck for best results!
Of Major Importance	Awareness; incentives (ie. subsidies)	it-security by design	awareness in organiations; upscaling of importance in companies; stricter company rules; stricter legal framework	Yes	- finances - information process - decision making process - control
		N/A.	N/A.		

1	2	3	4	5	6	7	8	9
Country	**If other please specify**	**You are employed in:**	**Other (please specify):**	**What is your area of work?**	**Other (please specify)**	**What is your position?**	**Other (please specify)**	**Are you directly involved in one of the EU pilot projects launched to prepare the European Cybersecurity Competence Network?**
Germany		Industry		Research and Higher Education		Manager/professor/head of group		Yes
Ireland		Academy		Research and Higher Education		Other		Yes
Slovak Republic		Industry		Professional, Scientific, and Technical Services		President/CEO/Member of Board		Yes
Italy		Industry		Information and communication		Officer/Researcher/Administrator/Member of Staff		Yes
Other	Switzerland	Industry		Professional, Scientific, and Technical Services		Officer/Researcher/Administrator/Member of Staff		Yes
		Academy		Research and Higher Education		Officer/Researcher/Administrator/Member of Staff		Yes
Other	Switzerland	Industry		Professional, Scientific, and Technical Services		President/CEO/Member of Board		Yes

10	11	12	13	14	15	16	17	18
Are you involved in CyberSec4 Europe?	**Which of the following Cybersecurity Vertical Sectors is your main area of expertise?**	**If other, please specify:**	**Which of the following verticals of the pilots is your main area of expertise:**	**What Europe should achieve as an overall goal in cybersecurity?**	**In your specific area of expertise, what is the key cybersecurity situation that must change (e.g. better resilience, transparency, trustworthiness, security metrics...)? If possible, explain also the motivations behind your indications.**	**In your area, what key capabilities are required by systems, people, institutions, etc, to achieve that change?**	**What is needed to achieve the capabilities you just mentioned?: Novel Technologies**	**What is needed to achieve the capabilities you just mentioned?: New or improved technical standards**
Yes			Finance and E-Commerce;Supply Chain Security Assurance	Europe needs to have systems that operate continuously without interruptions or failures and that protect the safety and security interests of their human users. To achieve this goal, Europe must have the ambition to identify and develop techniques and methodologies for the construction of IT that are secure by design.	The cybersecurity aspects that must change are: - Transparency - Trustworthiness	Existing models are not well catered to existing cybersecurity challenges. Therefore, the scientific and business communities should join forces to propose end-to-end security solutions that allow the unified management of digital information from the devices to the core of the network. This requires proper education of people, proper training within institutions, and proper testing and formal analysis of the security of the systems.	Essential	Of Minor Importance
Yes			Incident Reporting;Smart Cities		There are different challenges in the software engineering domain: - approaches to identify vulnerabilities at the software architecture level are very important. Current vulnerability assessment tools mainly identify security bugs rather than architectural flaws - approaches to provide assurances explaining which security controls should be implemented and why.This is important because many defence techniques are based on black box machine learning techniques.	Real Test-beds and datasets for security.	Essential	Of Minor Importance
Yes			Privacy-preserving Identity Management		systematic collection of hard data (e.g. about cybersecurity incidents) and their availability for research honest assessment of the cybersecurity situation (e.g. replacing political statements with expert, reasoned arguments)	political support and explicit request for honest expert assessment of the cybersecurity situation	Of Minor Importance	Of Major Importance
Yes			Smart Cities	The most dangerous (and in the same, attractive) environment for the cyber attacker is the dark web. Making "light" on it, would be actually disruptive in Europe and not only here.	What in Europe lack is the people awareness about data privacy. Too much people say "I don't care about the companies exploiting regarding my data if this allows them to offer me the right product." SMEs capacity to react to a cyber-attack. Networks like CERT or CSIRT more powerful. More interaction between actors in the cyber-security, not only the IT staff.	Governance campaigns for cyber education. Top manager awareness about cyber-security risk.		
Yes			Privacy-preserving Identity Management	The first and most important goal for the EU should be to improve awareness of and response to cyber-attacks aimed at member states or EU institutions.	Build momentum for the certification schemes in the field of cybersecurity	Improvement of the privacy culture. Strong interaction between legal and technical expertise.	Of Major Importance	Essential
Yes			Smart Cities	Cybersecurity by design Control mechanisms	Security-by-design: it involves moving Verification and Validation activities at design phase to avoid security weaknesses and drastically reduce security risk. Awareness. Attacks typically happen because of lack of attention/low confidence in the security risks.	Realize a national reference centre for cybersecurity and Increase the collaboration between academia, research and industries	Of Minor Importance	Of Minor Importance
Yes			Supply Chain Security Assurance	A harmonised approach toward cybersecurity with cooperation across Europe	The primary issue is trust and having secure solutions - and thus, standardisation and certification are important.	Development of a framework of standards and certification.	Of Minor Importance	Essential

19	20	21	22	23	24
What is needed to achieve the capabilities you just mentioned? : Other	**Other (please specify):**	**Please describe some specific technologies or technical standards that you have in mind, otherwise add N/A.**	**Please describe some specific organisational measures (e.g. skill sets, regulation, liability) that you think are important. Otherwise add N/A.**	**Should the Network and Centre push towards specialization of Member States and prioritize funding the development of different technologies in different Member States?**	**What additional information you would like to give us and that we forgot to ask for?**
		N/A	Regulation is extremely important in the sense to enforce cybersecurity practices that are recommended by experts in the community.	Yes	
		N/A	Skill sets: unfortunately software engineers do not receive appropriate training in university in relation to security and secure coding.	Only in special cases	
		N/A	N/A	No	
		N/A	N/A	No	
		N/A	certification schemes, development of trainings and skill sets	Only in special cases	
		N/A	national and regional cybersecurity centres	No	
		IoT is an area where standards and certification can be further developed	Regulation and governance are key areas	No	

3	4	5	6	7	8	9	10	11
You are employed in:	**Other (please specify):**	**What is your area of work?**	**Other (please specify)**	**What is your position?**	**Other (please specify)**	**Are you directly involved in one of the EU pilot projects launched to prepare the European Cybersecurity Competence Network?**	**Are you involved in CyberSec4 Europe?**	**Which of the following Cybersecurity Vertical Sectors is your main area of expertise?**
National Regulator		Public Administration		Senior administrator/head of department		No		
Academy		Research and Higher Education		Manager/professor/head of group		Yes	Yes	
Industry		Information and communication		Manager/professor/head of group		No		
Academy		Research and Higher Education		Officer/Researcher/Administrator/Member of Staff		Yes	Yes	
Academy		Research and Higher Education		Manager/professor/head of group		Yes	Yes	

12	13	14	15	16	17	18	19	20
If other, please specify:	**Which of the following verticals of the pilots is your main area of expertise:**	**What Europe should achieve as an overall goal in cybersecurity?**	**In your specific area of expertise, what is the key cybersecurity situation that must change (e.g. better resilience, transparency, trustworthiness, security metrics...)? If possible, explain also the motivations behind your indications.**	**In your area, what key capabilities are required by systems, people, institutions, etc, to achieve that change?**	**What is needed to achieve the capabilities you just mentioned?: Novel Technologies**	**What is needed to achieve the capabilities you just mentioned?: New or improved technical standards**	**What is needed to achieve the capabilities you just mentioned? : Other**	**Other (please specify):**
		Increase the capability of planning, delivering and monitoring the resilience and thrust of public services offered to citizens by ICT.	It is necessary to provide public service providers with tools and services (a framework) for deploying and managing resilient and trustworthy services, without hindering their usability, accessibility, and funcional properties.	IT Security, Secure system development and management, Secure application development and management. Change management, IT Procurement,	Of Minor Importance	Essential		
	Privacy-preserving Identity Management	Better coordination of the research activities and the economy of scale by means of consolidating solid research cluster of agents. Also the creation of stable network of researchers in the field to facilitate the leverage of individuals results.	Better management of the trustworthiness in dynamic and changing environment. The advent of the mobile communication, IoT and other is creating a new paradigm of security that need to cope with context of the security that are changing. Also the need for testing and labeling tools to validate the securioty and privacy by design following more formal methods wil be crucial on the digitalization of the economic sectors	As part of a research centre accreditation of skills and knowledge of the researchers it is crucial.	Essential	Essential		
		Coordination, funding and support of efforts in view of accelerating the emergence of an advanced, innovative, dynamic and integrated cybersecurity ecosystem that reaps the benefits of basic and advanced technologies, ensures their diffusion to all economic sectors, critical and non critical, and by all stakeholders (from large industries to SMEs, public authorities to NGOs) so that European Cyber Defense gets strengthened, the European major vertical industries get transformed in a secure and resilient manner, data are protected as per GDPR but also fuel the data economy.	There is a need for available and adapted tools for enhancing the preparedness of small and medium companies to face cyber-security incidents and respond to them adequately. I deem this important as SMEs are lagging behind i terms of cyber-security awareness and risk management.	We need people trained in an interdisciplinary manner on cybersecurity. A generation of professionals who master both the security of systems but also understand how cybersecurity affects the business in many other aspects is much needed. In terms of systems, we still need advanced and affordable systems for protecting systems as well as developing advanced situational awareness. Systems need to be better adapted to the specific needs for each sector. At institutional level, we certainly need better connections between CSIRTs and the society.	Essential	Essential		
	Supply Chain Security Assurance		Trustworthiness and resilience	Self adaptiveness, assurance, resilience	Of Major Importance	Of Major Importance		
	e-Health and Medical Data Exchange	European citizens need infrastructures, services and products that they can trust and need to be digitally sovereign. Europe must provide clear criteria for assessing if or to which extent infrastructures, services and products can be trusted and ensure that citizens are offered infrastructures, services and products with high levels of trustworthiness and that allows them to retain their digital sovereignty.	Standarisation/certification of infrastructures/services/products requiring clear security metrics, (continuously) verified with rigorous verification methods.	A proactive/preventive/by-design security mindset in people, institutions and in the blueprint of systems.	Of Major Importance	Of Major Importance	Of Minor Importance	

19	20	21	22	23	24
What is needed to achieve the capabilities you just mentioned? : Other	**Other (please specify):**	**Please describe some specific technologies or technical standards that you have in mind, otherwise add N/A.**	**Please describe some specific organisational measures (e.g. skill sets, regulation, liability) that you think are important. Otherwise add N/A.**	**Should the Network and Centre push towards specialization of Member States and prioritize funding the development of different technologies in different Member States?**	**What additional information you would like to give us and that we forgot to ask for?**
		Secure private and public cloud infrastructures and intrusion detection/management systems, web application protection systems, secure content delivery networks.	Policies for establishing a clear and possibly not hierarchical/bureaucratical organization of competencies and responsibilities. Policies and tools for achieving better coordination between administrations and centers for managing secure and reliable services. Involving public authorities in the process of development/deployment in order to ease monitoring and avoid false positives/negative as much as possible.	No	
		Advanced security like quantum technologies and distributed identity	Common and structured set of skill for different security employs and a more homogeneous definition of the cybersecurity skills	No	The role of ECSO and cPPP should be maintain as a central agent in the decisión process
		Technologies: SDP, TPM, TEE, SDN	Skill sets: cybersec preparedness, incident management (technical to business level) Understanding of cybersecurity insurance schemes.	Only in special cases	N/A
		N/A	N/A	Only in special cases	
Of Minor Importance		Formal verification (theorem proving, static analysis, model checking).	N/A	No	

1	2	3	4	5	6	7	8	9
Country	**If other please specify**	**You are employed in:**	**Other (please specify):**	**What is your area of work?**	**Other (please specify)**	**What is your position?**	**Other (please specify)**	**Are you directly involved in one of the EU pilot projects launched to prepare the European Cybersecurity Competence Network?**
Italy		Industry		Information and communication		Officer/Researcher/Administrator/Member of Staff		Yes
Italy		National Agency		Public Administration		Officer/Researcher/Administrator/Member of Staff		No
Greece		Academy		Research and Higher Education		Manager/professor/head of group		Yes
Cyprus		National Agency		Research and Higher Education		President/CEO/Member of Board		No
Other	Switzerland	Other	Research Association	Research and Higher Education		Officer/Researcher/Administrator/Member of Staff		No

10	11	12	13	14	15	16	17	18
Are you involved in CyberSec4 Europe?	Which of the following Cybersecurity Vertical Sectors is your main area of expertise?	If other, please specify:	Which of the following verticals of the pilots is your main area of expertise:	What Europe should achieve as an overall goal in cybersecurity?	In your specific area of expertise, what is the key cybersecurity situation that must change (e.g. better resilience, transparency, trustworthiness, security metrics...)? If possible, explain also the motivations behind your indications.	In your area, what key capabilities are required by systems, people, institutions, etc, to achieve that change?	What is needed to achieve the capabilities you just mentioned?: Novel Technologies	What is needed to achieve the capabilities you just mentioned?: New or improved technical standards
Yes			Smart Cities	Data Sovereignty, Data owner consciousness to get full control of data for a better transparency	Better Transparency and trustworthiness	Privacy policies and rules	Essential	Essential
				Increase the awareness about cybersecurity issues Increase the incident respose competence and capacity Develop more effective authentication methods Counteract social engineering attacks	Better resilience: as a public administration the resilience against a possibile service disruption is very important to guarantee operation of services to the citizen.	More expertise about: cybersecurity governance, technical specializations about malware analysis and network security.	Not Essential	Of Minor Importance
Yes			Privacy-preserving Identity Management;Smart Cities	Become a world leader in the area of security and privacy.	We need to support research and innovation in the area of cyber security.	Education in cybersecurity principles and practice	Of Major Importance	Of Major Importance
				Protection of citizens, businesses and state actors. The transition to a European Digital Economy can never be realized with out trust from all stakeholders and citizens, that their transaction are made with safety and privacy. Furthermore, citizens and businesses will never feel safe to invest time and money on line, should Europe does not invest in safeguarding the Cyber with regulating, legislating and taking precautions to proactively protect them but also its critical infrustructure.	1. Mentality. People and businesses have not yet realized what's at stake. 2. Resilience. Policy makers and politicians themselves have little knowledge of the real situation and jeopardy of a loose Cybersecurity, for the economy and the citizens. They just don't invest enough 3. Privacy. Even after GDPR has passed in theory, real life is very different. Most states and businesses don't comply. The implementation of GDPR is a joke. 4. Research. Not enough. EU think the 2 billion they said they will invest in Cybersecurity is enough. It's a redicule. Look at what others spend and you will understand. (US, China etc)	Man power. Not enough become Cybersecurity professionals or not enough people with basic digital skills to take over lesser roles critical for the Cybersecurity domino. Everything starts and ends here. The most important immaterial capital is people. People with skills to do the job effectively. All the rest follows.	Of Major Importance	Of Major Importance
				Cybersecurity is seen by the European Commission as "Cybersecurity Industrial, Technology, and Research Competence Centre" and a "Network of National Coordination Centres".	Security is a process (as ICT technology evolves, so do the threats), Security of the Common Infrastructure, Resilience rather than Defence and Dual-Use Technologies.	Cybersecurity Strategy Digital Single Market Strategy Legislative acts to fight cybercrime Development of network and information security Projects against cybercrime Capacity building	Essential	Of Major Importance

19	20	21	22	23	24
What is needed to achieve the capabilities you just mentioned? : Other	**Other (please specify):**	**Please describe some specific technologies or technical standards that you have in mind, otherwise add N/A.**	**Please describe some specific organisational measures (e.g. skill sets, regulation, liability) that you think are important. Otherwise add N/A.**	**Should the Network and Centre push towards specialization of Member States and prioritize funding the development of different technologies in different Member States?**	**What additional information you would like to give us and that we forgot to ask for?**
		Privacy-Enhancing Technologies, Self sovereignty Identity solution and Distributed ledgers (blockchain like)	Regulation and skill sets	Yes	
Not Essential		N/A	N/A	Yes	
		N/A	N/A	Only in special cases	
Of Minor Importance		Not enough space. Just use the services of CEN CENELEC and ETSI. Standards are the cornerstone of our effort.	Everything described in ISO 27000 series of standards.	Yes	ISACs. The compétence should facilitate the creation of National ISACs at first, then European sectoral ones. But we should start at National level, build trust among the industry and all actors, make them believe it works. And then move up to bigger scale.
Of Minor Importance		N/A	N/A	Only in special cases	

1	2	3	4	5	6	7	8	9
Country	**If other please specify**	**You are employed in:**	**Other (please specify):**	**What is your area of work?**	**Other (please specify)**	**What is your position?**	**Other (please specify)**	**Are you directly involved in one of the EU pilot projects launched to prepare the European Cybersecurity Competence Network?**
Spain		Industry		Information and communication		Officer/Researcher/Administrator/Member of Staff		Yes
Spain		Industry		Information and communication		Manager/professor/head of group		Yes
United Kingdom		Other	RTO	Other	Applied Reserach and Innovation	Manager/professor/head of group		No

10	11	12	13	14	15	16	17	18
Are you involved in CyberSec4 Europe?	Which of the following Cybersecurity Vertical Sectors is your main area of expertise?	If other, please specify:	Which of the following verticals of the pilots is your main area of expertise:	What Europe should achieve as an overall goal in cybersecurity?	In your specific area of expertise, what is the key cybersecurity situation that must change (e.g. better resilience, transparency, trustworthiness, security metrics...)? If possible, explain also the motivations behind your indications.	In your area, what key capabilities are required by systems, people, institutions, etc, to achieve that change?	What is needed to achieve the capabilities you just mentioned?: Novel Technologies	What is needed to achieve the capabilities you just mentioned?: New or improved technical standards
Yes			e-Health and Medical Data Exchange	As the cyberattacks and cybercrime are increasing sharply due to the digitalization of the public services and business as well as the citizen activities, Europe should tackle this problem developing common strategies, regulations and tools assuring security and privacy on transactions between organizations, business and citizens.	Trustworthiness between different stakeholders must be increased when sharing data between data providers and data consumers. Preserving user data privacy is a key when sensitive data are shared. Security must be assured when data are shared, stored, processed and transmitted.	Privacy preserving techniques Identity and access management tools	Essential	Of Major Importance
Yes			Incident Reporting	Incident reporting is a complex and tedious activity, particularly when addressing Financial Institutions. Europe should address this issue by developing tools that enable financial institutions to fulfill the mandatory incident reporting requirements according to the different procedures/methods specified by applicable regulatory bodies.	There is the need for standardised and coordinated cyber-security communication cooperation, this collaboration will pave the way towards a public and private cooperation to reach the common goal of an enhanced cyber resilience across Europe and beyond the EU borders.	- Technologies for Incident Reporting, - A common incident taxonomy taking into account all applicable regulatory requirements, - Tools & methodologies for the identification of the impact perimeter of an incident, - Tools and methods for the quantification of the potential or real impact of an incident to determine the overall severity of the critical event, - Trustworthy information sharing: secure and efficient protocols for information exchange (including Threat Intelligence Sharing), - Advanced Threat Intelligence: application of machine learning and AI to prevent attacks and threats, but also to	Essential	Of Major Importance
				To rise the capabilities in withstanding and avoiding cyberattacks. And recover after cyberattacks.	Ability to withstand and avoid cyberattacks. And recover after cyberattacks.	Operational Cyber Ranges	Of Minor Importance	Essential

19	20	21	22	23	24
What is needed to achieve the capabilities you just mentioned? : Other	**Other (please specify):**	**Please describe some specific technologies or technical standards that you have in mind, otherwise add N/A.**	**Please describe some specific organisational measures (e.g. skill sets, regulation, liability) that you think are important. Otherwise add N/A.**	**Should the Network and Centre push towards specialization of Member States and prioritize funding the development of different technologies in different Member States?**	**What additional information you would like to give us and that we forgot to ask for?**
Not Essential		There is not a standard eIDAS certification scheme for Trusted Service Providers. Markets should be open, not closed!	A comprehensive yet inclusive regulation for cybersecurity certification of professional products, that nowadays are under the umbrella of Common Criteria; this must include financial support towards certification.	Yes	
		Attributed Based Credentials,	N/A	Yes	
Not Essential		Wholistic governance approaches, e.g. COBIT 2019, regulation, e.g. General Data Protection Regulation (GDPR) and eIDAS, and standards.	Increased cybersecurity skill sets for existing and future IT security professionals in the field of authentication, encryption and privacy. Inclusion of business value of the cybersecurity in business and law-related studies. More clearly defined and EU-unified requirements in the regulation, connected to cybersecurity, e.g. GDPR. Enforce interoperability in solutions, services and products (e.g. to combat the problems arose with the eIDAS). Increased liability for cybersecurity challenged products and services even	Only in special cases	None.

1	2	3	4	5	6	7	8	9
Country	**If other please specify**	**You are employed in:**	**Other (please specify):**	**What is your area of work?**	**Other (please specify)**	**What is your position?**	**Other (please specify)**	**Are you directly involved in one of the EU pilot projects launched to prepare the European Cybersecurity Competence Network?**
France		Industry		Finance and Insurance		Other	architect	Yes
Other		Academy		Information and communication		President/CEO/Member of Board		No
Austria		Industry		Professional, Scientific, and Technical Services		President/CEO/Member of Board		No
Spain		Industry		Information and communication		Manager/professor/head of group		No
Spain		Academy		Information and communication		Officer/Researcher/Administrator/Member of Staff		No

10	11	12	13	14	15	16	17	18
Are you involved in CyberSec4 Europe?	Which of the following Cybersecurity Vertical Sectors is your main area of expertise?	If other, please specify:	Which of the following verticals of the pilots is your main area of expertise:	What Europe should achieve as an overall goal in cybersecurity?	In your specific area of expertise, what is the key cybersecurity situation that must change (e.g. better resilience, transparency, trustworthiness, security metrics...)? If possible, explain also the motivations behind your indications.	In your area, what key capabilities are required by systems, people, institutions, etc, to achieve that change?	What is needed to achieve the capabilities you just mentioned?: Novel Technologies	What is needed to achieve the capabilities you just mentioned?: New or improved technical standards
Yes			Finance and E-Commerce	Building a road map focused on concrete needs in critical sectors Creating a network providing a better cooperation between researchers and industry leaders	The régulations must become an opportunity for Europe to take a leadership and not a contraint for european actors	Researchers must be well informed about concrete needs in critical sectors Industry leaders must integrate the work achieved in research sector in their business Road Map	Of Major Importance	Essential
				Protect European companies data from being stolen. Protect European elections from fake news and external influence Protect European citizens from scam, identity usurpation, spyware, malware, virus	better resilience to protect my data and IP assets transparency to know who has which data about me and my business trustworthiness, in the selection of my providers, clients and partners security metrics to monitor how I should invest my time and money	There is a high price to pay for security and we need to prioritise our investments. Reducing the prices of cyberprotection for citizen and SMEs to give them access to security and compliance.	Essential	Of Major Importance
				Autonomy and independence from non-EU countries with regards to technology in general and cybersecurity in specific. Assuring high principles with regards to confidentiality, integrity and availability of European citizens, data and industry has to be assured by controlling the services and data ourselves.	Assurance of full transparency and trustworthiness along the security value chain, moreover the complete ICT value chain. This is a pre-requisition for assurance of resilience of services and providing confidentiality and integrity of services.	1) Transparency of the supply chain: where do upstream components come from? What is their trust level? How can it be improved? 2) Control of the supply chain: active management of trustworthy suppliers to achieve best possible output 3) Ownership of the supply chain	Of Major Importance	Essential
				New standars. New model of interchange of information. The enterprise and research group need to coolaborate for new models.	the resilence, the transparecen. I am working in pentest and the organization some time prefered not to kow, and avoid the reality. it is important that the companies perform simulations attacks close to reality.	people. Regulations	Of Major Importance	Of Major Importance
				Secuirty certification and labelling as a way to compare and inform end users about security.	Simplicity for applying it and automation to facilitate its adoption, homogeneity for comparison, labelling to facilitate the end user the understanding of the security of a product.Resilicency to react against attacks, and therefore a taxonomy of attacks based on measurable events to be able to detect when the system is being attacked or not.	training of people in terms of security to avoid social engineering and related attacks and Homogeneization and standarization of security assessment leaded by institutions.	Of Major Importance	Of Minor Importance

19	20	21	22	23	24
What is needed to achieve the capabilities you just mentioned? : Other	**Other (please specify):**	**Please describe some specific technologies or technical standards that you have in mind, otherwise add N/A.**	**Please describe some specific organisational measures (e.g. skill sets, regulation, liability) that you think are important. Otherwise add N/A.**	**Should the Network and Centre push towards specialization of Member States and prioritize funding the development of different technologies in different Member States?**	**What additional information you would like to give us and that we forgot to ask for?**
Of Major Importance	test	test	test	Yes	test
Essential	Develop technical frameworks to improve the lacks of the ones detected in the Tiber-EU (e.g. It cannot be possible to hire intelligence team and red team at the time because in order to evaluate the Red Team skills it should be defined the scope and level of the attack simulation, so the Red Team should be contracted always after the Intelligence analysis.)	I am working in a new attack standard called CAT, Cyber attack taxonomy, that It is built as an alternative to the Kill chain models, very questioned in the now a days attacks, more parallel than serial, and with phases not considered previously. This model (CAT) will incorporate the strategic phases, that are consolidated with Techniques, Tactics and procedures coming from other parties like Mitre or PwnWiki, so that develops a very compact methodology. This methodology allows also to identify protection measures for every single technique in a very structure way.	Tiber EU, CBEST, Tiber-NL, as samples of interesting sector frameworks for cybersecurity testing.	Yes	Every day I see hundred of companies affected by vulnerabilities that are exposed to the internet. These vulnerabilities open the door to cybercriminals that are out of the scope of our international laws. The companies store private date from EU citizens and they are responsible to keep them as safe as possible. Without a European regulation that force a cybersecurity testing, only the big data breaches will be published and fined. I think the Cybersecurity it should not be an option but a mandatory regulation by external examination of the cyber-health.
		In the past approaches such as "typed assembly languages" and "proof carrying code" have been developed so as to overcome some of the difficulties of checking software obtained from other developers: finding the annotations is computationally hard and is part of the programming task, checking the annotations is computationally easy and is part of accepting the software. It will be essential to retarget such approaches to lightweight formal techniques for ensuring security.	This should be incorporated in GDPR or similar initiatives.	Only in special cases	It is important to inform civil servants, politicians and industry managers that it is possible to build software systems that are virtually free from vulnerabilities (modulo brute-force-attack and hardware faults). That the development of an array of lightweight formal methods will make it practical to reap some of these benefits without incurring the colossal costs of fully achieving these goals for all software. To redirect the balance from reactive techniques (still needed of course) to proactive techniques. To stress that the strongest link in the current security landscape is the cryptography, despite
		Cyber Intelligence	Cyber Intelligence	Yes	
		AI-based autonomous police forces inside networks (like the Agents in Matrix). Security labels for most products (like those existing for energy consumption.	Liability should be imposed, even if lightly. Regulation should take liability and accountability into account (like in the GDPR) and establish the conditions for resilient networks and services to thrive in a market that encompasses insurance.	Only in special cases	

1	2	3	4	5	6	7	8	9
Country	If other please specify	You are employed in:	Other (please specify):	What is your area of work?	Other (please specify)	What is your position?	Other (please specify)	Are you directly involved in one of the EU pilot projects launched to prepare the European Cybersecurity Competence Network?
Belgium		Industry		Manufacturing		President/CEO/Member of Board		No
Greece		Academy		Education		Officer/Researcher/Administrator/Member of Staff		Yes
Netherlands		Academy		Research and Higher Education		Officer/Researcher/Administrator/Member of Staff		Yes

10	11	12	13	14	15	16	17	18
Are you involved in CyberSec4 Europe?	Which of the following Cybersecurity Vertical Sectors is your main area of expertise?	If other, please specify:	Which of the following verticals of the pilots is your main area of expertise:	What Europe should achieve as an overall goal in cybersecurity?	In your specific area of expertise, what is the key cybersecurity situation that must change (e.g. better resilience, transparency, trustworthiness, security metrics...)? If possible, explain also the motivations behind your indications.	In your area, what key capabilities are required by systems, people, institutions, etc, to achieve that change?	What is needed to achieve the capabilities you just mentioned?: Novel Technologies	What is needed to achieve the capabilities you just mentioned?: New or improved technical standards
				more competitive cyber security industry - innovations that cyber security industry can pick up instead of general academic activities	behavior and attitude every company, citizen should practice cybersecurity as a responsible person, not endangering others the attitude should move from reactive, defensive to proactive and innovative	too much process, procedures, rules and limitations security by innovation	Essential	Of Major Importance
Yes			Maritime Transport	Cybersecurity Independence, Privacy protection of EU citizens, Critical Infrastructure Protection.	Resilience, since Critical Infrastructures need to be able to absorb the impact of unwanted events, to quickly recover from attacks and to be able to operate at some level during an attack.	Security awareness, understanding and modelling security threats, identifying the proper security controls to mitigate the risks and hardening the security of the relevant systems.	Of Major Importance	Of Major Importance
Yes			e-Health and Medical Data Exchange	To be at the forefront of technical expertise to guarantee security and privacy in digital networks in order to remove impediments from barriers to economic development and innovation.	Security metrics to identify issues in cybersecurity and to be able to combat them	Technical know how on cyber attacks and threads, the means to identify them and to use data analytics to predict and prevent cyber attacks to occur or at least be quick in detecting and solving them.	Of Major Importance	Essential

19	20	21	22	23	24
What is needed to achieve the capabilities you just mentioned? : Other	**Other (please specify):**	**Please describe some specific technologies or technical standards that you have in mind, otherwise add N/A.**	**Please describe some specific organisational measures (e.g. skill sets, regulation, liability) that you think are important. Otherwise add N/A.**	**Should the Network and Centre push towards specialization of Member States and prioritize funding the development of different technologies in different Member States?**	**What additional information you would like to give us and that we forgot to ask for?**
		Privacy preserving techniques such as anonymization, pseudo-anonymisation, cryptographic technologies such as homomorphic encryption, functional encryption, multiparty computation. Identity and access management tools including blockchain technology or eIDAS for strong authentication.	Regulation related to derived identities, Stability SLA	Yes	
		Cybersecurity analytics: big data analysis of cybersecurity information	N/A	Yes	
Of Major Importance	Product liability, i.e liability that the products is used in a way that prevents cyberattacks.	In cloud security, Access Control based on XACML 3.0, i.e. ABAC, Attribute Based Access Control In IoT, user of COAP + DTLS + OSCORE On internet, use of end-to-end object security Deep defence with segmented networks, firewaals on multiple levels	Product liability, i.e liability that the products is used in a way that prevents cyberattacks. SOC opertional personell CISOs	No	

1	2	3	4	5	6	7	8	9
Country	If other please specify	You are employed in:	Other (please specify):	What is your area of work?	Other (please specify)	What is your position?	Other (please specify)	Are you directly involved in one of the EU pilot projects launched to prepare the European Cybersecurity Competence Network?
Netherlands		Industry		Information and communication		Manager/professor/head of group		No
Greece		Academy		Research and Higher Education		Other	Faculty member	Yes
Other	Norway	Academy		Information and communication		Officer/Researcher/Administrator/Member of Staff		Yes

10	11	12	13	14	15	16	17	18
Are you involved in CyberSec4 Europe?	Which of the following Cybersecurity Vertical Sectors is your main area of expertise?	If other, please specify:	Which of the following verticals of the pilots is your main area of expertise:	What Europe should achieve as an overall goal in cybersecurity?	In your specific area of expertise, what is the key cybersecurity situation that must change (e.g. better resilience, transparency, trustworthiness, security metrics...)? If possible, explain also the motivations behind your indications.	In your area, what key capabilities are required by systems, people, institutions, etc, to achieve that change?	What is needed to achieve the capabilities you just mentioned?: Novel Technologies	What is needed to achieve the capabilities you just mentioned?: New or improved technical standards
				Become world leader.	Knowledge distribution and funding. Most talent disappears towards the US, main reason is because the US is intellectually more challenging. There is not that much funding for new projects like there is in the US and China. Hence knowledgeable people disappear to one of those countries.	It's sad to say, but brilliant minds will disappear to spy agencies. At this moment those spy agencies are local, there's no European spy agency. If you combine these agencies knowledge will be shared between these people and new highs can be achieved. Simply said: the law of large numbers applies here. Group everything together, distribute it evenly, deduplicate, fund it propperly, profit! Make relocation easy!	Essential	Essential
Yes			Maritime Transport	Develop the cybersecurity skills and capabilities, in order to achieve technological cybersecurity independence with respect to third countries and to be able to adequately protect its critical infrastructures and services from cyber threats.	Better resilience	1) Cybersecurity awareness of the involved actors 2) Novel cybersecurity technologies following the resilience-by-design principle	Of Major Importance	Of Minor Importance
Yes			Maritime Transport	Become a world leader in reasearch and implementation Protecting the digital freedom of citizens	Very few digital services work across borders, this is hindering a lot of the economic potential for Eruope. Security research is fragmented, and there is a lot of duplication across Europe. Promising new companies move to Silikon Valley, they don't stay here.	Good communication Understanding of what is needed Enough resources	Of Major Importance	Of Minor Importance

19	20	21	22	23	24
What is needed to achieve the capabilities you just mentioned? : Other	**Other (please specify):**	**Please describe some specific technologies or technical standards that you have in mind, otherwise add N/A.**	**Please describe some specific organisational measures (e.g. skill sets, regulation, liability) that you think are important. Otherwise add N/A.**	**Should the Network and Centre push towards specialization of Member States and prioritize funding the development of different technologies in different Member States?**	**What additional information you would like to give us and that we forgot to ask for?**
Of Minor Importance		FIDO, France Connect and State Digital Identity	N/A	Only in special cases	N/A
		Anti-malware, anti-ransomware, trustworthy identication/authentication of individuals.	A cybersecurity skillset training program could be put in place for citizen, SME and large organisation so that their level of protection against cyber threats is optimised in accordance to their funding capacity.	Only in special cases	How can I contribute ? What is the role of the EIC in cybersecurity ?
		Standards for minimum security requirements of products and services and how to assess and verify them, initially and in market conformity assessments (ongoing).	It will be required that at least critical sectors will have to comply with requirements set by those standards, later expanding it to more and more sectors, up to general IoT	No	

1	2	3	4	5	6	7	8	9
Country	**If other please specify**	**You are employed in:**	**Other (please specify):**	**What is your area of work?**	**Other (please specify)**	**What is your position?**	**Other (please specify)**	**Are you directly involved in one of the EU pilot projects launched to prepare the European Cybersecurity Competence Network?**
United Kingdom		Industry		Professional, Scientific, and Technical Services		President/CEO/Member of Board		No
Germany		Academy		Research and Higher Education		Manager/professor/head of group		Yes
Greece		Academy		Information and communication		Officer/Researcher/Administrator/Member of Staff		Yes
Italy		Other	Finance	Finance and Insurance		Officer/Researcher/Administrator/Member of Staff		Yes
Estonia		Industry		Information and communication		Officer/Researcher/Administrator/Member of Staff		Yes

10	11	12	13	14	15	16	17	18
Are you involved in CyberSec4 Europe?	**Which of the following Cybersecurity Vertical Sectors is your main area of expertise?**	**If other, please specify:**	**Which of the following verticals of the pilots is your main area of expertise:**	**What Europe should achieve as an overall goal in cybersecurity?**	**In your specific area of expertise, what is the key cybersecurity situation that must change (e.g. better resilience, transparency, trustworthiness, security metrics...)? If possible, explain also the motivations behind your indications.**	**In your area, what key capabilities are required by systems, people, institutions, etc, to achieve that change?**	**What is needed to achieve the capabilities you just mentioned?: Novel Technologies**	**What is needed to achieve the capabilities you just mentioned?: New or improved technical standards**
				I'd suggest a balance, between privacy and security and facilitating functionaly, commercial and social interactons. Recognising the convergence of the cyber and physical worlds, especiall new services adn facilities from 5G and IoT now might be a good time to consider merging the cyber security (impirtant and specialised though it is) into the context of security in the round. A second point, adding (cyber) security as a business driver, e.g. SBD, and not an optional add-on might help buikd confidence and functionality.	See above.	Rounded and broad education of 'specialists' and the public and multi-disciplinary working witb the ability of specialists to speak to and understand one aother accross the cyber, physical, buinsess and operational domains.	Of Minor Importance	Of Major Importance
Yes			e-Health and Medical Data Exchange	high level of security and safety against attacks	trustworthiness More privacy more control over data	understanding of importance of IT structures understanding of importance of privacy low-cost-decisions	Of Major Importance	Of Major Importance
Yes			Maritime Transport	The main goal should be to enhance the security and resilience of Critical Information Infrastructures (CIIs) by providing advanced and innovative security and risk management solutions that are fully in-line with relevant regulations such as the GDPR and NIS directive.	_ Ports and maritime supply chain providers do not have a mature cybersecurity culture. Most EU commercial ports are not aware of emerging cybersecurity threats and are not prepared for catastrophic cybersecurity attacks. They do not perform regular risk assessments and they do not have incident handling strategies. _ Ports and maritime supply chain providers do not adopt "Good ICT supply chain security", i.e. they do not cope effectively with interdependent external threats _ Port authorities, maritime supply chain providers, governments and public authorities are reluctant to share cybersecurity-relevant information for fear of losing their reputation or of compromising commercial, enterprise or national security and competitiveness. Private undertakings are reluctant to share information on their cyber vulnerabilities and resulting losses for fear of compromising sensitive business information, risking their reputation or risking breaching data protection rules. Trust needs to be strengthened for public-private partnerships to underpin wider cooperation and sharing of information across a greater number of sectors. _ Certification plays a critical role in increasing trust and security in products and services that are crucial for the digital single market. At the moment, a number of different security certification schemes for ICT products exist in	_ Usage of big data and artificial intelligence technologies for the extraction of patterns in data and the identification of abnormal behaviors. _ Formulation of (soft) standards for information interoperability, focused on future systems that are relevant for maritime surveillance / maritime security, and taking into account commercial trade operations between logistics companies and (port) authorities. _ Integration of state-of-the-art elements for met/ocean prediction, risk prediction related to the occurrence of threats, sensor/platform allocation, and communications	Essential	Of Major Importance
Yes			Incident Reporting	In order to promote the economic development of the EU Digital Single Market, we all need to work to foster cybersecurity culture and to enhance EU cyber resilience.	Better coordination and information sharing would be beneficial to all major players especially to those linked to systemically relevant processes and critical infrastructures. While recent regulatory evolutions are already moving in this direction, additional joint public-private efforts are needed to overcome fragmentation and to operationalize coordination.	Besides the technical evolutions, that shall leverage the best available innovation to defend the assets that are possible targets under attack, there is a need for a paradigm shift, that takes cybersecurity as a major feature across all domains. This requires a revision of some processes, but first and foremost a need to spread cybersecurity culture, introducing the approach of security by design, that takes cybersecurity into account while building solution, rather than thereafter as an add-on. Next to this awareness programs shall disseminate a cyber-risk consciousness. In terms of people it is worth mentioning that we are going to		
Yes			Maritime Transport;e-Health and Medical Data Exchange	One topic that is very important for research to be possible is the sharing of data. However, if we are dealing with sensitive information, the data privacy issue becomes very important. It would be a great achievement if data were shareable in a privacy-preserving way between different countries in Europe.	At the moment, it is extremely difficult to share data internationally in a privacy-preserving way.	Data in different domains needs to comply to a specific standard (e.g., OMOP for the medical domain) and this would make it easier to include data from	Essential	Of Major Importance

19	20	21	22	23	24
What is needed to achieve the capabilities you just mentioned? : Other	**Other (please specify):**	**Please describe some specific technologies or technical standards that you have in mind, otherwise add N/A.**	**Please describe some specific organisational measures (e.g. skill sets, regulation, liability) that you think are important. Otherwise add N/A.**	**Should the Network and Centre push towards specialization of Member States and prioritize funding the development of different technologies in different Member States?**	**What additional information you would like to give us and that we forgot to ask for?**
Not Essential		Attack simulations tools (opensource). Standars to organize the mechanisms of simulation of attacks and the model of defense.	Coolaborated each other. Public new vulnerabilities each other in order to correct.	Yes	
Of Minor Importance		ARMOUR, RASEN and the associated ETSI standard. CVSS, CWSS and similars.	N/A	Only in special cases	
		ISAC - information exchange allow failure agile & dynamic non policy - partially risk oriented	education, training on the job, continuous improvement, leading by example, government first	Yes	
		N/A	N/A	Only in special cases	
		blockchain technologies; taxonomies for data analytics	standards for way of working and interpreting data on cyber attacks, training for young ICT professionals, knowledge exchange for SME's/companies to protect them from cyber attacks	Only in special cases	

1	2	3	4	5	6	7	8	9
Country	**If other please specify**	**You are employed in:**	**Other (please specify):**	**What is your area of work?**	**Other (please specify)**	**What is your position?**	**Other (please specify)**	**Are you directly involved in one of the EU pilot projects launched to prepare the European Cybersecurity Competence Network?**
Netherlands		Industry		Information and communication		Manager/professor/head of group		No
Greece		Academy		Research and Higher Education		Other	Faculty member	Yes
Other	Norway	Academy		Information and communication		Officer/Researcher/Administrator/Member of Staff		Yes
United Kingdom		Industry		Professional, Scientific, and Technical Services		President/CEO/Member of Board		No

10	11	12	13	14	15	16	17	18
Are you involved in CyberSec4 Europe?	**Which of the following Cybersecurity Vertical Sectors is your main area of expertise?**	**If other, please specify:**	**Which of the following verticals of the pilots is your main area of expertise:**	**What Europe should achieve as an overall goal in cybersecurity?**	**In your specific area of expertise, what is the key cybersecurity situation that must change (e.g. better resilience, transparency, trustworthiness, security metrics...)? If possible, explain also the motivations behind your indications.**	**In your area, what key capabilities are required by systems, people, institutions, etc, to achieve that change?**	**What is needed to achieve the capabilities you just mentioned?: Novel Technologies**	**What is needed to achieve the capabilities you just mentioned?: New or improved technical standards**
				Become world leader.	Knowledge distribution and funding. Most talent disappears towards the US, main reason is because the US is intellectually more challenging. There is not that much funding for new projects like there is in the US and China. Hence knowledgeable people disappear to one of those countries.	It's sad to say, but brilliant minds will disappear to spy agencies. At this moment those spy agencies are local, there's no European spy agency. If you combine these agencies knowledge will be shared between these people and new highs can be achieved. Simply said: the law of large numbers applies here. Group everything together, distribute it evenly, deduplicate, fund it propperly, profit! Make relocation easy!	Essential	Essential
Yes			Maritime Transport	Develop the cybersecurity skills and capabilities, in order to achieve technological cybersecurity independence with respect to third countries and to be able to adequately protect its critical infrastructures and services from cyber threats.	Better resilience	1) Cybersecurity awareness of the involved actors 2) Novel cybersecurity technologies following the resilience-by-design principle	Of Major Importance	Of Minor Importance
Yes			Maritime Transport	Become a world leader in reasearch and implementation Protecting the digital freedom of citizens	Very few digital services work across borders, this is hindering a lot of the economic potential for Eruope. Security research is fragmented, and there is a lot of duplication across Europe. Promising new companies move to Silikon Valley, they don't stay here.	Good communication Understanding of what is needed Enough resources	Of Major Importance	Of Minor Importance
				I'd suggest a balance, between privacy and security and facilitating functionaly, commercial and social interactons. Recognising the convergence of the cyber and physical worlds, especiall new services adn facilities from 5G and IoT now might be a good time to consider merging the cyber security (impirtant and specialised though it is) into the context of security in the round. A second point, adding (cyber) security as a business driver, e.g. SBD, and not an optional add-on might help buikd confidence and functionality.	See above.	Rounded and broad education of 'specialists' and the public and multi-disciplinary working witb the ability of specialists to speak to and understand one aother accross the cyber, physical, buinsess and operational domains.	Of Minor Importance	Of Major Importance

19	20	21	22	23	24
What is needed to achieve the capabilities you just mentioned? : Other	**Other (please specify):**	**Please describe some specific technologies or technical standards that you have in mind, otherwise add N/A.**	**Please describe some specific organisational measures (e.g. skill sets, regulation, liability) that you think are important. Otherwise add N/A.**	**Should the Network and Centre push towards specialization of Member States and prioritize funding the development of different technologies in different Member States?**	**What additional information you would like to give us and that we forgot to ask for?**
		Machine Learning Deep Learning Artificial Intelligence	N/A	No	-
		Targeted threat modelling and risk assessment technologies. Targeted trust management technologies.	N/A	Only in special cases	
		pan-european autthentication Payment services not relying on credit cards	Cross-disiplinary competence is needed (legal, technical, organisational, social knowhow)	Only in special cases	
		N/A	B/A	Only in special cases	

1	2	3	4	5	6	7	8	9
Country	**If other please specify**	**You are employed in:**	**Other (please specify):**	**What is your area of work?**	**Other (please specify)**	**What is your position?**	**Other (please specify)**	**Are you directly involved in one of the EU pilot projects launched to prepare the European Cybersecurity Competence Network?**
Germany		Academy		Research and Higher Education		Manager/professor/head of group		Yes
Greece		Academy		Information and communication		Officer/Researcher/Administrator/Member of Staff		Yes
Italy		Other	Finance	Finance and Insurance		Officer/Researcher/Administrator/Member of Staff		Yes
Estonia		Industry		Information and communication		Officer/Researcher/Administrator/Member of Staff		Yes

10	11	12	13	14	15	16	17	18
Are you involved in CyberSec4 Europe?	**Which of the following Cybersecurity Vertical Sectors is your main area of expertise?**	**If other, please specify:**	**Which of the following verticals of the pilots is your main area of expertise:**	**What Europe should achieve as an overall goal in cybersecurity?**	**In your specific area of expertise, what is the key cybersecurity situation that must change (e.g. better resilience, transparency, trustworthiness, security metrics...)? If possible, explain also the motivations behind your indications.**	**In your area, what key capabilities are required by systems, people, institutions, etc, to achieve that change?**	**What is needed to achieve the capabilities you just mentioned?: Novel Technologies**	**What is needed to achieve the capabilities you just mentioned?: New or improved technical standards**
Yes			e-Health and Medical Data Exchange	high level of security and safety against attacks	trustworthiness More privacy more control over data	understanding of importance of IT structures understanding of importance of privacy low-cost-decisions	Of Major Importance	Of Major Importance
Yes			Maritime Transport	The main goal should be to enhance the security and resilience of Critical Information Infrastructures (CIIs) by providing advanced and innovative security and risk management solutions that are fully in-line with relevant regulations such as the GDPR and NIS directive.	_ Ports and maritime supply chain providers do not have a mature cybersecurity culture. Most EU commercial ports are not aware of emerging cybersecurity threats and are not prepared for catastrophic cybersecurity attacks. They do not perform regular risk assessments and they do not have incident handling strategies. _ Ports and maritime supply chain providers do not adopt "Good ICT supply chain security", i.e. they do not cope effectively with interdependent external threats _ Port authorities, maritime supply chain providers, governments and public authorities are reluctant to share cybersecurity-relevant information for fear of losing their reputation or of compromising commercial, enterprise or national security and competitiveness. Private undertakings are reluctant to share information on their cyber vulnerabilities and resulting losses for fear of compromising sensitive business information, risking their reputation or risking breaching data protection rules. Trust needs to be strengthened for public-private partnerships to underpin wider cooperation and sharing of information across a greater number of sectors. _ Certification plays a critical role in increasing trust and security in products and services that are crucial for the digital single market. At the moment, a number of different security certification schemes for ICT products exist in	_ Usage of big data and artificial intelligence technologies for the extraction of patterns in data and the identification of abnormal behaviors. _ Formulation of (soft) standards for information interoperability, focused on future systems that are relevant for maritime surveillance / maritime security, and taking into account commercial trade operations between logistics companies and (port) authorities. _ Integration of state-of-the-art elements for met/ocean prediction, risk prediction related to the occurrence of threats, sensor/platform allocation, and communications	Essential	Of Major Importance
Yes			Incident Reporting	In order to promote the economic development of the EU Digital Single Market, we all need to work to foster cybersecurity culture and to enhance EU cyber resilience.	Better coordination and information sharing would be beneficial to all major players especially to those linked to systemically relevant processes and critical infrastructures. While recent regulatory evolutions are already moving in this direction, additional joint public-private efforts are needed to overcome fragmentation and to operationalize coordination.	Besides the technical evolutions, that shall leverage the best available innovation to defend the assets that are possible targets under attack, there is a need for a paradigm shift, that takes cybersecurity as a major feature across all domains. This requires a revision of some processes, but first and foremost a need to spread cybersecurity culture, introducing the approach of security by design, that takes cybersecurity into account while building solution, rather than thereafter as an add-on. Next to this awareness programs shall disseminate a cyber-risk consciousness. In terms of people it is worth mentioning that we are going to		
Yes			Maritime Transport;e-Health and Medical Data Exchange	One topic that is very important for research to be possible is the sharing of data. However, if we are dealing with sensitive information, the data privacy issue becomes very important. It would be a great achievement if data were shareable in a privacy-preserving way between different countries in Europe.	At the moment, it is extremely difficult to share data internationally in a privacy-preserving way.	Data in different domains needs to comply to a specific standard (e.g., OMOP for the medical domain) and this would make it easier to include data from	Essential	Of Major Importance

19	20	21	22	23	24
What is needed to achieve the capabilities you just mentioned? : Other	**Other (please specify):**	**Please describe some specific technologies or technical standards that you have in mind, otherwise add N/A.**	**Please describe some specific organisational measures (e.g. skill sets, regulation, liability) that you think are important. Otherwise add N/A.**	**Should the Network and Centre push towards specialization of Member States and prioritize funding the development of different technologies in different Member States?**	**What additional information you would like to give us and that we forgot to ask for?**
		N/A	n/A	No	
		security standards (e.g. ISO28000, ISO28001, ISO27001, ISO27005), directives (e.g. NIS, GDPS) and guidelines (IMO cybersecurity guidelines)	_ Risk assessment and management solutions and frameworks _ anomaly detection methods _ maritime surveillance platforms	Only in special cases	
		N/A	At least at EU level, an harmonization among different regulatory requirements related to cybersecurity issues would be highly appreciated by the private sector, and would be beneficial for all those multinational corporates that today have to cope with an excessive fragmentation.	Only in special cases	
		There are different ways of doing privacy-preserving data analysis, such as fully homomorphic encryption or secure multi-party computation. I would also bring out the OMOP common data model for the medical domain.	N/A	No	

Agenda Brainstorming Workshop of 6 June 2019

09:00	Opening	UPS-IRIT
09:20	E-Commerce	UPS-IRIT
09:45	Supply Chain Security Assurance	UMA
10:10	Privacy-Preserving Identity Management	KAU
10:35	Incident Reporting	UPS-IRIT
11:00	Coffee break	All
11:30	Maritime Transport	FORTH
11:55	Medical Data Exchange	KAU
12:20	Smart Cities	FORTH
12:45	Lunch	All
14:15	Experience sharing: Lessons learnt from D5.1	NEC
14:30	The higher vision from an economic actor	iBP
14:45	Conversation I: "Content: Salient & Common points"	All
15:30	Conversation II: "Form: The best manner to convey our content"	All
16:15	Next steps & Action points	UPS-IRIT
16:25	Closing	UPS-IRIT
16:30	Meeting ends	