



ENISA CYBERSECURITY MARKET ANALYSIS FRAMEWORK (ECSMAF)

APRIL 2022

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors, please use market@enisa.europa.eu

For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Louis Marinos (ENISA), Domenico Ferrara (ENISA), Silvia Portesi (ENISA), Eleni Tsekmezoglou (ENISA)

ACKNOWLEDGEMENTS

ENISA would like to thank the following persons and organisation:

- The ENISA Advisory Group, the ECCG and SCCG for their input during the scoping phase and for their feedback during the validation phase of this report;
- The Members and Observers of the ENISA Ad Hoc Working Group on EU Cybersecurity Market for their guidance and feedback during the validation phase of this report;
- Gartner Team for the support with the preparation of the framework;
- The ENISA Colleagues who provided input and/or review this report.

LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to the Regulation (EU) No 2019/881.

ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source.

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication.

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ENISA maintains its intellectual property rights in relation to this publication.





COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2022

This publication is licenced under CC-BY 4.0 "Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence <https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed, provided that appropriate credit is given and any changes are indicated".

For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

ISBN 978-92-9204-561-6 DOI 10.2824/55221



TABLE OF CONTENTS

1. INTRODUCTION	6
1.1 POLICY CONTEXT	6
1.2 PURPOSE, OBJECTIVES AND SCOPE	8
1.3 TARGET AUDIENCE	9
1.4 STRUCTURE OF THE REPORT	11
2. CONTENT OF THE ENISA CYBERSECURITY MARKET ANALYSIS FRAMEWORK (ECSMAF)	12
2.1 LOGICAL BLOCKS/MODULES OF ECSMAF	12
2.1.1 Market structure and segmentation	13
2.1.2 Demand-side research	15
2.1.3 Supply-side research	17
2.1.4 Technology research	19
2.1.5 Macro-Environmental Factors and Economic Market Characteristics	21
2.2 CONTEXTUALIZED ECSMAF COMPONENTS	23
2.2.1 Scoping the analysis and ECSMAF parametrization	24
2.2.2 Cybersecurity market taxonomy	26
2.2.3 Cybersecurity market trends	31
2.2.4 Market stakeholder types	32
2.2.5 Methods for collecting market data	34
3. RELATED AREAS	36
4. ISSUES, CONSIDERATIONS, CONCLUSIONS	40
4.1 GENERAL REMARKS	40
4.2 OPEN ISSUES AND WAYS FORWARD	41
A ANNEX: EXAMPLES	43
A.1 EXAMPLES OF MARKET STRUCTURE AND SEGMENTATION	43
A.2 EXAMPLES OF DEMAND-SIDE RESEARCH	44
A.3 EXAMPLES OF SUPPLY-SIDE RESEARCH	45
A.3.1 Example of Market Map	45



A.4	EXAMPLES OF TECHNOLOGY RESEARCH	46
A.4.1	Example of Scenarios and Technology Map	46
A.4.2	Example of market adoption forecast	47
A.5	EXAMPLES OF MACRO-ENVIRONMENTAL FACTORS AND ECONOMIC MARKET CHARACTERISTICS	48
B	MAIN ABBREVIATIONS	50



EXECUTIVE SUMMARY

In 2021, in its efforts to contribute to the achievement of its objectives as defined in the Cybersecurity Act (CSA)¹ and to the implementation of the ENISA Single Programming Document⁵, ENISA has kicked-off a series of activities in the area of cybersecurity market analysis.

Analysing how well cybersecurity products, services and processes succeed in the market is a key step in understanding how to improve their market diffusion, importance, quality and acceptance. Though cybersecurity has been considered in the past within market analysis efforts, the customisation and scoping of cybersecurity market analyses is still at low levels of maturity. Moreover, market data on cybersecurity products, services and processes are scarcely taken into account in the cybersecurity development life-cycle, e.g. within decision-making processes for the launching and development of cybersecurity initiatives, product ideas, policy actions, research funding, and deployments. By initiating this activity, ENISA delivers an important contribution towards a more targeted, market-driven decision-making process for the conception, launching and maintenance of cybersecurity products, services and processes within the EU.

This document is the cornerstone of ENISA activities in analysing the EU cybersecurity market: it presents a **cybersecurity market analysis framework** as a “cookbook” on how EU cybersecurity market analyses can be performed and be:

- *More transparent*: the fact that analysis method, parametrization, cybersecurity value chain, market trends and market stakeholders are fixed, leads to a more transparency as regards the results of the analysis.
- *More comparable*: by having set both the content of various components and the steps of the analysis process, the achieved results are more comparable, and thus reusable among various analyses performed.
- *More targeted towards specific cybersecurity value chains*: the availability of a standard taxonomy of cybersecurity value chains, allows for more targeted analysis with regard to specific cybersecurity areas, products, services and processes.
- *More customizable towards technology and market trends*: the possibility to customize an analysis according to various trends, allows for consideration of market dynamics by means for forecasts, market gaps and market niches.
- *More agile*: the inherent flexibility of setting market analysis foci and adapting accordingly the performed analysis process, increases agility of the proposed market analysis method.
- *More comprehensive*: the inclusion of all possible variables, criteria and contextual information on cybersecurity, as well as requirements and dependencies both from the supply and the demand sides, increases the comprehensiveness of the proposed market analysis method.
- *More coherence*: the use of the framework to perform market analyses facilitates information exchanges among specific market analysis reports by means of re-usability and coherence of created/maintained market information (both raw market data and analysis results).

The framework presented in this report is at its initial development phase. With increasing performance of cybersecurity market analyses, but also with interactions with stakeholders, ENISA will continuously develop, update and maintain the current framework to increase its efficiency and practicability. To this extent, it constitutes rather the starting point of a journey than a destination.

1. INTRODUCTION

In 2021, ENISA has initiated its activities in analysing the cybersecurity market. The Cybersecurity Act (CSA¹) has stipulated the task of performing market analyses in the area of cybersecurity (see also Section 1.1 below). Performing market analyses in the area of cybersecurity, constitutes a quite novel, yet challenging task because of the following:

- Given the considerable multiplicity of cybersecurity products, services and processes, a market analysis in this area may need to go significantly deeper than current market analysis practices;
- Cybersecurity functions are often “packaged” within existing products and services. As there is no established taxonomy or metrics in this area, it is difficult to collect and analyse information about detailed cybersecurity functions available. However, a detailed decomposition approach is often needed in order to assess various market characteristics of products, such as role, level of market penetration, market value, etc.;
- While until now market analyses and assessments have been performed mainly by experts with an economic background, cybersecurity market analysis requires significant, technically oriented cybersecurity knowledge;
- Finally yet importantly, the fact that cybersecurity products, services and processes entail a certain “blurriness” in their scope and boundaries, may introduce a certain degree of uncertainty in analyses and assessments, especially when innovation niches are in focus.

These facts indicate the need for developing differentiated analysis approaches, in order to encompass in the market analysis cybersecurity characteristics: unlike the rather high-level analysis of product and service markets, the analysis of cybersecurity market require novel approaches, based on novel market modelling, combined with cross-fertilization of skills.

The current document is an initial attempt to develop a market assessment approach and is meant to be a collection of tools to be used for cybersecurity market analyses. The developed approach comprises the ENISA Cybersecurity Market Analysis Framework (ECSMAF). The present output is expected to be an initial building block, an initial part of the content to be gradually developed in consecutive years. It will facilitate the analysis of the required market assessment, involved mechanisms and tools. On the outset, the definition of the cybersecurity market and its key components - in terms of products and services - will be addressed. During this development, market dynamics will gradually become integral part of this analysis², as the toolset developed will cover variety of needs and analysis requirements that will emerge through a series of cybersecurity market-analysis foci and objectives.

1.1 POLICY CONTEXT

As it has been stipulated in Article 8, as well as in Title III of the CSA¹, the consideration of developments in cybersecurity market constitutes a main focal point within CSA, in particular in the context of certification. Certification is considered as the main instrument to “*avoiding the fragmentation of the internal market*”³. In setting up Cybersecurity Certification, the main goal is “*to improve the functioning of the internal market*” (Art. 56 CSA). To achieve this goal, CSA foresees a number of actions to **analyse market trends**. These actions are mentioned in CSA, in particular where it provides that:

With ECSMAF, ENISA has created a toolbox for the performance of Cybersecurity Market Analyses. It introduces related content for targeted cybersecurity market analyses.

¹ <https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32019R0881&from=EN>, accessed November 2021.

² Market dynamics (and the cybersecurity market in general) are highly dependent on what is happening outside the EU, therefore defining the market geographically-wise would be needed.

³ See Article 1 par. 1 (b) CSA.

- “ENISA shall perform and disseminate regular analyses of the main trends in the cybersecurity market on both the demand and supply sides, with a view to fostering the cybersecurity market in the Union” (Art. 8 par. 7 CSA);
- “ENISA should develop and maintain a ‘market observatory’ by performing regular analyses and disseminating information on the main trends in the cybersecurity market, on both the demand and supply sides” (Recital 42 CSA).

In performing these tasks, ENISA receives advice and guidance from the Stakeholder Cybersecurity Certification Group (hereinafter, SCCG). The SCCG:

- “upon request, advise[s] ENISA on general and strategic matters concerning ENISA’s tasks relating to market, cybersecurity certification, and standardisation” (Art. 22 par. 3 (b) CSA).

The ENISA work on the EU cybersecurity market aims to contribute to reduce the EU internal market fragmentation and provides input to:

- The Union Rolling Work Programme for European Cybersecurity Certification by means of “market demand” (Art. 47 CSA);
- The promotion of “*the use of European cybersecurity certification, with a view to avoiding the fragmentation of the internal market [emphasis added]. ENISA shall contribute to the establishment and maintenance of a European cybersecurity certification framework in accordance with Title III of this Regulation, with a view to increasing the transparency of the cybersecurity of ICT products, ICT services and ICT processes, thereby **strengthening trust in the digital internal market and its competitiveness**” [emphasis added] (Art 4.6 CSA).*

Moreover, based on market information, ENISA provides support in the coordination of the Member States’ efforts in the area of market surveillance for supervision of certification⁴: The CSA provides that:

- The National cybersecurity certification authorities “*supervise and enforce rules included in European cybersecurity certification scheme [...] for the monitoring of the compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates that have been issued in their respective territories, in **cooperation with other relevant market surveillance authorities**” [emphasis added] (Art. 58 par 7 (a) CSA).*

The ENISA Single Programming Document 2012-2023 (SPD)⁵ takes into account these provisions and sets up corresponding actions under Activity 7, with the aim to “*to foster cybersecurity market in the Union and the development of the cybersecurity industry, in particular SMEs and start-ups, to reduce dependence from outside the Union and to reinforce supply chains inside the Union. It involves actions to promote and implement ‘security by design’ and ‘security by default’ measures in ICT products, services and processes, including through standardisation*”.

⁴ Knowing that this effort concerns mainly compliance issues of certification, it might provide valuable information on various aspects of the Cybersecurity Market. Thus, it may be used as a tool to obtain valuable information on the cybersecurity market. Though this facility is not yet operational, ENISA will coordinate efforts with Member States/Commission to increase the usability of this source within the context of the Activity 7 of the ENISA Single Programming Document (SPD) 2021-2023 (<https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-document-2021-2023>, accessed November 2021).

⁵ <https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-document-2021-2023>, accessed November 2021.

By delivering information on cybersecurity market, ENISA provides support towards the implementation of various Commission initiatives helping companies (SMEs, micro-enterprise) improve business/production processes, products, or services using digital technologies:

- European Digital Innovation Hubs⁶: market analyses provide evidence towards helping “SMEs expand and tap into other markets, develop EU value chains, create new business opportunities for companies or help commercialise earlier innovation experiments or pilots”⁷
- Emerging industries and value chains⁸: market analysis is an important instrument that may “help SMEs to innovate and develop cross-sectoral value chains by bringing different sectors and areas of expertise together to create new value chains across the EU and Horizon 2020 associated countries”.

1.2 PURPOSE, OBJECTIVES AND SCOPE

The purpose of the developed cybersecurity market framework is to serve a number of ENISA-internal, as well as Stakeholder needs. As regards ENISA-internal needs, one can highlight the following ones:

- To define a market analysis method capable of addressing the cybersecurity product, service and process market;
- To serve as a basis for amalgamation of knowledge emanating from market analysis and cybersecurity into a single knowledge source;
- To provide contextually detailed references to other related work, both within ENISA (e.g. areas such as research and innovation, cybersecurity index, policy development, knowledge and information) and outside ENISA (e.g. national market observatories, and national statistic organisations); and
- To be used as a model for prospective development of tools to support this task within ENISA, e.g. as a schema for storage of collected cybersecurity market data.

The satisfaction of these needs will empower ENISA to meet the following objectives:

- To identify potentially interesting cybersecurity fields that are innovative, emerging and represent a potential for both demand and supply;
- To identify cybersecurity market opportunities and risks based on demand and supply requirements;
- To assess the importance of relevant market segments to assess potential impact of incidents/threats/risks;
- To assess market needs for cybersecurity certification, and
- To leverage cybersecurity market data for informed decisions within EU and Member States cybersecurity policy actions.

As regards stakeholder needs, the proposed cybersecurity market framework aims at⁹:

- Serving as a model of reference for any stakeholder willing to engage in market analysis efforts;
- Helping vendors of cybersecurity products, services and processes to update their Go-To-Market strategies;
- Facilitating procurement and/or “make-or-buy” decisions, based on cybersecurity market data;
- Providing specific information about market developments w.r.t. cybersecurity products, services and processes;
- Identifying cybersecurity market trends w.r.t. market penetration of various cybersecurity products;

⁶ <https://digital-strategy.ec.europa.eu/en/activities/edihs>, accessed January 2022.

⁷ https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=70324, accessed January 2022.

⁸ https://ec.europa.eu/growth/industry/strategy/cluster-policy/emerging-industries-and-value-chains_en, accessed January 2022.

⁹ Stakeholder needs-list is indicative and non-exhaustive. Needs mentioned here are the ones assessed by ENISA so far.

- Assessing cybersecurity requirements to products, services and processes formulated by the demand side, and
- Providing terminology to understand of market segmentation in the area of cybersecurity;

It should be noted, that the proposed framework aims at analysing classes of cybersecurity products, processes and services, but not individual ones (i.e. by means of individual evaluations).

This initial version of ECSMAF lays the foundation for a robust structure that can be applied to existing market data and deliver satisfactory results.

The framework has been piloted and validated by means of an analysis in the area of interconnected devices. While the experience gained from this pilot are already fed back to the present methodology, an ongoing extensive review from the established Ad Hoc Working Group (AHWG) on the EU Cybersecurity Market¹⁰ is currently being performed. The received feedback will be taken account of in the continuous development effort of the framework.

For 2021, the validation of the developed framework is based on data and analysis prepared by external market analysts. As the knowledge on the ENISA Cybersecurity Market Analysis Framework matures, additional information sources will be included, such as own surveys, stakeholder feedback and OSINT.

As regards the supply and demand side, the current focus is on business-to-business relationships. The focus is mainly on companies that are in the “radar” of market analysis firms, and especially the ones dominating individual market segments. Emphasis has been given to requirements of operators of essential services (OESs) as well as regulated areas.

It should be noted, that when using the proposed framework, the size of business to be addressed (both demand and supply sides) depends on the survey scope. If desired, any size of business can be addressed. Depending on the scope, different stakeholder engagement and specific surveying techniques will be needed.

The proposed framework can be used for various market segments, in particular those that are related to cybersecurity (see also discussion about possible market stakeholder types and vertical industries in Section 2.2.4). In doing so, the framework can also be utilized to analyse certification market requirements, or market coverage of certified solutions in various vertical industries. Equally, it can be used to analyse market penetration of various cybersecurity products, services and processes, as they also make up a specific vertical industry. The introduced cybersecurity value chain and value stack components will enable an analysis at various levels of detail (see also Section 2.2.2).

In its current, initial, version, the framework remains at a relatively high level as regards its modules and their content. This is due to the relatively coarse granularity of available market data, as result of the low penetration of cybersecurity content at the level of market analysis organizations. In forthcoming versions, when alternative information collections methods will be used, a higher level of details regarding cybersecurity content will be striven for.

1.3 TARGET AUDIENCE

By constituting a set of tools and general-purpose components for cybersecurity market analyses, ECSMAF is potentially useful for a variety of stakeholders engaging directly or

¹⁰ The ENISA AHWG on the EU Cybersecurity Market has been established following the Call for expression of interest published at https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ad-hoc-working-group-on-cybersecurity-market, accessed November 2021.

indirectly in the area of market analysis. Below we provide some examples of such stakeholders, by stating potential elements of their market analysis related focus:

- *EU institutions, bodies and agencies (EUIBAs) (e.g. DG-CNECT, DG-GROW, DG-JRC, European Cybersecurity Competence Centre - ECCC, DG-RTD, DG-TRADE, Eurostat, etc.):* EU regulation often takes into account market issues, especially if it targets the EU internal market. Moreover, market analysis can be part of performed impact assessments of various decision-making activities prior to regulative texts. Market analysis activities hold a central role in any kind of statistics developed to assess market trends, as well as product related demand and supply issues. For all these use-cases, EUIBAs may use the content of ECSMAF to perform targeted market analyses covering market penetration of cybersecurity products, services and processes. Finally, the structuring presented within this work, can be a useful source of ideas to cover other areas (e.g. by adapting the taxonomy used to other thematic areas, by using the proposed scoping and parametrization workflow, and by using trending method).
- *Member States/Public Authorities (e.g. Cybersecurity Authorities):* The creation of cybersecurity market-surveillance activities at the level of EU Member States is subject of regulation (e.g. CSA). Reportedly, various EU Member States are about to create such capabilities, particularly in the area of market surveillance¹¹. Just as described above for the EUIBAs, Member States may use the proposed framework in a similar way. Moreover, ideas and practices developed by Member States may be consolidated in ECSMAF. This will facilitate mutual use of (open source) collected data, allowing thus for the implementation of synergies (e.g. data exchange, comparability of market analysis, and definition of common efforts).
- *ENISA Stakeholder Groups (e.g. ECCG, SCCG, ENISA Advisory Group):* By playing an important role in the area of EU-wide certification, members of these stakeholder groups may use the developed material to oversee market parameters affected by certification efforts. The developed material can serve as a decision-making basis for prioritizing certification efforts that are related to needs/requirements of both supply and demand. Moreover, ECSMAF can serve as guidance in spotting market gaps, providing thus outlooks for future certification activities.
- *Industry and Industry Associations (Ecosystem of Certification, EU TIC Council, Vendors / Manufacturers, ECSO):* The cybersecurity industry will be in the position to perform targeted market analyses for various cybersecurity products and for various sectors by supporting a variety of foci. Gap analysis (e.g. demand requirements vs. supply functions/features) may lead to early identification of market trends, thus enhancing time-to-market for new products, services and processes. Both elements can lead to the creation of competitive advantages to EU industry players and support the internal market for product, process and processes in the area of cybersecurity.
- *Consumer Organisations/Associations:* By using the proposed method/framework, such organisations may assess existing good practices for products, services and processes targeting the sector of their associated members. Moreover, they can capture requirements from the demand side, identify relevant gaps in the cybersecurity market, and assess market penetration of members' products, services and processes. Such information may be useful for cybersecurity product-, service- or process-procurement decisions.

¹¹ https://ec.europa.eu/growth/single-market/goods/building-blocks/market-surveillance/organisation_en, accessed January 2022.



- *Research Institutions and Research related entities*: Given their inherent interest in performing research creating competitive advantages in the European market, research institutions may:
 - use the proposed methodology to assess market areas that can affect the maturity of existing products;
 - cover market niches;
 - provide products, services and processes for emerging technology areas; and
 - use the proposed methodology to assess the market impact of deployed results.

1.4 STRUCTURE OF THE REPORT

The present document is organised as follows:

- *Chapter 1* (this chapter) presents the policy context, the purpose, objectives and scope of this report, the target audience, and the structure of the report.
- *Chapter 2* presents the entire structure, modules and content of ECSMAF. Besides the number of foreseen modules, it also presents a series of contextualized components, that is, components that capture cybersecurity related content and parametrization options for setting the scope of analyses (see chapter 2).
- *Chapter 3* presents the main interfaces of ECSMAF with other topics/ENISA activities, illustrating thus the “interaction” of the proposed method with other related work, both within and outside ENISA. This discussion sets the broader relationship of cybersecurity market analysis with activities in the area of cybersecurity, helping thus the reader to comprehend existing dependencies and interfaces (see chapter 3).
- *Chapter four* concludes the report by stating various issues encountered and formulating conclusions and future work (see chapter 4).
- *Annex A* contains examples of outcomes of the ECSMAF modules. This supporting information aims at increasing the understanding of the purpose of the developed framework (see Annex 4.1A).
- *Annex B* contains a table with Main Abbreviations.

2. CONTENT OF THE ENISA CYBERSECURITY MARKET ANALYSIS FRAMEWORK (ECSMAF)

This chapter gives an overview and provides the details of the various modules of the developed ENISA Cybersecurity Market Analysis Framework (ECSMAF). It delivers an overview and describes the various components. It has to be noted that in 2021 an initial version of the framework has been developed. With increasing experience in the field of market analysis, the proposed structure and components will be further specified/adapted to cover all aspects emerging during specific analyses.

The material presented below consists of two main component categories:

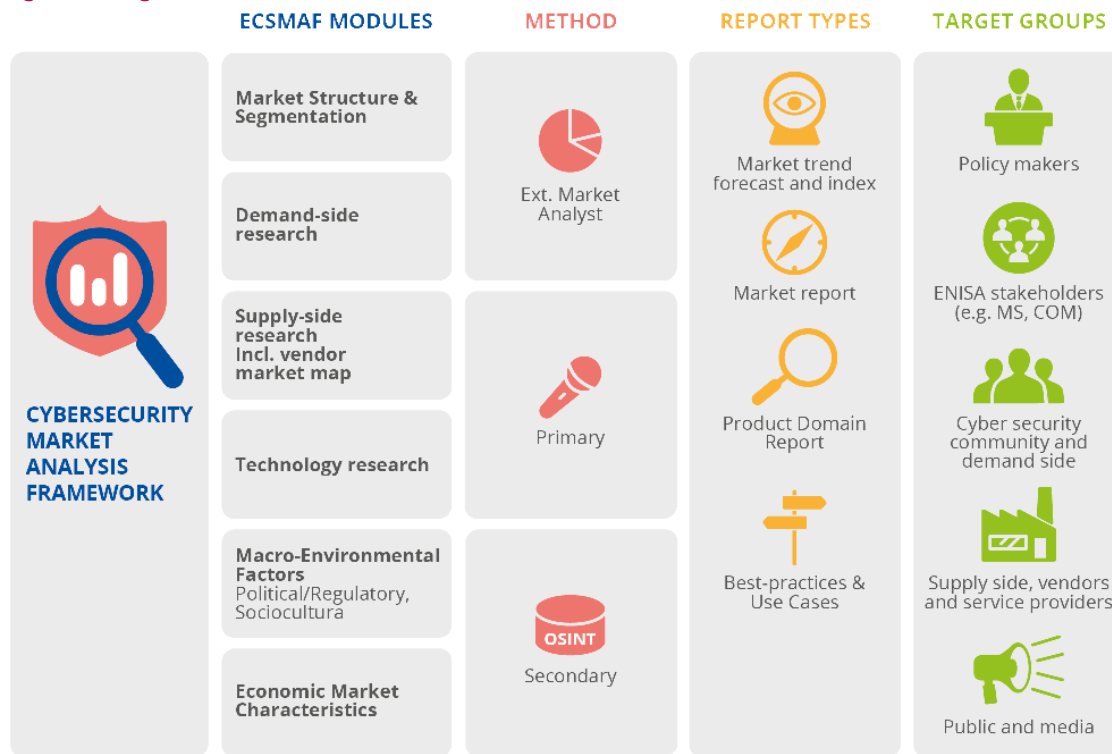
- **Logical blocks/modules of ECSMAF:** These modules represent the various aspects covered within an analysis and correspond to various content groups/phases performed for various market report types. These modules originate from generic market analysis techniques (see Section 2.1) rather than cybersecurity knowledge; and
- **Components that establish the cybersecurity context:** These are components capturing the structure and peculiarities of cybersecurity and helping to parametrise ECSMAF according to the selected scope of the analysis. They deliver scoping methods for cybersecurity market analysis based on typical cybersecurity-centred approaches (e.g. asset, threat and risk based, policy relevance, market measures, etc.). Moreover, they cover thematic topics of cybersecurity by means of a cybersecurity taxonomy to capture the entire value chain and value stack of cybersecurity products, services and processes. Cybersecurity trends and cybersecurity market stakeholder participating in the market roundup the cybersecurity market analysis context (see Section 2.2).

This chapter provides the available details of these categories of ECSMAF components.

2.1 LOGICAL BLOCKS/MODULES OF ECSMAF

The set of logical components of the developed framework are depicted in Figure 1 below.

Figure 1: Logical blocks/modules of ECSMAF



As can be seen in the figure above, the modules cover several elements required by CSA¹, such as the distinction between supply and demand, the inclusion of supply-chain, the consideration of trends, the consideration of socio-economic, policy and regulation aspects, as well as technology trends.

The six modules of the proposed method are subject to parametrization, prior to their execution (see Section 2.2.1). Parametrisation of the framework creates the scope for the analysis to be performed. It may lead to selective execution of the modules according to the needs of the analysis. To this extent, the modules are not performed in a sequential manner (i.e. waterfall model), but they can be configured in an agile way according to the analysis needs.

In the following sections, we give an overview of the various modules (see six ECSMAF modules in the figure above) and provide some examples demonstrating the kind of information that may be delivered through each module. The rest of the elements shown in Figure 1, namely Method, and Target Groups are discussed in Sections 2.2.5 and 1.3, respectively. Report Types are presented by means of examples in the Annex A (see Annexes A1-A4).

2.1.1 Market structure and segmentation

The module Market Structure and Segmentation has an important role in the entire market analysis. It is the phase where the scoping of the market analysis is being set. It consists of two main steps: the **determination of value chain at scope** and the **determination corresponding value stack**. The used definitions for value chain and value stack are as follows:

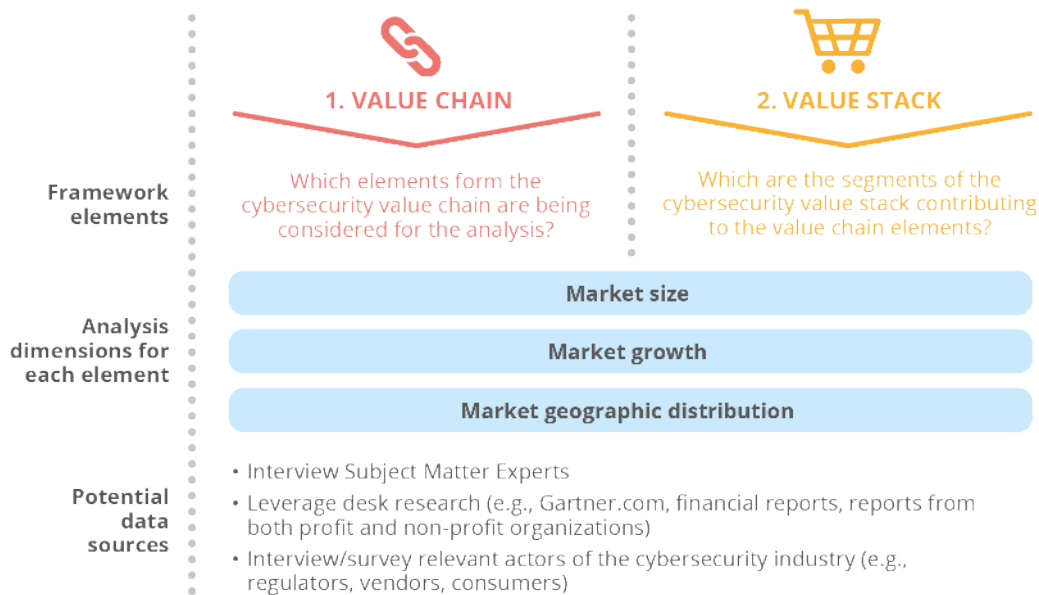
- Value Chain:** the term is used in accordance with the Porter’s Value Chain¹². Given the technological background focus of cybersecurity, emphasis is given to the primary value chain elements operations and services, as well as the secondary elements, infrastructure, technology development and procurement.

¹² <https://www.ifm.eng.cam.ac.uk/research/dstools/value-chain/>, accessed November 2021.

- Value Stack:** value stack is a collection of various activities contributing to the value production of an organisation. These activities may be manifold, supportive to a product or service and are necessary/vital for a value production fulfilling certain standards (e.g. quality, security, compliance, etc.). The Value Stack is considered particularly relevant for technology¹³. Following a similar approach, we consider the value stack as an element to decompose cybersecurity related topics. In ECSMAF, the value stack follows the structure of the introduced cybersecurity market taxonomy, representing a decomposition of cybersecurity topics and products, services and processes hereof. The cybersecurity market taxonomy, and conversely the value stack, is a notion that transcends ECSMAF and is used in various modules. A detail description of the cybersecurity taxonomy can be found in Section 2.2.1.

Figure 2 depicts these two steps (determination of value chain at scope and the determination of the corresponding value stack) as part of Market Structure and segmentation module.

Figure 2: Structure and steps within the module Market Structure and Segmentation



As regards the applicability of the above two steps, they heavily depend on the scoping workflow foreseen before the use of the five modules described. This workflow –described in a dedicated section below (see Section 2.2.2) - is of great importance for the identification of primary and secondary value chain elements and the depth of their decomposition via the value stack.

Main parameters for the scoping are:

- The market-research questions that need to be covered by the analysis;
- The identification of the necessary depth of analysis; and
- The availability of resources and sources for the market analysis (see examples of sources in Figure 2).

¹³ <https://www.linkedin.com/pulse/value-stack-4-powers-creation-tech-companies-daan-witteveen/>, accessed November 2021.



Given the business sector, product, service or process under analysis, and the expectation of a reasonable depth in the analysis, the determination of value chain at scope and the determination of the corresponding value stack may result in:

- An infrastructure diagram within the boundaries of the defined focus;
- A set of products, service processes in focus;
- Any related technical and organisational assets involved in the above (e.g. procurement);
- Cybersecurity related elements (products, services and processes) involved, and
- Market parameters of the above regarding market sizes, cost structures (e.g. CAPEX, OPEX, growth projections and geographic distribution).

Examples of information derived via the module Market Structure and Segmentation are given in Annex A.1.

2.1.2 Demand-side research

Although research on demand-side is a well-established topic in market research¹⁴, if it is placed within a cybersecurity focus it implements an important and rather novel element: it aims at capturing a variety of market-related information from (business-) end-users of cybersecurity market products, services and processes. This includes information about value-chain and value-stack of the relevant industry (i.e. the business value-chain to be protected), demand volume and growth, market trends, maturity of operations, and requirements (e.g. derived from the value-chain/value stack of the demand side, including thus procurement, operations and infrastructure). In other words, demand-side research contributes towards understanding protection requirements of valuable business assets. What it makes this module special is that it encompasses:

- User-needs emerging from dynamic changes of threat exposure of available business (through changes in the threat landscape);
- Requirements emerging from business and technological developments, and
- Experienced impact on businesses.

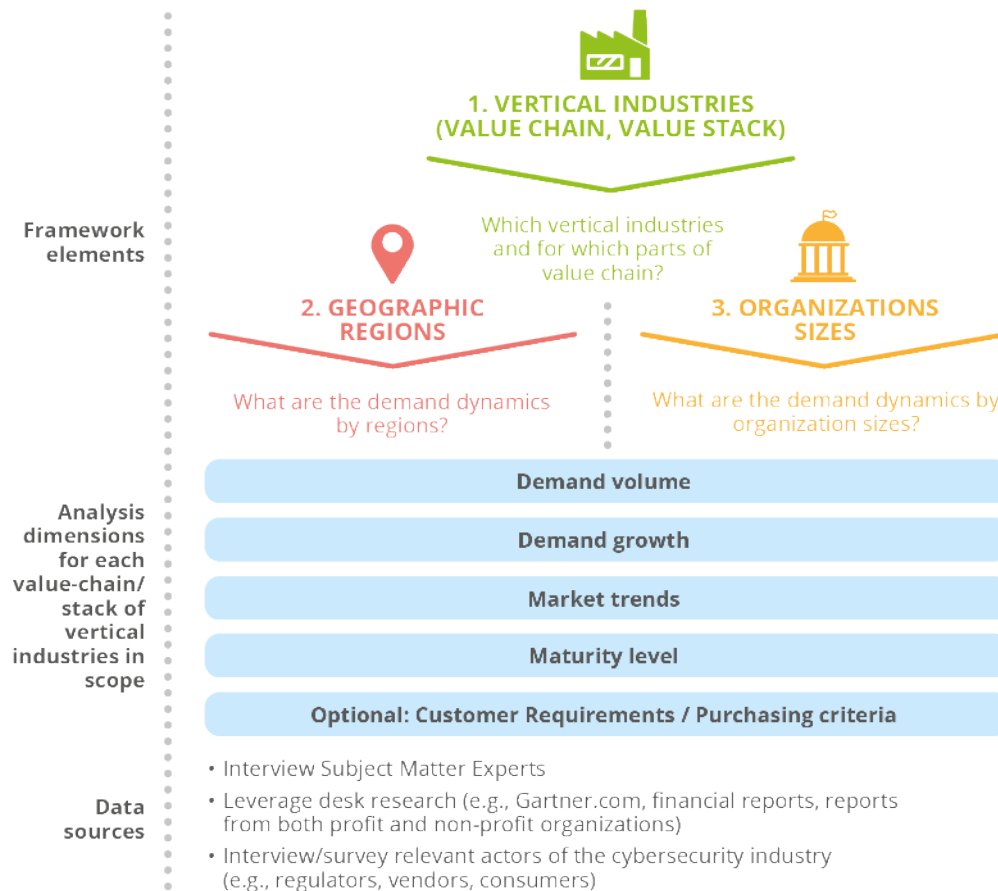
These dynamic changes are capable of leaving their footprint in the market at a high speed.

The structure of this module is depicted in Figure 3 below.

¹⁴ <https://www.investopedia.com/ask/answers/040915/what-demandside-economics.asp>, accessed November 2021.



Figure 3: Structure and steps within the module Demand-side Research



It is worth mentioning that the value-chain and value stack information of the demand side will not be identical with the ones of supply. While the demand side is an analysis of user-needs and requirements, supply side research takes into account market products offerings. The juxtaposition of these two views allows for the identification of market gaps, a very desirable piece of information in cybersecurity market analysis. Expectedly, potential market gaps will be visible from the assessed market trends of the demand side (i.e. comparison between demand requirements and functional characteristics of available product). On the contrary, assessed maturity levels and requirements may be useful for the identification of available offerings of the supply side.

The content of this ECSMAF module is created through an iterative process with the content of the previous model, Market Structure and Segmentation: the results from the execution of the previous module (see Market Structure and Segmentation above) deliver input for Demand-side Research. This happens by means of the value-chain elements identified in market structure. Demand-side should detail value-chains (e.g. by providing value stack information), or, in case a demand-side value-chain emerges in the demand-side assessment, it needs to be checked upon compliance to the market structure/segmentation results. Value-chain and value stack data have to be kept consistent in both modules.

As regards the results from the analysis, one can note the following:

- **Demand volume and growth** can be analysed starting from basic financial data. However, depending on the detail of the analysis (e.g. value stack), such data might be difficult to find/collect. Hereto, corresponding data sources will need to be used.

- **Market trends** can be of manifold nature. Some industries - typically with low risk - might need to follow technological developments. Others might orient themselves towards changes in the threat landscape affecting their sector. In those cases, market trends can be connected to technology foresight and threat analysis/landscaping, respectively.
- Cybersecurity **maturity** can be analysed through the penetration of cybersecurity products in the value-chain of an organisation, through the ratio of cybersecurity spending in IT-investments, through the number of incidents impacting their business, level of cybersecurity capability, etc.
- **Security requirements** – the most appropriate way to express demand needs – will be possible/efficient for rather detailed analyses focussing on detail elements of value-chain. Such data are usually difficult to find, especially if the market analysis scope included various stakeholders with varying maturity. For some areas, however, it will be possible and meaningful to track such requirements (e.g. in the area of certified products, services and processes).

Examples of information derived via the module Demand-side research are given in Annex 4.1A.2.

2.1.3 Supply-side research

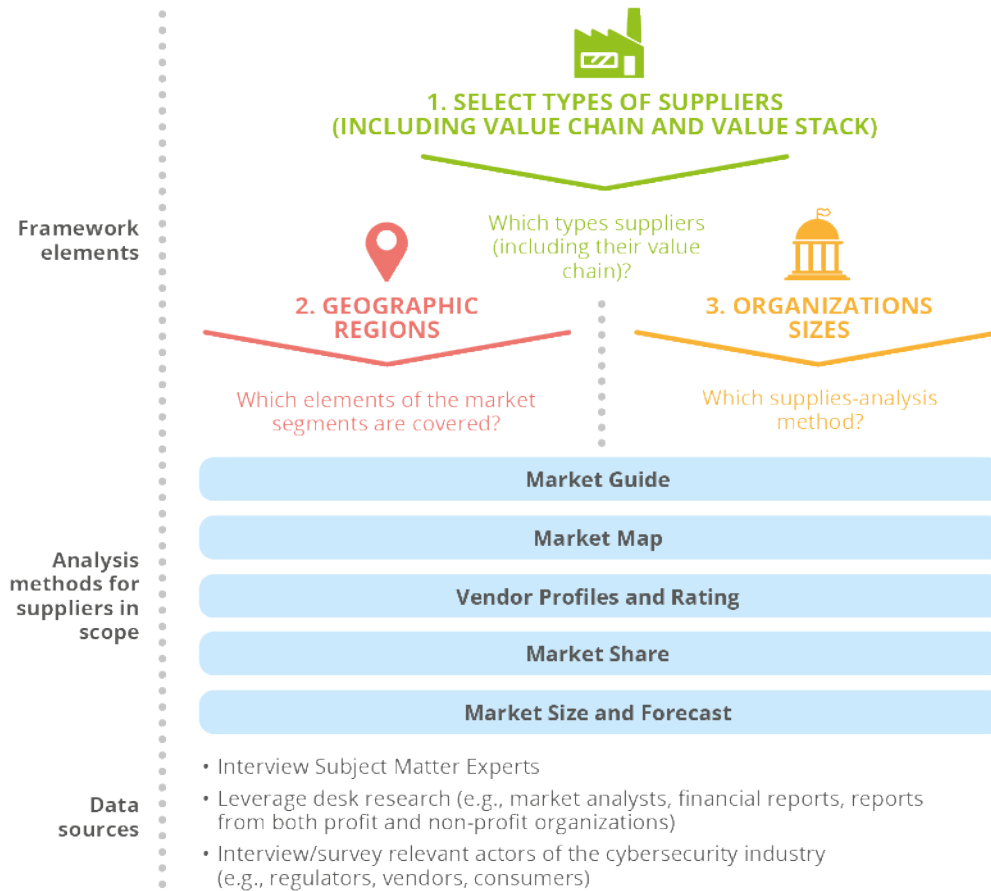
The module Supply-side research aims at analysing suppliers of cybersecurity products, services and processes. The research of supply is a very commonly performed activity within market analysis efforts. It is a baseline activity in market analysis and comprises a well-defined and highly matured domain of market research^{15,16,17}. So are the types of market reports covering the supply-side analysis, e.g. Market Guides, Market Maps, Vendor Profile Ratings, Market Shares and Market Size and Forecast. The structure of this module is depicted in Figure 4 below.

¹⁵ <https://www.coursehero.com/file/53744086/supply-side-substitution-2682pdf/>, accessed November 2021.

¹⁶ <https://www.biblio.com/book/macroeconomics-private-public-choice-gwartney-james/d/1438025693>, accessed November 2021.

¹⁷ <http://faculty.citadel.edu/sobel/GwartneyEcon14e.pdf>, accessed November 2021.

Figure 4: Structure and steps within the module Supply-side Research



The three activities within this module have the following purpose:

- **Select supplier types:** Given the focus of the market analysis (see also section 2.2.2), a set of supplier types will be selected. The various types of market stakeholders are drawn from the collection of market stakeholder types (see also section 2.2.4). Corresponding value-chain elements describing the products, services and processes will be identified for each supplier type taken into consideration. The level of detail for the value chain will depend on the focus of the market analysis exercise and will be in terms of value stack elements (including cybersecurity-related value stack elements as described in Section 2.2.1).
- **Create supplier mapping:** Within this activity, the mapping of the vendors meeting value-chain, value stack and other criteria (e.g. geographies, sizes and growth) is being performed. Some of these criteria are defined in module Market Structure and Segmentation, while value-chain and value stack are subject of the parametrization, on the one hand, and meet demand-side criteria/requirements on the other.
- **Create supplier analysis report(s):** In this activity, a supply-side report is created consolidating the information created in the previous two phases (which are Select supplier types and Create supplier mapping). The types of report should be selected according to the market research questions and the target group of the analysis. Most common report types for supplier-side research are (but not restricted to):

- *Market Guide/Market Landscaping*¹⁸: which is an overview of representative vendors;
- *Market Map*¹⁹: which defines the market from a supply-side perspective and should be as comprehensive as possible w.r.t. value chain and value stack, in particular if it is used as a baseline for market share analysis. The market map is a critical element to estimate vendor revenues per market segment; (see report example 4.1A.3.1);
- *Vendor Profiles*²⁰ and *Rating*²¹: where vendors are profiled and rated based on different methodologies e.g. Company overview, SWOT profiling (Strengths / Weaknesses / Opportunities / Threats), Magic Quadrant and Vendor Rating. Key results are typically used / referenced in the market map e.g. vendor overall rating; (see report example 4.1A.3.2);
- *Market Share*²²: which is a report predominantly quantitative but usually complemented with qualitative observations;
- *Market Size and Forecast*²³: where the baseline for market size is the revenue determined by a market map.

In order to draw parts of the content of supply-side research, iteration cycles with demand-side research, technology research and market structure will be necessary.

Examples of information derived via the module Supply-side research are given in Annex 4.1A.3.

2.1.4 Technology research

The aim of this module is to assess the impact of future technology and innovation in the relevant market. While it takes into account technology foresight, it also assesses state-of-play in research, thus estimating the readiness of available technology research results towards market deployment. Based on this information, this module evaluates the impact of the adoption of new technologies in the market, as well as time horizons for technology adoption. Though instruments of the latter kind already exist²⁴, the contextualization of such analyses for the area of cybersecurity is still out of the scope: Important variables to such a contextualization for cybersecurity technology may depend on different factors than in products, such as threats, cybersecurity challenges, impact statements, compliance, etc. As an example hereto, one can mention the necessity to map more generic trending information (e.g. digitization of everything) to the specific sector/scope at hand (e.g. how digitization of everything applies to the automotive sector).

Besides delivering evidence to perform market projections for prospective market sizes, technology research delivers information about trends. Hence, it contributes to the other modules - especially demand-side research -, by providing forecasts about upcoming demand-side requirements and technology-adoption preparedness and plans.

The activities of this module are presented in Figure 5 below:

¹⁸ <https://www.bridgespan.org/insights/library/nonprofit-management-tools-and-trends/market-mapping-and-landscape-analysis>, accessed November 2021.

¹⁹ https://en.wikipedia.org/wiki/Perceptual_mapping, accessed November 2021.

²⁰ <https://rfp360.com/vendor-profiles/>, accessed November 2021.

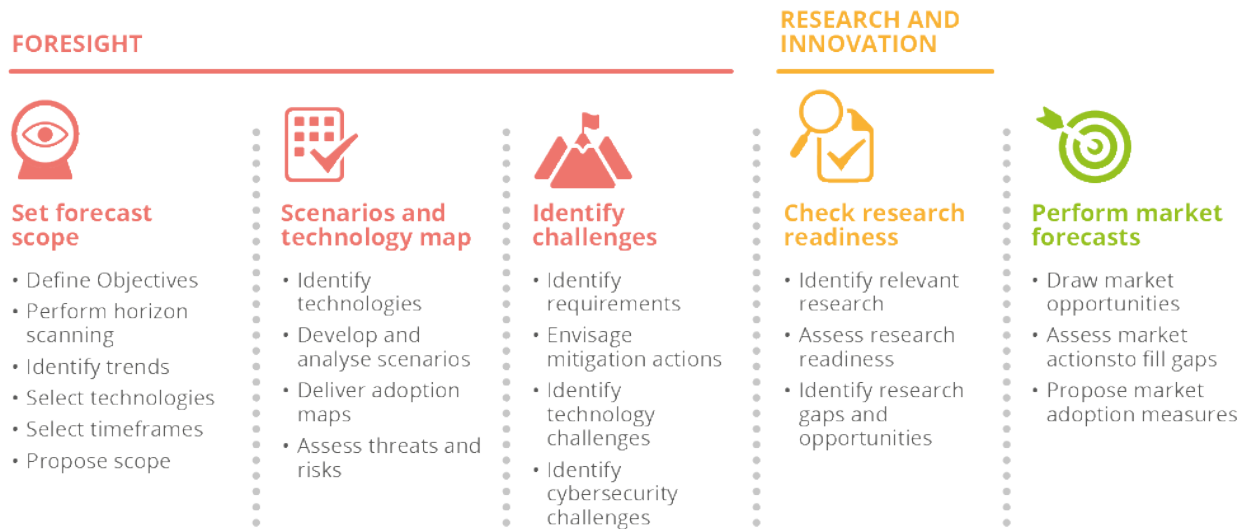
²¹ <https://www.gartner.com/en/research/methodologies/vendor-rating>, accessed November 2021.

²² <https://www.gartner.com/en/research/methodologies/market-share>, accessed November 2021.

²³ <https://www.mindtools.com/pages/article/market-sizing.htm>, accessed November 2021.

²⁴ <https://www.gartner.com/en/research/methodologies/gartner-hype-cycle>, accessed November 2021.

Figure 5: Structure and steps within the module Technology research



The various steps depicted in Figure 5 above make up the full scale of the activities of the module technology research. Below a short description of each step is given:

- Set forecast scope:** In this step, the scope of the module is being set. It consists of defining the objectives by means of concentrating on a certain part of technology and time-horizon, by also taking into account the overall scoping of the cybersecurity market analysis scoping and customisation, as described in Section 2.2.2 below. Within the remits of this customisation, a horizon-scanning activity, followed by the selection of the relevant technologies and trends within the defined period is being performed.
- Scenario and technology map:** By means of scenarios built for the use of the technology in scope, indicative development of trends is simulated. The scenario-building activity is important for understanding the context of technology-adoption within a use-case and its stakeholders, helping understanding its effects in all dimensions of the use-case. Based on the scenarios, a technology map is being developed to demonstrate the role/adoption of each technology in scope in the scenario constellation. For each particular scenario, an initial threat and risk assessment is being developed.
- Identify challenges:** Besides the assessed threat and risks of the previous step, stakeholder requirements for the various scenarios are being collected. Together the outcome of the threat/risk assessment of the previous step, requirements build up the basis for envisaging mitigation options/actions. Mitigation of risks, reduction of threat surface and fulfilment option of stakeholder requirements is the main source for the identification of cybersecurity challenges in relation to new technologies. Further to that, additional, cybersecurity-independent challenges are being envisaged. Technology challenges are related to deployment, operational and societal issues of technology adoption.
- Check research readiness:** In this step, research results – relevant to technology areas in scope - from various open source research activities (e.g. European projects, national and international research actions/projects), will be assessed in terms of their readiness levels²⁵. In this way, the maturity of available research results will be estimated. This information leads to the identification of gaps and opportunities related to the successful deployment of available research results that might influence innovation in the market

²⁵ https://ec.europa.eu/isa2/sites/default/files/technology_readiness_revisited_-_icegov2020.pdf, accessed November 2021.

segment in scope. As this task is highly prioritized within EU (e.g. European Cybersecurity Competence Centre, European Innovation Council, ENISA and in particular the work of the ENISA Research and Innovation Team²⁶), it is tightly related to actions around strengthening European research and innovation agenda.

- **Perform market forecasts:** The above-mentioned information is used in the performance of forecasts for adoption options of (cybersecurity) technology in the market. It will mainly be based on the assessed opportunities for the analysed use-cases/scenarios. If required, it may also propose corrective actions for filling identified gaps, should those being sought as enablers of major market drivers in the technology field, sector and geographical area in scope. The resulting proposals constitute market adoption measures for the technologies at scope.

As indicated in Figure 5, the majority of the discussed steps (1-4), are related to other disciplines than purely those relevant to market analysis. In particular, steps 1-3 (Set forecast scope, Scenario and technology map, and Identify challenges) are subject of the thematic area of foreseeing, an activity that is included in the ENISA Single Programming Document and covered by already published ENISA work²⁷. Whereas step 4 (Check research readiness) is a component of the work area of Research and Innovation, covered by a dedicated team within ENISA²⁸. These interfaces underline the links of cybersecurity market analysis with other disciplines and establish important knowledge exchanges hereto. By activating these interfaces within cybersecurity market research, all available ENISA results will be fully integrated into market analysis efforts.

Examples of information derived via the module Technology Research are given in Annex 4.1A.4.

2.1.5 Macro-Environmental Factors and Economic Market Characteristics

Market analysis is typically carried out by considering multiple perspectives, in order to provide a compressive overview of key trends. In this respect, the PEST analysis²⁹ is one of the most frequently applied measurement tool used to analyse how four external factors (Political, Economic, Social and Technology)³⁰ affect the operations of an organisation or a specific market segment

Once analysed through PEST, these factors would help public and private organisations understand potential impacts through scenarios, take better decisions, allocate resources more efficiently and introduce changes to generate improvements in suboptimal and impacted areas. PEST methodology is also employed for tracking developments across these four factors, identify current and future opportunities and risks, allowing for effective preparation of how to best manage them.

The process for carrying out the PEST analysis typically include the following main stages:

- Identification of the key events within the four external factors;
- Analysis of possible impacts on the organisation or market segment;
- Categorization into opportunities and threats: and
- Tracking of the trends.

²⁶ See ENISA organisational chart, in particular Research and Innovation team (RIT): <https://www.enisa.europa.eu/about-enisa/structure-organization>, accessed December 2021.

²⁷ <https://www.enisa.europa.eu/publications/foresight-challenges>, accessed December 2021.

²⁸ ENISA organisational chart: <https://www.enisa.europa.eu/about-enisa/structure-organization>, accessed December 2021.

²⁹ https://en.wikipedia.org/wiki/PEST_analysis, accessed December 2021.

³⁰ Variants that build on the PEST framework include PESTLE, which puts more emphasis on the legal and environmental factors.

On this basis, organizations can develop corrective or pre-emptive strategic actions.

The following PEST analysis example clarifies how the four external factors work and what type of information should be included in the analysis:

Table 1: PEST analysis example

Factor	Political	Economic	Social	Technological
Event	e.g. increased geopolitical tensions;	e.g. cost of production	e.g. emerging cultural consciousness	e.g. technological advancements
Possible impact	e.g. trade barriers to protect domestic suppliers;	e.g. high energy price may increase cost of production	e.g. adjust to new consumers' preferences such as environmental concerns	e.g. new technology can be adopted to be ahead of competitors
Type of impact (opportunity and threat)	negative	possibly negative	unknown	positive
Tendency	unchanged	increasing	increasing	unchanged

Due to its wider applicability and good-practice status, PEST analysis is used within ECSMAF in the Macro-Environmental Factors and Economic Market Characteristics modules (see Figure 1) to determine how these external factors affect the performance and trends of a market segment under examination. PEST analysis will complement the other insight layers adding new perspectives and potential scenarios, especially technology research, where trends are assessed.

The present section provides additional details regarding the external factors part of the PEST analysis with illustrative examples for each factor.

The **Political factor** of the PEST methodology aims to assess how new government policies and changes in legislation affect a specific market segment or organizations' operations. Typical examples are tax, employment, environmental and judicial laws. The Political factor also encompasses aspects such the general political climate of a country, the degree of government stability, as well as its international relations and posture, as well as issued regulations.

The **Economic factor** of the PEST methodology aims to assess the key determinants of a certain economy's performance such as the inflation rates, exchange rates, cost of production, economic growth, disposable income of consumers and, unemployment rate. These determinants may have a direct or indirect impact on organizations and market segments, for example, a trend in a certain direction may affect the purchasing power of consumers and could change the demand/supply models in the economy. As a result, the way organisations price their products and services on the market can also change.

The **Social factor** refers to the demographic characteristics, cultural attitudes and customs of the population within which organizations operate. Typically, this includes trends such as the population growth rate, age distribution, income distribution, cultural barriers and, emerging

lifestyle attitudes and consciousness (e.g. environmental, privacy and health) affecting consumers' behaviours and preferences.

The **technological factor** pertains to innovations in technology that may affect the operations of organizations and a specific market segment. This factor refers to technology advancement and maturity, the emergence of disruptive technologies, the level of innovation, automation, research and development (R&D) activity, technological change and the amount of technological awareness that a market possesses. These factors may influence decisions to adopt new technologies, enter or not other sectors, launch or not other products or outsource production activities.

An overview of the PEST method is given in the figure below (see Figure 6):

Figure 6: Overview of PEST method as adopted within ECSMAF



Some examples of the various PEST components are given in Annex 4.1A.4.3

2.2 CONTEXTUALIZED ECSMAF COMPONENTS

As the content and structure of market analysis effort heavily depends on the scope and purpose, so does also cybersecurity market analysis. Hence, within ECSMAF, parametrization holds a significant role. Through a series of ECSMAF-internal elements, the analysis can be adapted to the needs, be it the definition of the value chain, the selection of the reports type to be produced, the number of ECSMAF modules to be performed, the method for information collection, etc.

In this section, we present the elements of the proposed method that allow for the customisation of the scope and content that will be covered in the analysis. It has to be noted, that the need for such components emerges from the complexity of cybersecurity value chains.

In the below sections, the parametrized elements of ECSMAF are discussed in more detail.

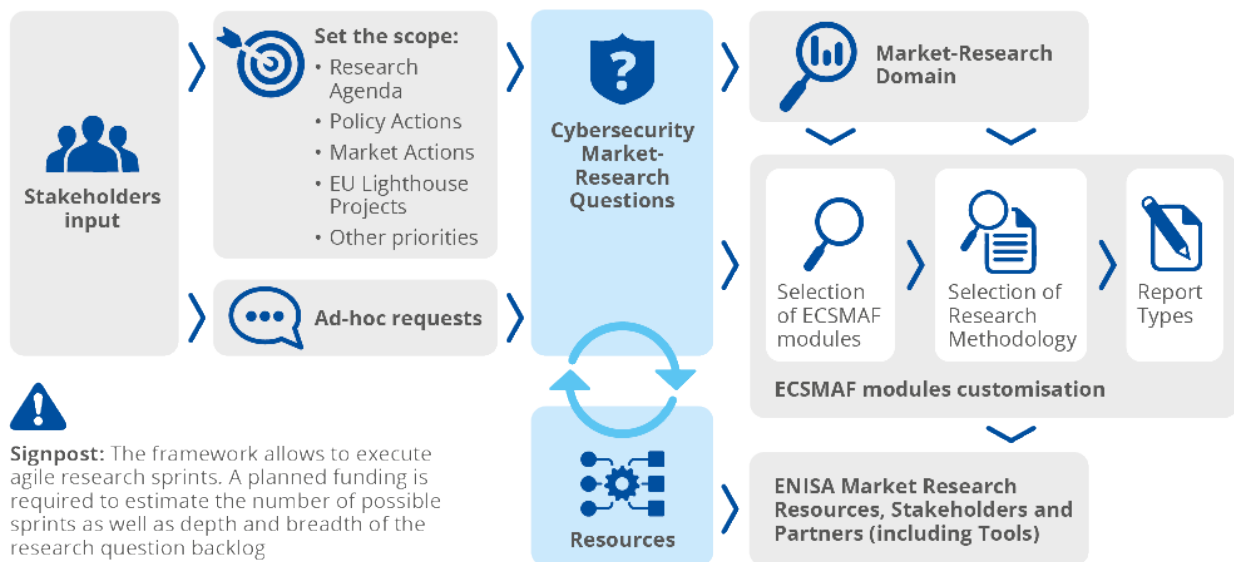
2.2.1 Scoping the analysis and ECsMAF parametrization

During the development of ECsMAF, but also through a performed pilot in the area of IoT³¹ and discussions within the ENISA Ad Hoc Working Group on EU Cybersecurity Market³², it became apparent that for the purpose of each cybersecurity market research analysis effort, it is key to identify the scope, prior to the performance of the analysis. In other words, the use of the proposed frameworks needs to possess an inherent agility, to cover the specific needs of any potential analysis focus (i.e. depth and breadth of the analysis).

The foreseen agility of the method will lead to a selection of the modules to be performed, while it will allow for different types of reports, data collection methods and outcomes. All these variables will heavily depend on the scope of the analysis. This fact underlines the non-waterfall nature of the proposed framework, as regards the use and sequence of the presented modules: only the elements that lead to the coverage of the proposed scope will be subject of a cybersecurity market analysis effort.

In order to perform necessary parametrization of ECsMAF during setting the scope, a workflow has been developed. The structure and content of the workflow is presented in Figure 7 below.

Figure 7: Structure and content of the ECsMAF parametrization workflow



The above workflow consists of various phases (depicted through various rectangles) as described below:

- Stakeholders:** These are actors that are entitled/mandated to propose ideas for priorities for the performance of cybersecurity market analysis. They might be institutional stakeholders participating in the ENISA process (e.g. Member States, Commission and other EUIBAs), Industrial Associations, Stakeholder Groups, but also ENISA-internal stakeholders, such as ENISA Management Team, and ENISA Advisory Group (AG). For this initial market analysis framework, input in this respect is provided by the ENISA Management Team and by the Members of the newly established ENISA ad hoc Working Group on EU Cybersecurity Market^{Error! Bookmark not defined.}.

³¹ <https://www.enisa.europa.eu/publications/cybersecurity-market-analysis-iot-in-distribution-grids>, accessed April 2022.

³² https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ad-hoc-working-group-on-cybersecurity-market, accessed November 2012.

- **Set the scope:** the input of stakeholders is “passed” through an activity whose purpose is to set the scope of the proposed cybersecurity market-analysis effort and identify their priority. For this purpose, proposed ideas are checked upon a number of criteria that allow for the assessment of their relevance/priority. The criteria check the relevance of a submitted cybersecurity market analysis idea w.r.t. various facts, such as:
 - What is the trigger of the cybersecurity market analysis (e.g. policy action, investment strategy, market intervention policy, market-supportive measures, incident/threat, necessary risk mitigation, observed market trends, etc.)?
 - What intended to be part of an analysis (demand, supply, market penetration of products, market requirements, etc.)?
 - What is the exact content of the value-chain and value stack in scope (depth vs. breadth)?
 - What are the main economic criteria for the market scanning (e.g. market size, demand size, growth, market gaps, etc.)?

In this initial framework such criteria are quite basic; hence, they are used currently in a rather qualitative manner. Some work on in this area is planned for the forthcoming version of ECSMAF, following initial experiences collected by the classification/mapping of currently submitted proposals. Obviously, due some urgent topics that can emerge, ad hoc cybersecurity market analysis requests may also arise, e.g. due to some incidents, and global happenings in cybersecurity. This depicted in the figure through the rectangle labelled as “**Ad hoc requests**”. All produced proposals (including the criteria met), will undergo a validation by ENISA stakeholders (i.e. ENISA Management and ENISA bodies).

- **Cybersecurity market-research questions:** In this phase, the scope set for a specific analysis is translated into a set of so-called “market-research” questions. These are obviously the questions that the particular cybersecurity market analysis is supposed to answer. Those questions allow for the identification of the content of the resulting analysis. Therefore, at this stage, an estimation of the effort needs to be performed. By taking into account the available resources the feasibility of the analysis should be checked (see rectangle labelled “**Resources**”). If the comparison does not balance, an adaptation of the questions and/or the available resources might be necessary.
- **Market-research domain:** This activity stands for the identification of the domain/sector to be analysed. It consists of identifying the infrastructure at stake, the value chain/value stack of the domain and the various assets and actors involved (both at the demand and supply-side, depending on the scope). Though this activity is independent from market analysis subjects, it is essential for the understanding of the sector/domain in scope. Its performance will require solid sectoral knowledge that will need to be brought in to the market analysis effort through sector/domain experts.
- **ECSMAF modules customisation** (embracing Selection of ECSMAF modules, Research Methodology and Report Types): In this phase, once the scope, the market-research questions, the identification of the relevant domain/sector have been performed, a decision about the ECSMAF modules to be included in the analysis is being made. The selection takes into account available resources. In order to accompany the analysis and run the effort, relevant stakeholders, partners and tools are identified (see rectangle labelled **ENISA Market Research Resources, Stakeholders and Partners**).

Although the elements of the above-mentioned parametrisation have been identified at this stage of ECSMAF development, further work regarding their quantification is necessary. Within the performed pilot of the framework, the parametrisation was oriented towards empirical methods proposed by the pilot project team. Additional input is expected from the experience collected by the work of the ENISA ad hoc Working Group on this matter (i.e. prioritisation of prospective cybersecurity market research areas).

2.2.2 Cybersecurity market taxonomy

The main challenge in cybersecurity market analysis is the “blurriness” in the identification of the offerings included existing cybersecurity products, services and processes. A typical example is the market segment of Managed Security Services: while some companies include Security Operation Centre functions, Threat Analysis, Penetration testing, etc., others are more protection-device oriented, covering firewalls, end-point security, configuration management, etc. This diversification of services that are sold under the same name, makes market analyses for this market sector imprecise and often incomparable, both regarding supply and demand sides (e.g.³³ and ³⁴). The complexity of cybersecurity offerings comes to aggravate the “blurriness” issue of performed analyses.

In order to alleviate this deficiency, the proposed framework adopts the concept of a **cybersecurity product, service and process taxonomy**. Its aim is to deliver widely recognised, sharply defined categories for cybersecurity offerings. The cybersecurity taxonomy used within ECSMAF has been derived from relevant work already performed within the EU, in particular within a cooperation between the European Commission’s Joint Research Centre (JRC)³⁵ and the European Cyber Security Organisation (ECSO)³⁶. While the ECSMAF taxonomy is based on this material, some minor (structural) adaptations have been performed, in order to adjust it to the detail and structure conceived for mapping cybersecurity market offerings. To this extent, the taxonomy presented in this section is an initial version: both through experiences gained from cybersecurity market analysis pilots and through an envisaged cooperation between ENISA, JRC and ECSO, a consolidation back to the original JRC-taxonomy³⁷ will be performed. Aim of this cooperation is to create a single, multi-purpose and managed reference, while at the same time make it as comprehensive as possible w.r.t. additional cybersecurity elements³⁸. Additional steps to ensure the acceptance of this material will be initiated (e.g. open dialogue with private and public actors in this area).

Just as it is required within the various modules of ECSMAF, the used cybersecurity taxonomy is split into three levels, covering various levels of value stack details, each one decomposing its predecessor. The level of detail to be considered in each cybersecurity market analysis depends on the selected scope and the depth. To this extent, the selection of the detail of the analysis is parametrised during the scoping of the analysis, so as to better match the objectives set (see also section 2.2.1).

At this point it should be noted, that the introduction of a cybersecurity taxonomy within market analysis efforts is a novelty. None of the contemporary market analysis methods seems to introduce such an instrument in order to enhance transparency, comparability and “sharpness” within market analyses.

The developed taxonomy concentrates mainly on cybersecurity value stack. Other, non-security related value chains and value stack elements that will be encountered through market analysis (i.e. vertical industries, see also Figure 8), are not covered in this version of the document. This information (also referred to as adjacent markets³⁹ from the perspective of cybersecurity) is

³³ <https://www.ibm.com/security/services/managed-security-services>, accessed December 2021.

³⁴ <https://services.global.ntt/en-us/services-and-products/security/managed-security-services>, accessed December 2021.

³⁵ The European Cybersecurity Taxonomy is available at: <https://ec.europa.eu/jrc/en/science-update/european-cybersecurity-taxonomy>, accessed November 2021. For more information on the JRC: <https://ec.europa.eu/jrc/en>, December 2021.

³⁶ The Taxonomy of the ECSO Cybersecurity Market Radar is available at: <https://www.ecs-org.eu/documents/uploads/ecso-cybersecurity-market-radar-taxonomy-table.pdf>, accessed November 2021. For more information on ECSO: <https://www.ecs-org.eu/>, December 2021.

³⁷ <https://ec.europa.eu/jrc/en/science-update/european-cybersecurity-taxonomy>, accessed November 2021.

³⁸ It is expected that with a growing number of cybersecurity market analyses, the taxonomy will undergo a development to cover all necessary cybersecurity elements that may be within focus.

³⁹ <https://www.forbes.com/sites/stephenwunker/2019/10/15/a-five-step-roadmap-to-grow-into-an-adjacent-market/>, accessed December 2021.

useful to fully identify markets to which cybersecurity is horizontal to, thus to understand value chain dependencies between cybersecurity and other products, services and processes.

The structure and content of the cybersecurity taxonomy is shown in the table below.

Table 2: Structure and content of the ECSMAF cybersecurity taxonomy

Value Stack level 1	Value Stack Level 2	Value Stack Level 3
R&D and education	Education: This market primarily consists of offerings related to cybersecurity education.	Cybersecurity academia / research
		Cybersecurity professional education
	R&D: This market primarily consists of all services related to cybersecurity research and development.	Cyber threat and vulnerabilities research
		Cryptography research
		Software & Hardware Research & Development
		Cybersecurity standards development
Software	Application security SW: This market primarily consists of application security testing (AST) software, vulnerability assessment (VA) software and web application firewall (WAF) software.	Application Security Testing Software
		Vulnerability Assessment Software
		Web Application Firewalls Software
		Other Application Security Software
	Cloud security SW: This market primarily consists of solutions that improve the cybersecurity, governance and reliability of public and private cloud computing such as Cloud Access Security Brokers (CASB), Cloud Security Posture Management (CSPM) and Cloud workload protection platforms (CWPPs).	Cloud Access Security Brokers
		Cloud Security Posture Management
		Cloud Workload Protection Platforms
		Other Cloud Security Software
	Data Security SW: This market primarily consists of encryption software, enterprise data loss prevention (DLP) software and tokenization software.	Encryption Software
		Enterprise Data Loss Prevention Software
Tokenization Software		
Other Data Security Software		
Software security Module		
Identity and Access Management SW: This market includes four segments: Access Management (AM) software, Identity governance and administration (IGA) software, Privileged Access Management	Access Management Software	

	(PAM) software and User authentication software.	
		Identity Governance and Administration Software
		Privileged Access Management Software
		User Authentication Software
		Other Identity and Access Management SW
	Infrastructure Protection SW: This market primarily consists of networks and endpoints (including servers, laptops, mobile device, OT/IoT device) protection software, cybersecurity information & event management and threat intelligence products.	Endpoint Protection Platform (Enterprise) Software
		Secure E-mail Gateway Software
		Secure Web Gateway Software
	Operational software platforms: This market consists of software products in form of – usually hosted - platforms that allow the collection, collation and filtering of cybersecurity related information and its management.	Security Information and Event Management (SIEM) Software
		Threat Intelligence Software
		Other Infrastructure Protection Software
	Integrated Risk Management / GRC SW: This market primarily consists of Digital Risk Management (DRM), Vendor Risk Management (VRM), Business Continuity Management (BCM), Audit Management (AM), Corporate Compliance & Oversight (CCO) and Enterprise Legal Management (ELM) technologies.	Digital Risk Management (DRM)
		Vendor Risk Management (VRM)
		Business Continuity Management (BCM)
		Audit Management (AM)
		Corporate Compliance and Oversight (CCO)
		Enterprise Legal Management (ELM)
		Other Integrated Risk Management / GRC SW
Hardware	Network security equipment: This market primarily consists of cybersecurity products within enterprise network equipment market such as Firewall and Next-Generation Firewall solutions, Unified threat management (UTM) products, Intrusion Detection and Prevention Systems (IDPS),	Firewall Equipment, Intrusion Detection and Prevention Systems, Network Access Control Equipment, Network Detection and Response, Zero Trust Network Access

	Network Access Control (NAC), Network Detection and Response (NDR).	
	Hardware security: This market primarily consists of physical hardware that generates and stores cryptographic keys and executes cryptographic operations to encrypt and sign data.	Trusted Platform Module
		Hardware security module
		Network security equipment
	Biometric-based security equipment/systems: This market consists of physical hardware that is used to recognize biometric signals.	Hardware biometric security module
		Software biometric security module
Distribution	Distribution: This market primarily consists in the delivery of cybersecurity software or hardware to end-users, resellers or organisations that provide B2B cybersecurity services.	Software resale
		Hardware resale
		Managed Services resale
Advisory & Consulting	Advisory & Consulting: These activities include among others: cybersecurity and risk strategy, advisory and research, testing, assessment, compliance and audit, cybersecurity operation process and tooling design, digital forensics, cybersecurity project management and staff augmentation.	Security and risk strategy, planning and management advice, maturity assessment
		Security advisory and research
		Security testing, and risk and threat assessment (Penetration Testing, Red-Blue Teaming)
		Security Operations Centre (SOC) services (i.e. Design and build SOC processes and tooling, pre-assessment for gathering service requirements)
		Security Compliance and Audit (Compliance Management, Compliance Audits, Ex-post assessments)
		Digital forensics: post event (incident / intrusion) analysis, Investigation and proof preservation
		Security project management, staff augmentation (Provide named resources, remote or on-site, to act as an extension of the internal team)
		Other IT/cybersecurity consultancy services
Implementation services	Implementation design: This market primarily consists of cybersecurity solutions design & architecture development.	Security design, engineering and architecture development

	Integration services: This market primarily consists of integration, planning, scheduling and testing.	Implementation and integration, interoperability testing
	Development: This market primarily consists of cybersecurity development, implementation and testing.	Implementation support (technical assistance/expert support services)
Managed Services	Managed response services: This market primarily consists of cybersecurity operations and technology maintenance services that include incident management and response.	Managed Detection and Response (MDR)
		Incident Response
	Cybersecurity Device management: This market primarily consists of managed services for cybersecurity related components.	Security device management (including maintenance, patching, testing and decommissioning).
		Co-managed Services
	Threats and Vulnerabilities: This market primarily consists of service related to vulnerability and threat management.	Vulnerability Management
		Threat Detection Services (Basic threat detection, Advanced Threat Detection, entrapment and observation of attacker in high interaction artefacts, integrated proactive threat hunting, active attacker engagement)
		Threat intelligence
	Virtualized cybersecurity services: This market primarily consists of hosted cybersecurity related services (e.g. platforms, cybersecurity protection software, etc.) whereas the responsibility of usage lies with the customer.	Cybersecurity as a service (CSaaS)
	Security training: This market primarily consists of cybersecurity managed training services in all cybersecurity areas.	Security training services (Security Awareness Program Platforms, cybersecurity Awareness Content Development and Delivery Systems, Phishing Simulation Testing and Remediation/response Platform, Cybersecurity Awareness Training, etc. as a Managed Service)
	Other managed services: This market primarily consists of any other managed services.	Other Managed Services (Managed Identity & Access Management, Assurance Services, Application Security Services, User Behaviour Analytics, Emergency Threat Response)
Certification Services	Product Cybersecurity Certification services: This market primarily consists of services related to the creation of certificates and their maintenance. Though usually this activity is being performed by/on behalf of national/non-profit organisations, numerous companies offer this know how.	All services related to the assessment and implementation of assurance levels for product certification (e.g. component criticality assessment, risk/threat assessment, identification of attacker potential, formulation of requirements, gap analysis, identification of product evaluation levels, identification of controls, testing, etc.).

	<p>Service/process Certification services: This market primarily consists of services related to the cybersecurity certification service and process, such as development, operations, production processes and services.</p>	<p>All services related to the assessment and implementation of assurance levels for service/process certification (e.g. criticality assessment, risk/threat assessment, identification of attacker potential, formulation of requirements, audit, gap analysis, identification of controls, etc.)</p>
	<p>Professional Certification services: This market primarily consists of the infrastructure (human, technical, documents) to obtain professional cybersecurity certificates (note: though it has overlaps with Cybersecurity training above, it is proposed as a separate element due to its market size and importance).</p>	<p>All services related to cybersecurity certification courses and examination of acquired knowledge (development of course material, maintenance of related standards, provision of course and examination infrastructure, certificate maintenance, etc.).</p>
	<p>Accreditation services: This market primarily consists of the services that lead to an accreditation of an organisation to offer and perform cybersecurity-related certification efforts (see above mentioned services)</p>	<p>All services related to the accreditation of cybersecurity certification (accreditation of testing infrastructures/labs, accreditation of processes and skills).</p>

2.2.3 Cybersecurity market trends

Market trends are in fact one of the main elements to understand and estimate market developments. The identification of market trends is explicitly mentioned in CSA¹. The challenge with market trends lies mainly on the fact that they emerge from a variety of factors, while they may be of generic nature, but also sector-specific. The identification of the degree of relevance of market trends for a specific analysis requires a multi-level assessment to cover all these dimensions. ECSMAF takes this challenge fully into account.

Firstly, it foresees the identification of technology trends at the level of the module **Technology Research**. These are trends related to generic technology development/emergence issues, as result of generic, sector-independent foresight efforts⁴⁶. Secondly, trends will be identified within the defined scope of the cybersecurity market analysis through the activities of the ECSMAF modules **Marco-Environmental Factors and Economic Market Characteristics** (see also Section 2.1.5). The scope-related trend assessments are going to be performed under the context of supply and demand characteristics of the current analysis, thus adding an additional level of detail to the more generic trends assessment.

Subsequently, identified trends will be taken into account in the activities of ECSMAF modules **Demand-side research** (see Section 2.1.2) and **Supply-side research** (see Section 2.1.3).

As an experience gained from the performed ECSMAF pilot in 2021, one can note the following: depending on the market research method chosen (in this case using an external market analysis organisation/service) and the foreseen analysis resources, available trending information can be used as-is (i.e. as provided by the contractor), without performing the corresponding ECSMAF modules. This approach can deliver satisfactory results, when the trends happen to be already identified by market analysts. In case of “deeper” analyses of emerging sectors/technologies, however, it might be meaningful to perform these modules to identify trends in a more targeted manner for the area/sector in focus. The costs of such an effort might be justified by the benefit of the analysis precision.

After the performance of cybersecurity market analyses, the identified market trends will be – as far as possible – consolidated back to relevant trending information provided by relevant ENISA projects/efforts to a single trending record, enhancing thus comprehensiveness of available trending knowledge.

2.2.4 Market stakeholder types

The identification of market **stakeholder types** that are subject to a specific cybersecurity market analysis are very important for the achievement of the analysis objectives. They are primarily determined from the scope of the analysis (i.e. which types of businesses the market analysis should concentrate on?), but also from various other factors, such as types of market stakeholder dynamics (i.e. innovation power, quick rates, niche-product development, research oriented, etc.).

Another important element in market stakeholder type identification is the association to a specific **vertical industry**. The importance of this piece of information is twofold:

- Firstly, the use of a uniform vertical industry name convention increases transparency and comparability of achieved analysis reports.
- Secondly, to every vertical industry, a certain value chain (including value stack) can be assumed, that characterizes their core business. This allows performance of more precise mappings of their turnover. Furthermore, this will further enhance transparency and comparability and also help highlight nuances among various market stakeholders acting in the same industry.

It is worth mentioning, that stakeholder types and vertical industries are used within both the demand- and supply-side market research.

As regards first experiences in the performed pilot regarding stakeholder types, some indicative ones are provided below, including value chain and value stack information, both for their main business and cybersecurity services:

- **Multi-domain industrial asset vendors:** Have a broad and solid market offering when it comes to the provision of products, services and processes in a certain domain. Below some examples of their offerings:

Value Chain: Hardware, Software, Implementation, Advisory and Consulting, Managed Services.

Value Stack IT: Management Platforms, Connectivity, Remote Sensors, Remote Operation.

Value Stack Cybersecurity: Application security software, Cloud security, Data security, Identity and access management, Infrastructure protection software, Network security, Advisory, Implementation, Managed security services.

- **Multi-domain vendors:** Have capabilities in those areas that are critical to collect, manage and maintain user requirements and information on product, services and processes, offering thus customised solutions. Below some examples of their offerings:

Value Chain: Software, Implementation, Advisory and Consulting, Managed Services.

Value Stack IT: Management Platforms, Connectivity.

Value Stack Cybersecurity: Application security software, Cloud security, Data security, Identity and access management, Infrastructure protection software, Network security, Advisory, Implementation, Managed security services.

- **Single-domain specialised vendors:** Have targeted, specialised capabilities in a specific domain, covering wide range of customer requirements in a narrow technological spectrum. Below some examples of their offerings:

Value Chain: Hardware, Software, Advisory, Implementation.

Value Stack IT: Management Platforms, Connectivity, Fault detection, Remote Operation.

Value Stack Cybersecurity: Application security software, Cloud security, Data security, Identity and access management, Infrastructure protection software, Network security, Advisory, Implementation, Managed security services.

- **Cybersecurity specialist vendors:** Are specialised in cybersecurity market segments, often ones that are not part of core portfolios of by larger vendors. They emerged in developing cybersecurity market segments where they leverage innovative, state-of-the-art cybersecurity technologies to ensure differentiation. Below some examples of their offerings:

Value Chain: Hardware, Software and Advisory.












Value Stack Cybersecurity: Identity and access management, Network security, Hardware security modules, Advisory, Threat analysis, Risk Management, Penetration testing.

As regards vertical industries, an initial proposal is presented in Figure 8 below. With increasing experience in cybersecurity market analysis but also by considering available best practices⁴⁰, this list is going to be updated/consolidated accordingly. It is worth mentioning, that these vertical industries in the current version do not entail any cybersecurity related industries. Cybersecurity is assumed as “horizontal” to these industries. Moreover, the core value chain and value stack (i.e. product, service and process offerings) of those industries may entail cybersecurity as an *integrated part of the offering* that is built-in feature of their offerings and *not as their main product*.

⁴⁰ <https://www.hackmageddon.com/2021/02/10/january-2021-cyber-attacks-statistics/>, accessed December 2021.



Figure 8: Proposed list of vertical industries (initial, non-exhaustive)

BANKING AND SECURITIES		<ul style="list-style-type: none"> • Banking • Securities
COMMUNICATIONS, MEDIA AND SERVICES		<ul style="list-style-type: none"> • Entertainment • Publishing and advertising • Broadcasting and cable • Telecommunications • Other business, technical and consumer services • Information technology services and software
EDUCATION		<ul style="list-style-type: none"> • Primary and secondary education • Higher education
GOVERNMENT		<ul style="list-style-type: none"> • National and international government • Local and regional government
HEALTHCARE PROVIDERS		<ul style="list-style-type: none"> • Physician • Hospital
INSURANCE		<ul style="list-style-type: none"> • Health insurance (payer) • Insurance (other than health)
MANUFACTURING AND NATURAL RESOURCES		<ul style="list-style-type: none"> • Automotive • Consumer nondurable products • Energy resources and processing • Heavy industry • IT hardware • Life sciences and healthcare products • Natural resources and materials
RETAIL		<ul style="list-style-type: none"> • General retailers • Grocery • Restaurants and hotels • Specialty retailers
TRANSPORTATION		<ul style="list-style-type: none"> • Air transport • Motor freight • Pipelines • Rail and water • Warehousing, couriers and support services
UTILITIES		<ul style="list-style-type: none"> • Electric and gas utilities • Water utilities
WHOLESALE TRADE		<ul style="list-style-type: none"> • Wholesale durable and nondurable goods

2.2.5 Methods for collecting market data

The method chosen for the collection of market analysis data is of major role for the utilization of the available resources and the achievement of the targeted quality of findings, in accordance to the scope of the analysis (see also discussion in Section 2.2.1).

The existing methods for data collection⁴¹ (also depicted in Figure 1 through the box labelled Method) consist of:

- **Primary research:** Consists of collection of data directly from organization that is targeted by the market analysis effort (i.e. relevant market stakeholder types from relevant vertical

⁴¹ <https://www.bdc.ca/en/articles-tools/blog/how-conduct-market-research-small-businesses>, accessed December 2021.

industry, see Section 2.2.4). Primary research is usually implemented through surveys and interviews (online, per phone or mail). This method has the advantage of direct involvement in the collection, the possibility to steer the discussion with interviewed organizations and the ownership of the collected data. A disadvantage of this methods is that it might imply quite significant costs.

- **Secondary research:** This research consists of data collection from already published, open source (OSINT) market analysis information. It is usually sufficient to provide a good generic overview on market issues related to a specific domain. It should be the principal choice in the starting phases of market research efforts, for example during the scoping of an analysis (see also Section 2.2.1). The advantage of this method is its low costs, its efficiency and ownership of collected data. A disadvantage might be that the information publicly available might be limited or inaccurate.
- **Use of market analyst services:** The research can be contracted to external market analyst companies. They provide “turnkey” market analyses given a number of “(market) research questions”. Though this method leverages on existing skills and data collection infrastructure, it is necessary to precisely formulate the research questions and ensure that the analysis will produce the desired results in the desired manner (i.e. report types). This can be achieved, for example, by performing a scoping exercise, as described in Section 2.2.1 above, prior to contracting a market analyst organisation. A disadvantage of this method is that the collected data will reside by the contractor.

3. RELATED AREAS

As mentioned in CSA¹, cybersecurity market analysis is a multi-purpose tool that can be used in a variety of ways towards developing cybersecurity within Europe. In this chapter we provide information on how cybersecurity market analysis interacts with other areas, respectively how other areas may contribute or may profit from available market analysis efforts.

- **Certification:** Cybersecurity market analysis very relevant for certification. Through targeted market analyses, the market effects of certification can be identified: market analysis can help assessing the market penetration of various certification labels (including prospective EU labels). Moreover, market analysis can provide insights about the size and value chains of organisations engaging in certification businesses, with the objective, for example, to strengthen their market presence. From initial experience through the ECSMAF pilot^{Error! Bookmark not defined.}, it became apparent, that cybersecurity certification market analyses will need to have a narrower scope. In order to assess certification needs, for example, the efficiency of current protection policies need to be illuminated. This means, that “deeper” levels of the cybersecurity value stack will need to be taken into account; or detailed assets exposure to threats need to be considered. In both cases, the analysis will need to embrace particular details of the relevant assets in scope. Having said that, it seems more appropriate to analyse certification needs via second or even third tier “dives” into product, service and process structures to assess the effects of or the need for certification. The interaction between cybersecurity certification and market analysis may be:

Cybersecurity certification -> Cybersecurity market analysis: may support cybersecurity market analysis during the phase of setting the scope, by providing distinct sector and the elements (assets) of the infrastructure to be analysed.

Cybersecurity market analysis -> Cybersecurity certification: Market analysis can provide proposals for areas to be taken into account for cybersecurity certification. These may be particular infrastructure parts that have been assessed by means of market gaps, while they are considered to be important parts/enabler of value stack elements.

- **Cybersecurity Research and Innovation:** Cybersecurity market analysis has a strong relevance to research and innovation. This is manifested via the role of technology trends for supply and demand market dynamics in the resulting market analysis. Such trends may be developed within research and innovation work. Moreover, innovation actions, in particular (e.g. deployment activities, establishment of research priorities, innovation activities, etc.), generate market drivers that will affect internal market. Hence, research and innovation information is best suited as input towards parametrization of ECSMAF for targeted cybersecurity market analyses. On the other hand, cybersecurity market analysis can provide valuable input regarding market gaps and niches that can affect research and innovation strategies, aiming at strengthening internal market.

Cybersecurity research and innovation -> Cybersecurity market analysis: may provide trending information according to identified research and innovation priorities. It may provide scoping information for areas/technologies/sectors that have been addressed in research activities and seem to be good candidates for deployment actions.

Cybersecurity market analysis -> Cybersecurity research and innovation: Cybersecurity market analysis can be performed prior to the identification of research and innovation

actions, as a form of “market scouting” effort. By extrapolating market gap / market niche information to existing (matured) research results and/or innovation areas, for example, one can assess their adequacy/potential as market enablers.

- **Policy actions:** Cybersecurity market analysis can be an important tool during impact assessments performed within policy proposals. As market is a strong indicator, but also discrete focus of most policy actions, the performance of analyses within the scope of policy actions is very useful. One point that could be stated at this point as example is the policy area of strategic autonomy and sovereignty: cybersecurity market analysis can contribute towards identification of dependencies of cybersecurity supply chains, degree of market domination by various types of vendors in various cybersecurity topics, identification of (regional) demand requirements, etc. Such information may generate strong evidence for prospective targeted policy actions in the area of cybersecurity. On the other hand, policy actions can deliver proper scoping information towards targeted market analyses (e.g. market segment, desired market outcomes and market stakeholder types (demand and supply sides)).

Policy actions -> Cybersecurity market analysis: Policy actions can provide concrete scope for cybersecurity market analysis, either within impact assessment, or for the purpose of evaluation of issued policy actions for various market segments.

Cybersecurity market analysis -> Policy actions: Cybersecurity market analysis can deliver valuable information regarding estimated market trends and/or observed market effects of policy actions. It can also provide insights about discrete parts of cybersecurity value chain, in support of evidence needed to issue new or further develop existing policy actions. In addition, market analysis is a key element of market observatories, mentioned in various policy documents (see also next bullet point).

- **Cybersecurity market observatories:** Market observatories perform wide-scope assessments w.r.t. various market parameters (i.e. dynamics, price development, demand development, identification of market players, etc.)^{42,43,44}. Cybersecurity market analysis overlaps with observatories, as far as a broader scope is taken into account. Here, a clear synergy potential does exist, as far as used analysis techniques and experiences on market analyses is concerning. This is particularly interesting in cases of observatories established within Member States and/or EU-Institutions: here the synergies with ENISA are evident, as a stronger exchange, both at the level of analysis method and market data exchange may emerge.

Cybersecurity market observatories -> Cybersecurity market analysis: Multiple synergies can be implemented, both regarding knowledge transfers regarding the used market analysis method and collected information (both raw data and market analysis findings).

Cybersecurity market analysis -> Cybersecurity market observatories: All relevant outputs from cybersecurity market analysis can be easily adopted by cybersecurity observatories, depending on the maturity level available or planned capabilities. As regards institutional observatories of EU/Member States, ENISA actively seeks for cooperation opportunities, among other things by means of the established ad hoc Working Group of EU Cybersecurity Market^{Error! Bookmark not defined.}.

- **Incidents / threats /risks landscaping:** Cybersecurity market analysis uses incident, threat and risk information/assessments in order to identify market trends and possibly

⁴² <https://cyberstartupobservatory.com/>, accessed December 2021.

⁴³ <https://cyberstartupobservatory.com/cyber-security-europe/>, accessed December 2021.

⁴⁴ <https://www.cyberwatching.eu/>, accessed December 2021.

scoping information for analysis: often, observed incidents and threat exposures lead to the deployment of new products (e.g. ransomware protection offerings⁴⁵). Moreover, threat exposure and incident statistics have been turned to be a useful criterion in scoping the ECSMAF pilot performed in 2021. Though possible, we do not assume at the time being that cybersecurity market analysis can contribute to incidents, threat and risk landscapes content-wise. Nonetheless, market analysis may contribute to the assessment of demand-requirements, as well as usage of products, services and processes related to incident, threat and risk management (i.e. management platforms, managed services and product offerings).

Incidents / threats /risks landscaping -> Cybersecurity market analysis: Cybersecurity market analysis can process landscaping information as an important criterion to set foci of market analyses.

Cybersecurity market analysis -> Incidents / threats /risks landscaping: Cybersecurity market analysis may analyse market data of existing offerings w.r.t. products, services and processes covering incident, threat and risk assessment and management.

- **Emerging trends - Foresight⁴⁶:** As indicated in the discussion so far, emerging trends play a multiple role within cybersecurity market analysis. Firstly within the module technology research; but are also part of macro-economic factors. Furthermore, they are also a useful insight even at the scoping phase. For these reasons, it is expected that an intense interaction between market analysis and foresight will be necessary. But also market analysis results may be useful for foresight: it might be the case, that the performance of a market analysis produces trending information for a certain, relatively narrow-scoped area/sector that might be an interesting feedback for foresight (i.e. was originally out of scope of a certain foresight focus). Such information, if deemed relevant, may be fed to consecutive iterations of the foresight exercise, or serve as validation of already created forecasts.

Emerging trends – Foresight -> Cybersecurity market analysis: Emerging trends provide valuable information to cybersecurity market analysis by means of trending information that can be used for technology research and potentially for macro-environmental factors.

Cybersecurity market analysis -> Emerging trends – Foresight: Cybersecurity market analysis may provide some more detailed information to foresight, related to some “deeper” trends that have been assessed within analyses with more specific foci.

- **Cybersecurity index:** An ENISA-activity in the area of cybersecurity index aims at the creation of composite cybersecurity index providing for an aggregated assessment of the maturity level of cybersecurity across the EU. Its aim is to map the impact of cybersecurity by means of quantitative and qualitative indexes and on developing cybersecurity taxonomies and (quantitative and qualitative) assessments of cybersecurity. As it can be assumed that cybersecurity market maturity is one key dimension for the cybersecurity maturity within the EU, market analysis results may directly flow in the cybersecurity index as additional qualitative/quantitative data. Equally important is the use of a consolidated taxonomy, as it will enable comparability of cybersecurity topics. Another element is the provision of scoping information to market analysis: maturity cybersecurity (from low to high) can become an interesting focus for market analysis. Hence, cybersecurity index can

⁴⁵ https://www.antivirusguide.com/best-ransomware-protection/?lp=true&utm_source=google&utm_medium=cpc&sgv_medium=search&utm_campaign=6478205166&utm_content=77388860066&utm_term=anti%20ransomware&cid=508925511743&pl=&feeditemid=&targetid=aud-755007040539:kwd-13149176227&mt=b&network=g&device=c&adpos=&p1=&p2=&geoid=9067692&qclid=Cj0KCQiAzMGNBhCyARIsANpUkzMK2cFBPpIf0r8MNE9eQfzvQxXwA0m_nwN4AoyhMwmCEJZdLqcgzYaApvVEALw_wcB, accessed December 2021.

⁴⁶ <https://www.enisa.europa.eu/news/enisa-news/step-towards-foresight-on-emerging-cybersecurity-challenges>, accessed November 2021.

act as an indication for the need to assess a specific market sector. Last but not least, product, service and process maturity issues are subject of market analysis too (see demand-side research in Section 2.1.2). This information can be mutually exchanged among cybersecurity index and market analysis as described below:

Cybersecurity index -> Cybersecurity market analysis: Cybersecurity index can provide scoping information for cybersecurity market analysis. Moreover, it maintains a taxonomy that can be input to and/or consolidated with the cybersecurity market taxonomy.

Cybersecurity market analysis -> Cybersecurity index: Cybersecurity market can assess maturity of products, services and processes. Should they be in the focus of a market analysis, they can serve as input to the cybersecurity index. Equally, the developed cybersecurity market taxonomy can be used as input to and/or consolidated with the cybersecurity index taxonomy.

Concluding this chapter, we would like to state that quite few of the interaction points mentioned above are covered through regular interactions/coordination, mainly with ENISA-internal stakeholders/units, but also external ones. Some of those are going to lead to activities in 2022, and are covered in the forthcoming chapter by means of future work (see Section 4.1).

4. ISSUES, CONSIDERATIONS, CONCLUSIONS

In 2021, ENISA was in the position to start building capabilities in the area of cybersecurity market analysis. The framework presented in this report, an initial pilot of the framework and the creation of the ENISA Ad Hoc Working Group on the EU Cybersecurity Market have been the main activities performed by the Agency in 2021 in this area.

4.1 GENERAL REMARKS

The market research for the pilot of the framework has been conducted by a major market analyst organisation. From this initial experience in the area of market analysis, the issues surfaced can be summarized as follows and some general remarks can be made:

- **Cybersecurity market analysis is at a crossroad:** When cybersecurity meets market analysis, one can speak about a meeting point of two different disciplines: a highly, structured, relatively new technological area comes to profit from one area of economics with much longer record and established methods. In order to establish the mutual understanding of these disciplines, a significant knowledge transfer is necessary: cybersecurity specialists need to understand the functioning rules of the market, while economists/analysts need to gain an insight of the cybersecurity product, service and process landscape. It seems that this is the root-cause for vivid discussions between cybersecurity experts and market analysts e.g. regarding terminology and used analysis methods, report content and structure. It has become evident, that there some time is needed for both disciplines to mutually understand each-other, and that the development of some basic tools to pass this knowledge are necessary (e.g. cybersecurity market taxonomy).
- **Scoping is the key to success:** Scoping, in Scoping the analysis, in particular defining the area of the cybersecurity market to focus the analysis on, is maybe the most important, yet not simplest step in market analysis efforts. Firstly, because security is a matter that can only be analysed when a certain depth of knowledge has been reached. Secondly, because of the divergence of views and methodological backgrounds between involved experts (see also previous point). Hence, at the current stage of “bridging” cybersecurity and market analysis, knowledge exchanges need to take place in order to understand how a cybersecurity scope can be formulated, how can it be “translated” into (market-) research questions, and how much effort is necessary to achieve the expected outcome at the expected quality.
- **Your data vs. my data vs. our market data:** The data collection strategy has to be selected in accordance with to the market analysis strategy. There are a number of questions that matter in this respect, such as: Is market data collection and analysis going to be mostly contracted or mostly done in-house? Are the market analysis objectives for a certain domain/sector fixed, or they might variate over time? What are the long-term approaches for cybersecurity market analysis efforts (one-off, repetitive, iterative, evolutionary, dynamic, varying)? Are raw data for a certain analysis interesting for longer term, or just the market analysis results count? Are raw data for the defined scope the already available, or need to be raised through dedicated surveys? Are available data free of bias! Answering these questions should be a priority for the determination of the amount of resources, for selecting market research methods (primary, secondary, outsourcing), for

selecting a data management approach and for establishing a corresponding human and toll infrastructure (including confidentiality issues, see next point).

- **Confidentiality issue emerging from collected market data:** Given the nature of raw market data, - both at the supply and demand sides - they entail a mix of competitive, confidential and intellectual property related information. Hence, specific confidentiality requirements emerge for the use/processing of this information, or even parts of it (i.e. processing, storage, management, dissemination, etc.). The inherent confidentiality of market information may be an inhibitor for the motivation of stakeholder to provide this information, unless a trust relationship and evidence for adequate processing techniques are available (i.e. data protection in transit and at rest, anonymization, implementation of relevant security controls, etc.). These issues need to be addressed, the latest when this information is stored and processed locally.

4.2 OPEN ISSUES AND WAYS FORWARD

Concluding this report, we would like to highlight a series of open issues that should constitute the short to middle term priorities in advancing the work on the EU cybersecurity market. ENISA will draw from these points the actions to be performed in the area of market analysis in 2022 and 2023. Identified open points that fall in the responsibility of other players in the EU ecosystem are proposal that will be validated by, discussed and followed up with the corresponding entities.

Cybersecurity Market and ENISA:

- **Streamline ECSMAF content:** The content of the framework needs to be better specified in a greater detail level for some ECSMAF modules and horizontal components. This will include identification of economic sizes to be measured, consolidation of vertical industries and identification of content of report types. The highest priority will be the creation of a coherent/consolidate taxonomy, allowing for usage within various cybersecurity topics (incidents, threats, market analysis, cybersecurity index, etc.). Hereto, a cooperation with JRC is envisaged.
- **Perform scoping exercises:** Scoping of analysis is a key activity within ECSMAF. It will be very important to gain experience with this activity, including defining criteria, checking parametrization techniques to cover varying foci (e.g. wide vs. deep analyses, thematic vs. generic analyses, iterative vs. one-off analyses, etc.). This work will help towards better representing scope for various cybersecurity market analysis topics and various detail levels of analysis (e.g. certification).
- **Tooling for Cybersecurity Market Analysis:** The development of necessary tools for the performance of primary and secondary market research is important for the market analyses. These tools include tools for storage of collected information (database), creation of reports based on analytics, and availability of a means for performing own primary research (surveys, questions).
- **Continue coordination:** As indicated in Chapter 3, cybersecurity market analysis has various interfaces to other ENISA activities. The coordination of this work will be a main priority for 2022 and beyond.

Cybersecurity Market and Member States:

- **Identify and establish synergies:** Member States have already or are about to establish cybersecurity market surveillance functions, notably for “*monitoring the compliance of ICT products [...] with the requirements of the European cybersecurity certificates*”¹. Such activities will create important synergies in the area of cybersecurity market analysis, both within Member States and with ENISA. The identification of the state-of-play with regard to development of market surveillance in Member States will be a priority for ENISA in 2022 and beyond.

Cybersecurity Market and Commission:

- **Identification of potential cybersecurity market analysis needs:** Cybersecurity market analysis may become an important tool for the need of EU policy actions. It will be important to assess potential foci of EU cybersecurity market analysis in order to identify resources and needs for know-how transfer. Moreover, in order to follow ENISA work in this area, the European Commission and interested Member States may desire to play an observer role within the ENISA Ad Hoc Working Group on EU Cybersecurity Market, to provide support regarding e.g. scoping exercises.

A ANNEX: EXAMPLES

A.1 EXAMPLES OF MARKET STRUCTURE AND SEGMENTATION

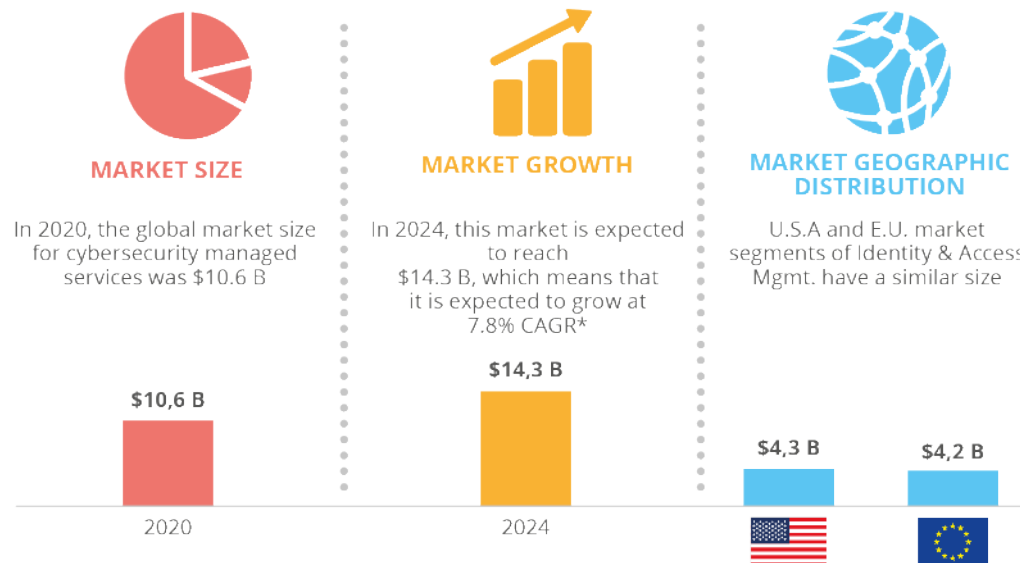
1. THE CYBERSECURITY VALUE CHAIN IS COMPOSED OF 7 DIFFERENT ACTIVITIES OF THE VALUE STACK



2. FOR EACH ELEMENT OF THE VALUE STACK, THREE DIFFERENT DIMENSIONS ARE TYPICALLY ANALYZED: MARKET SIZE, GROWTH AND GEO DISTRIBUTION

Illustrative example for Value Stack Identity & Access Management (Non-exhaustive)

MARKET SEGMENT: IDENTITY & ACCESS MGMT



* CAGR: Compounded Annual Growth Rate

A.2 EXAMPLES OF DEMAND-SIDE RESEARCH

1. DEMAND VOLUME AND GROWTH ARE TYPICALLY COLLECTED FOR A PARTICULAR ACTIVITY OF THE VALUE CHAIN, VALUE STACK SEGMENT



Illustrative example to estimate the demand volume and growth by region



2. USUALLY, THREE DIFFERENT TYPES OF ORGANIZATIONS CAN BE ANALYZED IN MARKET STUDIES

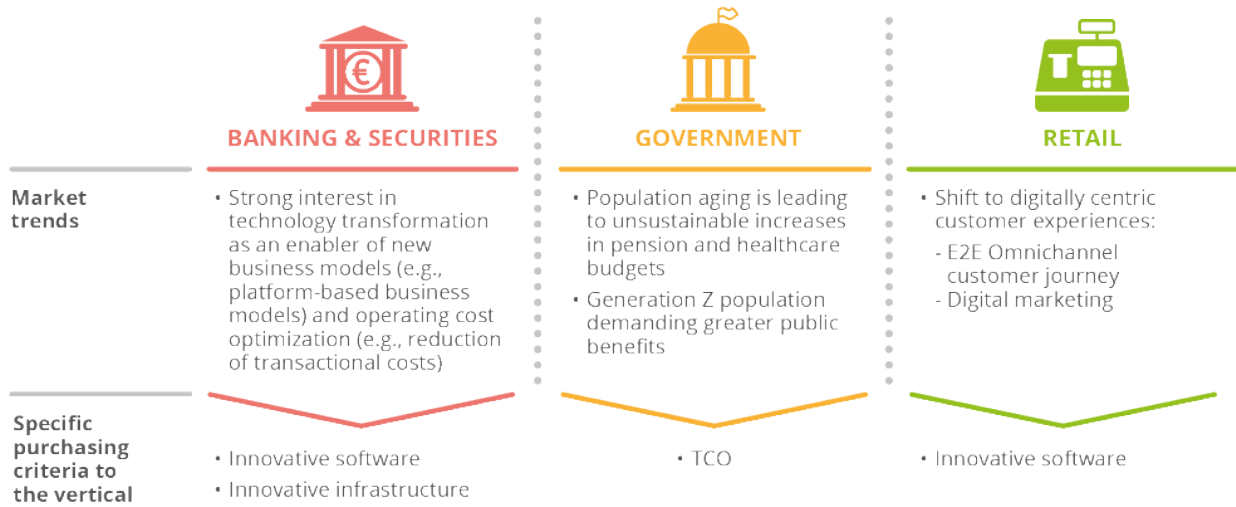
Typical segments of organization sizes

	SMALL SIZE ORGANIZATIONS	MEDIUM SIZE ORGANIZATIONS	LARGE SIZE ORGANIZATIONS
Number of employees	10 to 49 employee	50 to 249 employee	250 employees or more
Turnover	< € 10 m	< € 50 m	> € 50 m
Implications for the cybersecurity market	<ul style="list-style-type: none"> Typically, will participate in industries with very low IT spending relative to overall costs (e.g., transportation) Most of these organizations do not have a cybersecurity function 	<ul style="list-style-type: none"> Most of the medium size organizations have IT departments However, a large share of these organizations participate in industries in which there are minimal cybersecurity requirements (e.g., manufacturing) 	<ul style="list-style-type: none"> These organizations will typically have significant IT departments and cybersecurity requirements in most vertical industries



3. DIFFERENCES IN MARKET TRENDS ACROSS VERTICAL INDUSTRIES MAY HAVE AN IMPACT ON THEIR PROCUREMENT REQUIREMENTS

Illustrative examples of purchasing criteria specific to different verticals



A.3 EXAMPLES OF SUPPLY-SIDE RESEARCH

A.3.1 Example of Market Map

Non-exhaustive

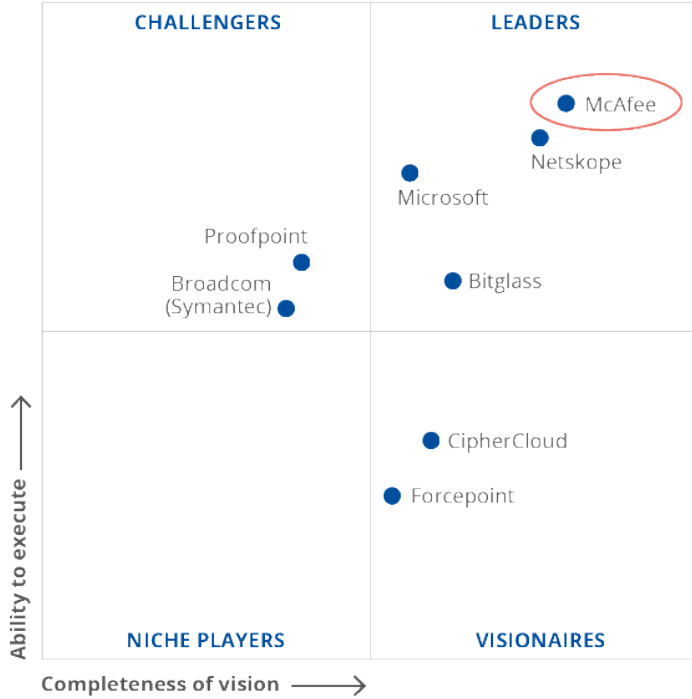
	Megasuite Application vendors Provide SW solutions in multiple domains	Providers of IT services Specialize in the provision of IT services	Security Suite Application vendors Provide security SW solutions across multiple domains	IT Hardware manufacturers Manufacture IT hardware for multiple purposes	Hidden Champions Specialize in a particular security market segment
Value stack	Microsoft	accenture	McAfee	CISCO	Daon
Application security SW	●		●	●	
Cloud security SW	●		●	●	
Data Security SW	●		●	●	
Identity and Access Management SW	●		●	●	●
Infrastructure Protection SW	●		●	●	
Integrated Risk Management / GRC SW	●		●	●	
Network security equipment				●	
Hardware security module				●	
Biometric-based security equip./systems				●	
Distribution	●	●	●	●	
Advisory & Consulting	●	●			
Implementation services	●	●	●	●	
Managed Services	●	●	●	●	

Example of Vendor Profile Rating

Non-exhaustive

MCAFEE: VENDOR RATING

2020 MAGIC QUADRANT



As of Oct 2020
© Gartner, Inc

MCAFEE: VENDOR PROFILE

Advantages

- A wide array of policies can take full advantage of API inspection, forward-proxy redirection, reverse-proxy insertion and RBI, facilitated by a single agent that directs traffic to McAfee’s CASB or SWG .
- The Mitre ATT&CK framework is well-supported in the interface for incident investigation and response.
- McAfee offers extensive CSPM capabilities that exceed those of even some pure CSPM vendors for IaaS/PaaS and SaaS. It includes strong auditing and compliance scanning, plus multiple options for automatic and guided manual remediation.

Cautions

- McAfee’s position is that managed devices interacting in predictable ways should be given direct access to SaaS collaboration applications and not passed through the forward or reverse proxy. Customers will need to assess whether this stance aligns with their supported enterprise security policies.
- UEBA is functional, but there is not a “user risk score” perspective that is both dynamic and informed by its advanced analytics, when compared to some of its competitors.
- McAfee is still regarded as a large heritage security vendor by a number of Gartner clients and may struggle with perception issues, especially among organizations adopting a cloud-first strategy

A.4 EXAMPLES OF TECHNOLOGY RESEARCH

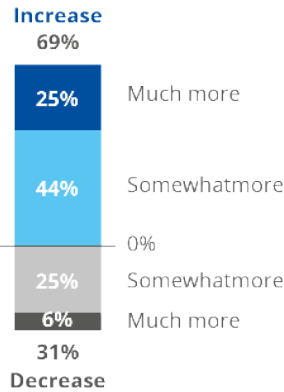
A.4.1 Example of Scenarios and Technology Map

ESTIMATION OF TECHNOLOGY ADOPTION BASED ON DATA FROM SMES (SOURCE GARTNER)

Sample of a Gartner's Cloud survey

Planned Use of Cloud as Result of COVID-19

Our organization plans to **increase** our cloud spending in the wake of the disruption caused by COVID-19.

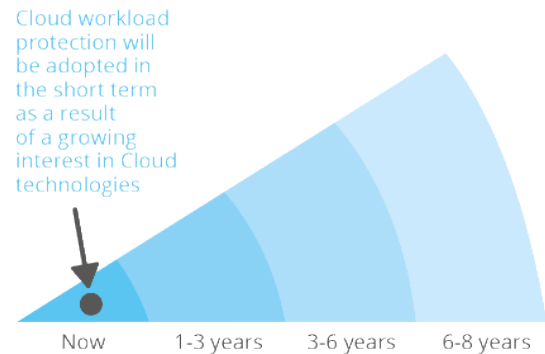


Our organization plans to **reduce** our cloud spending in the wake of the disruption caused by COVID-19.

n = 839, total respondents, excluding "don't know/not sure"
 Question: Please select the statement that best represents your perspective.
 Source: 2020 Gartner CloudEnd-user Buying Behaviour Survey ID: 748510

Estimated time to adopt Cloud Workload Protection

"Growing interest to adopt Cloud technologies in the short term leads to short term investments in Cloud security"



Time needed for significant adoption →

A.4.2 Example of market adoption forecast

Illustrative Gartner's market size estimation methodology

ILLUSTRATIVE TECHNOLOGY TRENDS



Cloud Workload Protection Platform

Passwordless Authentication

ILLUSTRATIVE DRIVERS



Cloud Security

- Growing need to govern the use of cloud and protect sensitive data in the cloud
- Enterprise adoption of tablets and smartphones

Common factors

- CIO willingness to adopt technologies
- Availability of commercial offerings
- Business transformation of organizations
- Regulatory changes

Access Management

- Digital disruption will cement the requirement for more robust authentication, authorization and access management
- Remote access technologies must be complemented by authentication and/or access management tools

ESTIMATED MARKET SIZE IN 2025



High

Very High

A.5 EXAMPLES OF MACRO-ENVIRONMENTAL FACTORS AND ECONOMIC MARKET CHARACTERISTICS

Examples of PEST outcomes for the various components/dimensions:

Example of a Political Factor: Country A has changed government for the third time in four years. The new coalition government has unveiled its programme, with a number of priorities and timeframe for implementation. One of them includes the approval within one year of new laws, which increase the rate of corporate taxation and introduce subsidies to support local business. A foreign company established in this country for 10 years has assessed the potential impact of these new policies and had determined that they would adversely affect the company's operations and increase the degree of competition from local players. In addition, as these measures enjoy a widespread consensus among citizens, it is very likely that the new government would strive to implement them, especially as the next election will be organized next year. As a result, this company is considering moving its operations in another country with a more favorable and competitive business environment.

Example of an Economic Factor: Because of a new legislation, an SME forecasted a 40% growth in the demand of its Industrial Control Systems solutions in the upcoming years. In order to satisfy the future demand, this SME has decided to expand its operations, by making investments to finance the opening of a new laboratory in another country, purchase new machinery as well as starting a recruitment process. This investment decision is expected to indebted the organization for the upcoming years, after which a return on investments is made. In order to lower the impact of the debt over the years, the analysts of this organization have monitored for the last six months the economic indicators in a number of countries. This helps identifying combining a number of favorable economic conditions, such as a low interest rate on corporate loans, an IT-savvy workforce associated with reasonable labor costs, and an affordable price of electricity (relative to other countries), which has remained stable over a period of five years.

Example of Social Factor: The smartphone industry has been object of a negative media coverage in one of its most profitable country, due to the insufficient measures to decrease its carbon footprint (e.g. e-waste, end-of-life) and ensure an appropriate level of data protection of smartphone devices. A survey clearly shows that adult consumers between 30-60 years old, living in the country's largest cities, are the most sensitive to environmental and privacy aspects. These consumers represent the industry's main target audience and the wealthiest group of the country. In addition, the vast majority of this group declared that the sustainability practices employed by companies and the provision of clear information regarding the data protection features of IT devices are key elements influencing their purchases. These findings partly explain the steady and continuous decrease of the smartphones sales of leading companies in this country in favour of more sustainable and more privacy-friendly ones. As a result, one smartphone company is considering to support initiative for sustainable and ethical smartphones, develop a Corporate Social Responsibility programme, commit to use 80% recycled materials, introduce privacy-by-default features in its devices, allow options to install alternative operating systems and create a label to help consumers understand its privacy policy.

Example of Technological Factor: Due to the COVID-19 pandemic, shopping centers have been obliged to implement the new government restrictions, aiming to limit human contacts and the number of people entering a shop in a given timeframe. Many stores have adopted e-payment methods to speed up the checkout process while contributing to maintain a safer environment for both employees and customers.

To be ahead of its competitors and ensure compliance with the new rules, a supermarket chain has decided to make full use of digital technology. As a result, the IT department has developed a mobile shopping app, which makes it convenient for consumers to browse and shop online,

and book a home delivery service. In addition, the online and physical stores of this chain have decided to accept a growing number of e-payment options. The chain has also started its own brand-specific mobile wallet app that would facilitate transactions both online and in physical stores, further encouraging touchless and secure e-payments. In addition, thanks to these technology uptakes, the accounting department of the chain will be able to process transactions more easily and quicker.

B MAIN ABBREVIATIONS

Abbreviation	Description
AM	Audit Management
AST	application security testing
BCM	Business Continuity Management
B2B	Business-to-business
CAPEX	Capital expenditure
CCO	Corporate Compliance & Oversight
CSA	Cybersecurity Act
CSaaS	Cybersecurity as a service
DG-CNECT	Directorate-General Communications Networks, Content and Technology
DG-GROW	Directorate-General Internal Market, Industry, Entrepreneurship and SMEs
DG-JRC	Directorate-General Joint Research Centre
DG-RTD	Directorate-General Research and Innovation
DG-TRADE	Directorate-General Trade
DRM	Digital Risk Management
EC SMAF	ENISA Cybersecurity Market Analysis Framework (EC SMAF)
ECCC	European Cybersecurity Competence Centre
ECCG	European Cybersecurity Certification Group
ELM	Enterprise Legal Management
EC SO	European Cyber Security Organisation
EUIBAs	EU institutions, bodies and agencies
ENISA	European Union Agency for Cybersecurity
IDPS	Intrusion Detection and Prevention Systems
IoT	Internet of Things
NAC	Network Access Control
NDR	Network Detection and Response
OES	Operator of Essential Services

OPEX	Operational expenditure
OSINT	Open-source intelligence
PEST	Political, Economic, Social and Technology
R&D	Research and development
SCCG	Stakeholders Cybersecurity Certification Group
SIEM	Security Information and Event Management
SME	Small and medium-sized enterprises
SOC	Security Operations Centre
SPD	Single Programming Document
SWOT	Strengths, Weaknesses, Opportunities, and Threats
SW	Software
UTM	Unified threat management
VA	Vulnerability Assessment
VRM	Vendor Risk Management
WAF	Web Application Firewall



ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA

European Union Agency for Cybersecurity

Athens Office

Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office

95 Nikolaou Plastira

700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu



ISBN: 978-92-9204-561-6
doi: 10.2824/55221