ENISA CYBERSECURITY MARKET ANALYSIS FRAMEWORK V2.0

(ECSMAF) – V2.0

MARCH 2023

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

AUTHORS

David Wright, Trilateral Research
Nikola Tomić, Trilateral Research
Silvia Portesi, ENISA
Louis Marinos, ENISA

Cut-off date for the data collection for this report: 15 December 2022.

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 reference 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

CONTENTS

EXECUTIVE SUMMARY

Though cybersecurity has been considered within market analysis efforts in the past, the customisation and scoping of cybersecurity market analyses are still at low levels of maturity. Moreover, market data on cybersecurity products, services and processes are scarcely taken into account in the cybersecurity development lifecycle, e.g., within decision-making processes for the launching and development of cybersecurity initiatives, product ideas, policy actions, research funding and deployments. According to Article 8 par. 7 of the Cybersecurity Act (CSA)[1], ENISA has been tasked to "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".

This document is the cornerstone of ENISA activities in analysing the EU cybersecurity market. It presents a **cybersecurity market analysis framework**, a guidance, on how EU cybersecurity market analyses can be performed and be:

- More transparent: a better structuring of the analysis method and understanding of the market, market trends and stakeholders lead to more transparency regarding the results of the analysis.
- More comparable: a structured analysis process makes results more comparable and reusable.
- More customisable towards technology and market trends: the updated market analysis framework can be better customised to take account of trends and dynamics in the cybersecurity market as well as forecasts, market gaps and market niches.
- More agile: the inherent flexibility of setting the market analysis focus and adapting the analysis process to the needs increases the agility of the proposed market analysis method.
- More comprehensive: the inclusion of 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 coherent: the framework facilitates information exchanges of specific market analysis reports, their re-usability and coherence of both raw market data and the analysis of the results.

This framework is subject to future iterations. With increasing performance of cybersecurity market analyses and interactions with stakeholders, ENISA will further develop and update the current framework to increase its efficacy and practicability.

The framework comprises seven major steps to help the analyst conduct a cybersecurity market analysis, as follows:

Step 1 – Choose the market segment for analysis
Step 2 – Scope the market segment analysis
Step 3 – Analyse the market segment
Step 4 – Decide what to ask stakeholders
Step 5 – Collect the data
Step 6 – Analyse the data
Step 7 – Disseminate the results.

---

[1] Regulation (EU) 2019/ of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN.

The framework is targeted at supporting various stakeholders, including the following[2]:

- EU institutions, bodies and agencies (EUIBAs)
- National public authorities, especially cybersecurity authorities
- Industry
- Companies providing cybersecurity products, services and/or processes (supply side)
- Companies needing cybersecurity products, services and/or processes (demand side)
- Consumer organisations and associations
- Research institutions
- Other ENISA stakeholders.

Depending on their requirements, market analyses could have different types of users and stakeholders.

---

[2] There are different ways of grouping. Another way of grouping stakeholders could for instance include: SMEs, Clients and Customers, Supply chain participants, and End-users.

INTRODUCTION

What distinguishes the conduct of a cybersecurity market analysis from any other market analysis?

Cybersecurity is inherently about security, hence, the rules governing the market are different from those selling toothpaste. Some details may be confidential.[3] Many of those with whom the cybersecurity market analyst would like to consult may not wish to reveal much information. It may be challenging to gather the data to make an informed market analysis and informed decision about whether to enter the market.

Such sensitivities may be at work on both the demand side (those wishing to procure a cybersecurity solution) and on the supply side (those wishing to sell their solutions), which may complicate the high-level analysis of both sides undertaken by public authorities and industry associations.

Some cybersecurity products, services or processes may be subject to secrecy obligations or commercial sensitivities. Some products may raise social concerns such as the navigation systems on our smart phones that allow the big companies to know where we are and often what we are doing (picking up the kids from school, going shopping, hanging out at the gym, going for a drink with colleagues).

Cybersecurity solutions, needs and requirements are often kept confidential so that hackers and attackers are not tipped off about the actions of the defender.

Unlike many other markets, the cybersecurity market is highly competitive, as the European Council has determined that it is populated by 60,000 companies[4] – some niche companies and some full-service companies.

The sensitive nature of cybersecurity for companies means a general unwillingness to share data and information. This difficult access to information is compounded by the fact that the cybersecurity market is a diluted and fragmented market – diluted because it is often part of or embedded within other markets – fragmented because it is composed of a myriad of actors.

Given the considerable multiplicity of cybersecurity products, services and processes, a credible cybersecurity market analysis may need to go significantly deeper than other market analyses. Furthermore, cybersecurity is dynamic; it is evolving constantly as attackers adopt new technologies and new strategies to carry out their attacks.

Cybersecurity functions are often a component within existing products, services and processes. A detailed decomposition is often needed to assess various market characteristics of products, such as role, level of market penetration, and market value.

Until recently, market analyses and assessments have been performed mainly by experts with an economics background. Cybersecurity market analysis, however, requires a significant, multi-disciplinary, technically oriented, cybersecurity knowledge. A multi-disciplinary approach helps address the challenges of defining the boundaries of different

---

[3] Confidential here does not explicitly refer to EU classification levels, although it could. The main point is to hide or guard sensitive data against potential attackers.
[4] https://www.consilium.europa.eu/en/policies/cybersecurity/#funding

cybersecurity market segments. Hence, there are many differences between the conduct of a cybersecurity market analysis and other types of market analysis.

This new version of the ECSMAF Version 2.0 (V2.0) is an evolution of the ECSMAF Version 1.0 (V1.0)[5] with the lessons learned from the pilots, i.e. the ENISA EU Cybersecurity Market Analysis - IoT in Distribution Grids[6] and the Cloud Cybersecurity Market Analysis [7], and the contributions of the ENISA AHWG on EU Cybersecurity Market. More evolutions are expected, as ENISA continues to improve its guidance to cybersecurity stakeholders. Future analyses will be able to use V2.0 as a guidance and, in due course, V3.0. Hence, some differences in the structures and approaches of the cybersecurity market analyses based on this framework are inevitable in this still evolving stage.

AIMS OF THIS FRAMEWORK

This cybersecurity market analysis framework aims to:

- perform "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"[8];
- define a method for market analysts for
  o analysing cybersecurity market segments;
  o amalgamating knowledge from cybersecurity market analyses;
- serve as a guide for any stakeholder undertaking a cybersecurity market analysis.

This framework is mainly intended to help ENISA and its stakeholders:

- identify cybersecurity fields that are innovative, emerging and have potential for both demand and supply;
- identify cybersecurity market investment opportunities and risks based on demand and supply requirements;
- help promote an EU-based security market and its objectives by analysing and monitoring the EU cybersecurity market and its evolution;
- assess the importance of market segments in the context of potential threats and vulnerabilities;
- assess market needs for cybersecurity certification; and
- leverage cybersecurity market data for informed policy decisions regarding cybersecurity within the EU and Member States;
- support the European cybersecurity market analysts by applying more rigour and a more comprehensive, structured approach to the analysis of the market prospects for new products, services and/or processes.

TARGET AUDIENCE

We have prepared this framework as an aide to those who wish to undertake an analysis of a cybersecurity market segment.

We can distinguish two types of customers or users of the ECSMAF: those with a fixed budget who have to adapt their strategy to their budget and those (high assurance) customers for whom budget is not the main limitation whereas assurance is.

We especially address *market analysts*, a term that we use in a broad sense and not confined to the private sector. On the contrary, we are especially addressing market analysts who work for the institutions listed below. These institutions are interested in a

---

[5] ENISA, ENISA Cybersecurity Market Analysis Framework (ECSMAF), Version 1.0,
https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf.
[6] https://www.enisa.europa.eu/publications/eu-cybersecurity-market-analysis-iot-in-distribution-grid
[7] https://www.enisa.europa.eu/publications/cloud-cybersecurity-market-analysis
[8] Art. 8 par. 7 of the CSA, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN.

higher level view of the markets, both the demand and supply sides, than individual companies who are more interested in the prospects for their product, service or process. Nevertheless, while companies are not the main targeted stakeholders, they too may find that this framework provides a useful tool.

The framework is targeted at supporting the following stakeholders:

- EU institutions, bodies and agencies (EUIBAs), e.g., the European Commission and its Directorates Generals, such as DG-CNECT, DG-GROW, DG-JRC, DG-RTD, DG-TRADE, but also Eurostat[9] and the European Cybersecurity Competence Centre (ECCC)[10]. EU regulations and impact assessments often take into account market issues. Market analyses are important to help policymakers understand trends as well as related demand and supply issues. Market analyses can help shape future calls in Horizon Europe and other EU programmes where there are market gaps.
- National public authorities, especially cybersecurity authorities. Cybersecurity market surveillance is subject to regulation. The framework and its application may help in comparative market analyses and identifying shared efforts between the Member States.
- ENISA stakeholder groups, e.g., the European Cybersecurity Certification Group (ECCG)[11], Stakeholder Cybersecurity Certification Group (SCCG)[12], and ENISA Advisory Group[13]. The framework may support decision-making for prioritising certification efforts and spotting market gaps.
- Industry and cross-sectoral associations, e.g., TIC Council[14], the European Cyber Security Organisation (ECSO)[15] and the Information Security Forum (ISF)[16]. Industry and professional associations can use the framework to analyse market opportunities, trends, challenges and vulnerabilities and the creation of competitive advantages to EU industry players.
- Consumer organisations and associations, e.g., European Association for Coordinating Consumer Representation in Standardisation (ANEC)[17] and the European Consumer Organisation (BEUC)[18]. By using this framework, such organisations may assess the needs and requirements of consumers for cybersecurity products, services and processes, and their prospects in the European cybersecurity market.
- Research institutions may use the proposed methodology to assess the maturity of existing products and markets and guide the development of new technologies and services.
- Companies providing cybersecurity products, services and/or processes (supply side). As noted above, the European Council has estimated that there are 60,000 such companies in Europe. Some are major companies who already conduct sophisticated market analyses, but by far the majority could benefit from some market analysis advice. For some companies, cybersecurity is their principal business; for others, it is just one line of business among others.
- Companies who need cybersecurity technologies, products, services and/or processes (demand side). Such companies may have information security professionals and/or procurement personnel who need to improve their companies' cybersecurity. Hence, they need to analyse what is available on the market to meet their needs and requirements.

---

[9] https://ec.europa.eu/eurostat
[10] https://cybersecurity-centre.europa.eu/index_en
[11] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-group
[12] https://digital-strategy.ec.europa.eu/en/policies/stakeholder-cybersecurity-certification-group
[13] https://www.enisa.europa.eu/about-enisa/structure-organization/advisory-group
[14] https://www.tic-council.org/
[15] https://ecs-org.eu/
[16] https://www.securityforum.org/
[17] https://www.anec.eu
[18] https://www.beuc.eu

- Venture capitalists, to make them aware of investment opportunities in the cybersecurity realm.

POLICY CONTEXT

ENISA supports cybersecurity market analysis in line with Article 8 and Title III of the Cybersecurity Act (CSA), which stipulates that consideration of developments in the cybersecurity market is a focus of the legislation, in particular, in the context of certification. The CSA considers certification as a main instrument for "avoiding the fragmentation of the internal market"[19]. The goal of cybersecurity certification is "to improve the functioning of the internal market" (Art. 56 CSA). To achieve this goal, the CSA foresees actions to **analyse market trends**. The CSA says that:

- "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 (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 the reduction in EU internal market fragmentation and to provide 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. 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" (Art 4.6 CSA).

Moreover, based on market information, ENISA can provide support in the coordination of the Member States' efforts in market surveillance for supervision of certification.[20] 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" (Art. 58 par 7 (a) CSA).

Some EU legislative initiatives that are worth it to be mentioned because they might be of relevance to the cybersecurity market are the following:

---

[19] See Article 1 par. 1 (b) CSA.
[20] Since this effort concerns compliance issues of certification, it may be used as a tool to obtain valuable information on various aspects of the cybersecurity market. ENISA will coordinate efforts with Member States and the Commission to increase the usability of this source within the context of the Activity 7 of the ENISA Single Programming Document (SPD) 2022-2024. https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-document-2022-2024.

- The proposed Cyber Resilience Act (CRA)[21] that foresees an obligation for the manufacturers and vendors to comply with cybersecurity requirements to address market needs and protect consumers from insecure products and services. It will introduce common cybersecurity rules for connected products and associated services. The CRA will complement the NIS2 Directive and the Cybersecurity Act. It will also complement the Delegated Regulation of 29 October 2021 under the Radio Equipment Directive, by setting up streamlined cybersecurity requirements covering a wide range of digital products and their ancillary services.
- The proposed new Directive on the security of network and information systems (NIS2) that is "part of a package of measures to further improve the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole. It covers the field of cybersecurity and critical infrastructure protection".[22]

The ENISA Single Programming Document 2022-2024 (SPD)[23] takes account of these provisions and sets up corresponding actions under Activity 7, with the aim of fostering

> "a cybersecurity market (products and services) in the EU and the development of the cybersecurity industry and services, in particular SMEs and start-ups, to reduce the 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".

By delivering information on the cybersecurity market, ENISA provides support towards implementation of various European Commission initiatives helping companies (SMEs, micro-enterprises) improve business and production processes, products or services using digital technologies. Examples of such initiatives include:

- European Digital Innovation Hubs[24]: 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"[25];
- Emerging industries and value chains[26]: 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".

To respond to the above exigencies, ENISA began analysing the cybersecurity market, as stipulated by the CSA. It created an Ad Hoc Working Group (AHWG) on the EU Cybersecurity Market[27] and published in April 2022 the first version of the ENISA Cybersecurity Market Analysis Framework Version 1.0 (ECSMAF V1.0), the output of which was intended to facilitate market analysis.[28] This updated framework – Version 2.0 (ECSMAF V2.0) is the successor to the ECSMAF V1.0. There are quite some differences between V1.0 and V2.0, partly based on the pilots[29] of the ECSMAF V1.0 and the feedback

---

[21] Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en . Possible future versions of the ECSMAF may recommend to consider goals and (measurable) effects from the CRA more explicitly.
[22] https://digital-strategy.ec.europa.eu/en/policies/nis-directive
[23] https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-document-2022-2024
[24] https://digital-strategy.ec.europa.eu/en/activities/edihs.
[25] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=70324.
[26] https://ec.europa.eu/growth/industry/strategy/cluster-policy/emerging-industries-and-value-chains_en.
[27] https://www.enisa.europa.eu/topics/market/ad-hoc-working-group-on-cybersecurity-market
[28] https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf
[29] The EU Cybersecurity Market Analysis - IoT in Distribution Grids, available at https://www.enisa.europa.eu/publications/eu-cybersecurity-market-analysis-iot-in-distribution-grid and the Cloud Cybersecurity Market Analysis, available at https://www.enisa.europa.eu/publications/cloud-cybersecurity-market-analysis.

from stakeholders, and partly because the authors of V2.0 wanted a simpler, easier-to-grasp framework.

HOW TO USE THIS FRAMEWORK

The framework consists of seven steps, which the market analyst can follow for identifying a segment of the cybersecurity market to be analysed and for conducting the analysis.

Step 1: Choose the market segment for analysis
Step 2: Scope the market segment for analysis
Step 3: Analyse the market segment
Step 4: Decide what to ask stakeholders
Step 5: Collect the data
Step 6: Analyse the data
Step 7: Disseminate the results

Figure 1: Cybersecurity market analysis steps and actions
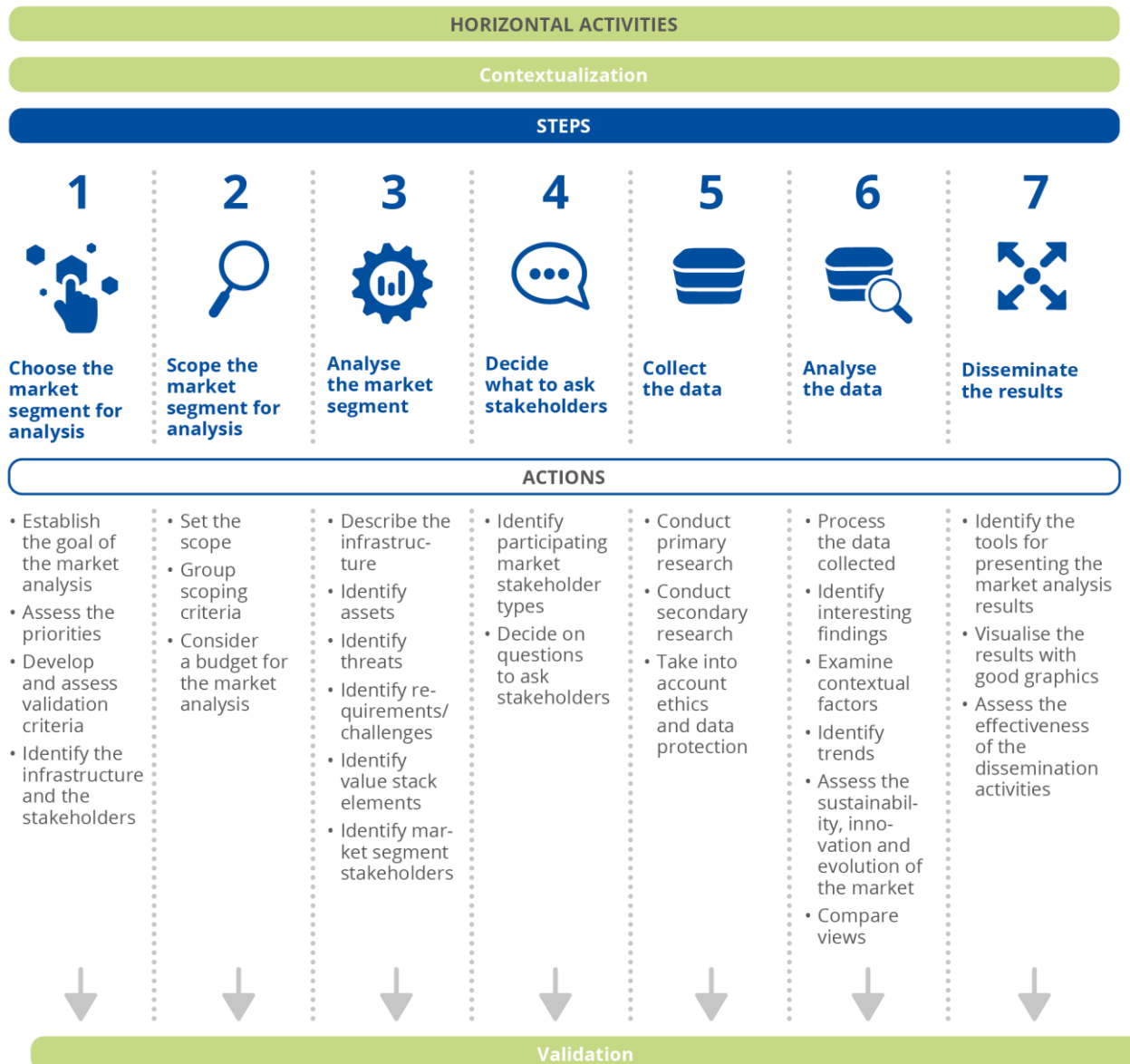
The first two steps of a cybersecurity market analysis are: *Step 1 - Choose the market segment for analysis* and *Step 2 - Scope the market segment for analysis.* These steps set the parameters of the analysis. These parameters set the topic, breadth and depth of the analysis and determine the resources needed for the study, whether in terms of time, budget, human resources or tools. The third step – *Step 3 – Analyse the market segment* – consists of a closer look at the market segment and all its elements, ranging from the infrastructure or architecture of the supply chains, value chain and value stack, assets, threats to those assets, safety controls protecting the assets as well as a snapshot of the major market segment actors. The combined outputs of Steps 1, 2 and 3 influence the structured formulation of questions in *Step 4 – Decide what to ask stakeholders* that take into account the scope of the analysis, the elements of the market segment and the types of stakeholders who will answer the questions. *Step 5 – Collect the data* is the actual process of data collection, using the questions developed in Step 4, but also the use of other primary and secondary research. Following data collection, *Step 6 – Analyse the data* represents a methodical analysis of the data, including an analysis of patterns and the formation of topics or outputs of the analysis. *Step 7 – Disseminate the results* involves careful consideration of how these outputs are presented, including the consideration of potential audiences, timelines, formats, etc.

The market analyst can follow the steps sequentially, carrying out the first and then the next and so on. However, we have provided a detailed table of contents so that the market analyst can refer to particular sections or subsections without needing to follow the whole process if he or she does not need to do so. Each step and this current "How to use this Framework" chapter has some explanatory text followed by some questions, marked off in a blue box, to help the analyst undertake the analysis. The questions are intended to be indicative. Others can be added.

All of the steps involve iterative horizontal activities, in particular *Validation* with stakeholders and *Contextualisation*.

Concerning *Validation*, in Step 1 of the analysis, the market analyst consults stakeholders and/or his or her managers who have sponsored or will benefit from the study on which market segments should be analysed. In Step 2, the market analyst, in consultation with stakeholders (internal and external), selects the criteria to be used in scoping the market analysis. In Step 3, the analyst describes the market segment to be analysed, which may require validation or consultation with external stakeholders, such as cybersecurity or industry experts. In Step 4, the market analyst develops questions to gather the views of stakeholders while keeping in mind that the questions to be asked will likely need to be tailored to the particular stakeholder types. In Step 5, the analyst collects and processes data from a variety of sources, including responses to the questions from stakeholders. The analyst may usefully invite the stakeholders interviewed to review the synthesis. Step 6 is about analysing the data collected. In Step 7, the market analyst selects which visualisation methods to use and presents the results to stakeholders, external or internal to their organisation, for final sign-off.

Concerning *Contextualisation*, the market analyst should pay attention to:

– what is happening in the overall economy, especially with regard to market characteristics such as market dynamics, competition, ownership, profitability, all of which could affect the cybersecurity market segment being analysed;
– macro-environmental, political, regulatory and social factors since they impact the cybersecurity market;
– the state of the art in technology research, trends in going beyond the state of the art, and how an emerging technology might impact the market;
– the importance of the different segments from a disruption viewpoint. The main issue with cybersecurity attacks is that they can disrupt a small retail shop or a whole economy. A successful cyberattack on a small retail shop will not have the

same impact on the economy as one that disables energy or water supplies or even defence systems.

While using this framework, the analyst should keep in mind the internal organisation of the entity he or she is conducting the analysis for as well as the project management cycle that the organisation follows, and engage relevant experts in the analysis as deemed appropriate.

In addition to the above sections, the framework has several annexes to which the reader can turn for more detail on specific aspects relevant for analysis of a particular market segment.

To help the analyst undertake the analysis, we have added some reference questions, which are indicative only; others can be added.

Questions:

- Are you clear on the objectives or purposes or aims of the market analysis you are about to undertake?
- Have you formulated and agreed them with your senior managers?
- If you have been handed the objectives, have you asked yourself if they are clearly written or could be revised to make them more precise?
- Do you and/or your team have the flexibility to deal with ad hoc or urgent requests (new or modified objectives) as a result of an incident with far-reaching impacts?
- Have you considered for whom you will be conducting your cybersecurity market analysis? Are your targets only people internal to your organisation or do they include other decision-makers?
- Have you consulted or are you planning to consult with stakeholders to gather their perspective on particular market segments, their growth prospects, the opportunities for European industry?
- Do you foresee that your market analysis might be shared with others outside your organisation?
- Have you developed a comprehensive contact list of target stakeholders?
- Have you read the whole of this framework? Do you know which bits you want to use?
- Can you apply the framework for the analysis of your particular market segments?
- Are there any commercially confidential aspects of your market analysis that might affect its distribution?
- Have you considered the workflow for implementing the market analysis?

STEP 1: CHOOSE THE MARKET SEGMENT FOR ANALYSIS

If a market analyst is going to conduct a market analysis, he or she should first determine what is the goal, the purpose, the objective of the analysis. The market analyst should identify relevant potential market segments for analysis and choose which to pursue. The 'cybersecurity market' is of vast proportions, especially when one considers the number of existing and emerging technologies, users, types of cyber threats, cybersecurity providers and solutions. The complexity of the cybersecurity market requires segmentation of the market for more manageable analysis. The first step in a cybersecurity market analysis is thus to broadly scan the cybersecurity market and identify the segments, technologies and/or services of interest to the governmental authority, industry association or other stakeholder for whom the analysis is to be undertaken. Market segments can revolve around the supply chain of a technological product or a service, for example, cloud services, 5G networks, Internet of Things (IoT) products and services, etc. Surveying the market will help determine whether some intervention or regulation or support is needed in the market.

This step includes the following actions:

- Establish the goal of the market analysis
- Assess the priorities
- Develop and assess validation criteria
- Identify the infrastructure and the stakeholders.

ESTABLISH THE GOAL OF THE MARKET ANALYSIS

The market analyst should clarify the goal of the market analysis to be conducted. The goal should be as specific and concise as possible. The goal may be driven by legislation (e.g., the CSA). He or she should recognise that the goal may (need to) be recalibrated at a subsequent step. The goal and scope of the analysis are linked. This framework is intended for use at both macro and micro levels. By macro, we mean at industry or market segment scale; by micro, we mean an individual technology or product, service or process.

ASSESS THE PRIORITIES

The market segment to be analysed may be chosen in different ways – suggested by colleagues or experts or stakeholders[30] or, in the instance of industry and consumer associations, by their members. Funding opportunities or incentives, such as tax or R&D credits, may factor in the setting of priorities. In smaller enterprises, the segment can be assigned by company strategy or upper management, so the market analyst may have little choice in the matter. In some instances, the markets to be analysed may be impelled by legislation, such as the CSA[31] or the proposed AI Act[32] or proposed Cyber Resilience Act[33].

The initial survey of the market may produce several market segments of interest. In such scenarios, when choice is plenty, a transparent way of deciding the segment to be analysed is to use a priority scoring table, like the one below. In this table, the market analyst can either singlehandedly or as part of a working group or panel assign numeric values (1 to x)

---

[30] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act. In the instance of ENISA, for example, a request for priorities would be sent to the National Liaison Officers Network, the Advisory Group, the Ad Hoc Working Group (AHWG) on the EU Cybersecurity Market Analysis, or ENISA internal stakeholders (all Units).
[31] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881
[32] https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence
[33] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:454:FIN

or qualitative values (low, medium, high) to the relevance, impact or urgency of particular segments. The added scores will produce a priority list and the first market segment on that list becomes the chosen focus of the cybersecurity market analysis.

Table 1: Example of scoring cybersecurity market segment priorities

Proposed market segment	Threat/ urgency/ [optional category]	Market share/impact/need (Supply)			Market share/impact/need (Demand)			Relevance for analyst's company/ organisation	Total
		Big companies	SMEs	Macro level	Big companies	SMEs	Macro level		
Market segment A									
Market segment B									
Market segment C									
Market segment D									
High relevance: 3 points; Medium relevance: 2 points; Low relevance: 1 point									

In the example table, the first column lists the multiple market segments that the market analyst shortlisted. The columns to the right are for illustration purposes and may be adapted to the needs and triggers of the market analysis. The scores are tallied in the rightmost column and the top scoring market segment is chosen for analysis.

DEVELOP AND ASSESS VALIDATION CRITERIA

As the market analyst contemplates the market segment to be analysed, he or she should already be thinking about relevant criteria for validation of the market analysis, how to assess different proposals from stakeholders for priorities to analyse and validating the choice of segment to be analysed[34]. The criteria referenced in Step 2 and Annex 3 draw on those mentioned in the first version of the ECSMAF.

IDENTIFY THE INFRASTRUCTURE AND THE STAKEHOLDERS

As the market analyst identifies the market segment, he or she should also identify the infrastructure at stake, the value chain and value stack of the domain and the various assets and actors involved (stakeholders at both the demand and supply-side, depending on the scope). Analysis of these elements requires solid sectoral knowledge that will need to be brought into the market analysis effort through sector or domain experts.

To help the analyst undertake the analysis, we have added some reference questions, which are indicative only; others can be added.

Questions:

- What is the trigger of the cybersecurity market analysis (e.g., a policy action, investment strategy, market intervention policy, market-supportive measures, a cyber incident or threat, necessary risk mitigation, observed market trends)?
- Is the goal of your analysis clear, specific, not ambiguous?
- Do you have a method for prioritising market segments?
- Do you need validation for your choice? Who can validate the choice of your market segment?

---

[34] The criteria referenced in Step 2 and Annex 3 draw on those mentioned in the first version of the ECSMAF.

STEP 2: SCOPE THE MARKET SEGMENT FOR ANALYSIS

Once the market analyst, on his or her own or as part of a working group, decides on the market segment, the next step in the analysis is to set the scope of the analysis using various criteria. Market analysts, whether at the EUIBAs or national authorities or associations, will have differing **resources** and **time** at their disposition for the conduct of a cybersecurity market analysis, hence, the level of detail they can analyse will similarly vary. Moreover, they may find that it is not necessary to follow all of the steps nor undertake all of the actions described in this framework. In such cases, they should only undertake those *steps*, *actions* and *horizontal activities* that are relevant and in as much depth as time and resources allow.

Familiarity with the market segment may also influence the scoping of the analysis. If the market analyst is somewhat unfamiliar with the chosen market segment, this step may be better left after *Step 3 – Analyse the market segment*, in which the market analyst breaks down the market segment into its core elements. This order may improve the quality of the analysis scoping exercise. If the market analyst has only a distant familiarity with the chosen market segment, he or she should look for support from an expert advisory or working group who can assist with setting the scope of the analysis. In other cases, the market analyst can proceed directly to scoping the analysis using the prescribed criteria below. Given that *Step 1 – Choose the market segment for analysis* and *Step 2 – Scope the market segment analysis* are non-linear, the market analyst needs to determine their order based on his or her circumstances.

The aforementioned criteria help respond to market-relevant questions, in particular: What will the analysis comprise (demand, supply, market penetration of product, services and processes, market requirements, etc.)?

Step 2 includes the following actions:

- Set the scope
- Group scoping criteria
- Consider a budget for the market analysis.

SET THE SCOPE

Setting the scope includes:

- Balancing the resources available to conduct the analysis. The market analyst may need to revise his or her initial estimates after performance of Step 3 when he or she has a better idea of what would be involved in conducting a credible market analysis. In scoping a particular market segment, the market analyst should aim to capture all important market issues while taking into account available resources for the conduct of the analysis.
- Agreeing the depth and breadth of analysis. The market analyst will need to decide into what depth he or she can go, how far they can "drill" down into a topic. Similarly, the analyst will need to decide on the "breadth" of the analysis, i.e., he or she might be able to cover a wider range of cybersecurity markets, but not to the depth they might like if they were not covering so many topics. Hence, the market analyst may need to recalibrate his or her initial estimates after Step 3.

- Understanding the maturity of the market segment to be analysed. Analysis of cybersecurity markets will most likely involve new and emerging technologies, some of which will be more mature than others – mature, in the sense that they have already penetrated their markets, at least to some credible extent.

The market analyst – and stakeholders – can set the depth and breadth of their analysis using various criteria. The more criteria, the more granular will be their scoping. Stakeholders, whether internal or external, can contribute to the number and precision of criteria.[35]

The market analyst uses the scoping criteria for a specific analysis as the basis for market research questions for stakeholders. Their responses, together with a literature review, contribute to the raw material for preparation of the market analysis. The analyst synthesises their responses into the content of the analysis. The market analyst should circulate the draft analysis to selected stakeholders for comment before finalising it.

GROUP SCOPING CRITERIA

The scoping criteria can be grouped and subdivided according to various criteria, some of which will be relevant and others not, it depends on the specific analysis conducted. The criteria for scoping the analysis can emerge in different ways (from colleagues of the market analyst, stakeholders, literature review, interviews, focus groups). Below, we present the various criteria that the market analyst can consider in scoping his or her market segment.

Criteria for the *demand side* include the following:

- Business impact of procurement of the cybersecurity product, service or process for the demand side
- Required demand-side capability or maturity for deploying the procured product, service or process
- Role of the product or service or process in risk mitigation
- Demand-side presence in various geographic locations
- Demand-side requirements to be met by the procured product, service or process
- Identification of gaps in products, services or processes available to meet demand-side requirements
- Investment plan for financing procurement of the product, service or process
- Assessment of generic company data for the demand side
- Market barriers to procuring the product, service or process.

Criteria for the *supply side* include the following:

- Business impact of the product, service or process for the supplier
- Capabilities to deploy the product, service or process
- Role of the product, service or process in reducing threats
- Presence in different geographic spaces of the supplier who delivers the product, service or process
- Assessment of product requirements
- Gaps and emerging requirements
- Supply-side targets
- Supplier financial measures
- Investment plan to finance development of the product, service or process
- Assessment of supply-side company data

---

[35] For example, members of ENISA AHWG on Cybersecurity Market Analysis have contributed to the scoping criteria in the ENISA Cloud Cybersecurity Market Analysis, https://www.enisa.europa.eu/publications/cloud-cybersecurity-market-analysis.

- Market barriers.

Criteria for *research & development* include the following:

- Identification of market niches
- R&D financial figures
- R&D organisational details
- Assessment of relevant contemporary research activities in market area
- Assessment of efficient funding instruments
- Market drivers in related market area
- Market trends and barriers
- Importance of skills
- Innovative research topics in related technology areas.

Criteria for *regulation* include the following:

- Type, size and areas of influence of the organisation
- Market segments, areas, sectors under regulatory supervision
- Regulatory instruments used
- Cybersecurity threats the exposure to which will be reduced via regulatory activities
- Assessment of transition plans to new regulatory instruments
- Market drivers for regulatory compliance
- Market barriers for regulatory compliance
- Foreseen incentives to support transition by market players.

The various criteria above can be included in a table. The key question for each criterion has a 'yes' or 'no' answer, namely: should this criterion be included in the analysis's scope or not? Here, as an example, is an extract from a table used in ENISA's Cloud Cybersecurity Market Analysis[36].

Table 2: Scoping criteria table (sample)

Criteria group	Criterion	Included in the scope? (Y/N)	Comment/ context criterion	Optional detailed criterion	Included in the scope? (Y/N)	Comment /context detailed criterion
Demand-side criteria	*Business impact of procurement for demand-side:* focuses on the value ratios between the product to be procured and the value chain	Yes		*Value rate of assets enrolled in the product:* indicates the rate between protected assets and total assets	Yes	Consequence of criterion inclusion
				Value rate of procured service: indicates the rate between the value of cybersecurity product and the total income achieved by the entire supply chain	No	Can be omitted (simplification of survey)
	Required demand-side capability or maturity: focuses on the capability level of	Yes		*Capability available:* demand side	Yes	Consequence of criterion inclusion

---

[36] https://www.enisa.europa.eu/publications/cloud-cybersecurity-market-analysis

Criteria group	Criterion	Included in the scope? (Y/N)	Comment/ context criterion	Optional detailed criterion	Included in the scope? (Y/N)	Comment /context detailed criterion
	the demand-side to deploy/manage the procured product			possesses necessary capabilities already		
				Capability to be developed: necessary capability is not available at demand side, but will be developed	Yes	Should be considered to assess implementation effort
				Capability outsourcing: demand side plans to outsource the capabilities needed to deploy/maintain the product	Yes	An important argument for use of cloud computing

Once the criteria for the study are agreed with management and/or stakeholders, the market analyst can devise a set of questions for stakeholders to understand and describe the market segment. Each of the criteria could lead to one or more questions. Step 4 of the framework covers the use of the scoping criteria to formulate questions in more detail. Annex 3 includes a detailed list of criteria used in the Cloud Cybersecurity Market Analysis.[37] Most of these criteria are applicable to the scoping of any cybersecurity market analysis. However, there are also interrelationships and differently structured market segments that should be considered by the analyst in each individual case.

CONSIDER A BUDGET FOR THE MARKET ANALYSIS

The market analyst should prepare a detailed *budget* for undertaking the market analysis. This framework will help the analyst decide which activities he or she should undertake. The market analyst should, however, call upon the expertise of others in his or her organisation to have a realistic budget for the analysis. The budget should be as comprehensive as possible and make provision for human resources, travel, materials, venue hire and catering for focus groups, workshops, market surveys and other consultative methods. Strategic, tactical and/or operational factors are likely to drive budget considerations.

At this stage, the market analyst needs to estimate the effort needed for the analysis. By taking account of the available resources, the market analyst can check the feasibility of the analysis. If there is a mismatch between the scope and available resources, the sponsors of the analysis may need to adapt the analysis criteria and/or the available resources.

The analyst should ensure he or she has a budget agreed with their senior managers in advance of undertaking the analysis. The analyst and his or her finance officer should review the budget and ongoing costs regularly, at least monthly, to avoid the risk of an over-run. If such an over-run seems desirable, the analyst should raise the matter as soon as possible with his or her manager or whoever approved the budget initially.

To help the analyst undertake the analysis, we have added some reference questions, which are indicative only; others can be added.

Questions:

---

[37] ENISA, Cloud Cybersecurity Market Analysis, https://www.enisa.europa.eu/publications/cloud-cybersecurity-market-analysis.

- Have you considered the depth and breadth that would be necessary for meaningful actions by government entities and industry associations?
- How much time do you have to conduct the market analysis?
- How familiar are you with the market segment that your analysis is targeting?
- May your colleagues suggest scoping criteria? May your stakeholders suggest scoping criteria? May scoping criteria emerge from literature review?
- What findings are you hoping to get from the analysis? **May i**nterviews and focus groups contribute to the scoping criteria?
- Do you know where and how you can get the resources needed to carry out the analysis?
- What is the trigger for the cybersecurity market analysis (e.g., policy action, investment strategy, market intervention, market-supportive measures, incident/threat, risk mitigation, market trends, etc.)?
- What will be included in the analysis (demand, supply, market penetration of products, services, processes, market requirements, etc.)?
- What are the market research questions that need to be covered by the analysis?
- What is the 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.)?
- Does the market analysis have a fixed budget?
- Who has to approve the budget for the market analysis?

STEP 3: ANALYSE THE MARKET SEGMENT

Once the market analyst has identified the market segment for analysis, he or she has to analyse it. This step does not strictly have to come *after Step 2 – Scope the market segment for analysis –* and if an existing description or analysis of the market segment exists and is readily available to the market analyst, the duration of this step can be significantly shortened. Either way, the chosen market segment to be analysed will possess certain unique **traits** and **elements** that distinguish it from other market segments. For instance, the way in which the cloud market is structured is different from the way in which the Internet of Things (IoT) is structured and that is different from the way in which the 5G market is structured (or is being structured).

In addition to the **structure** (infrastructure, architecture, models, etc.), different market segments have **different assets that require cyber protection, have different threats and vulnerabilities, and different solutions and controls to protect those assets.** Hence, the analyst may need to consider how a product, service or process is delivered to customers, i.e., the **supply chain**, but also how along that path cybersecurity products, services or processes play a role.

When analysing a market segment, the market analyst should first list its various building blocks, such as infrastructure components, models and service architecture. In the context of a cybersecurity market analysis, the role of the presented material is to set the scene for the various cybersecurity properties, mechanisms, threat models, etc. of important market segment assets. To identify these assets, the market analyst should list as many elements as necessary to capture the market segment.

A good approach to this step is to rely on existing standards and expert publications. The presented structure of a market segment will then be based on an open source analysis of existing information found in various publications, standards and analyses. Most of the collected material will reflect the status of the chosen market segment as it emerged in recent years. The market analyst should thus be aware that existing literature can present a rather static view of the market segment; hence, he or she should follow recent developments and adoption of emerging technologies, such as IoT, 5G and AI, but also the digital transformation imposed by events such as the Covid-19 pandemic.

Some relevant actions in this step are:

- Describe the infrastructure
- Identify assets
- Identify threats
- Identify requirements/challenges
- Identify value stack elements
- Identify market segment stakeholders.

The analyst should ensure he or she has validation, as a horizontal activity going on during all steps, from relevant stakeholders, who can tell him or her if he or she is going in the right direction.

One can envisage the **value chain** literally as a chain where the initial link for a developer might be the development of the product and the final link might be deployment of the

product into the marketplace. Each stakeholder in the value chain might also have a **value stack** that comprises the elements or components, services or processes that they bring to the value chain. For example, in the value stack of the developer might be AI developers, data scientists and technology researchers. Further along in the value chain might be a system integrator who may have a value stack comprising software, red teams to see if they can penetrate the software and network operators. Another link in the value chain might contain a value stack comprising the sales team and lobbyists. See Annex 4 for examples of value stack elements.

DESCRIBE THE INFRASTRUCTURE

The infrastructure of a market segment will differ from segment to segment. It represents the unique constellation of physical points, including the software embedded in the hardware, in which assets can be located. Despite the differences between market segments, the market analyst can structure the description of the market segment infrastructure according to the following levels:

- data level (data storage, data in transit, data channels)
- application level (listing all installed applications using the resources of the market segment, including hardware and software details)
- network level (where are network nodes, supply channels, network security elements).

Other additional levels may be relevant for specific market segments. The market analysts can add these accordingly.

When describing the infrastructure, it is important to consider also the attributes of the market segment. If the infrastructure describes the components of a market segment and 'things that exist' in the market segment, the **attributes** describe how these elements work and what they do. The attributes of a market segment also differ between individual segments, but the market analyst can structure his or her description in the following way:

- essential attributes: how the resources and services are paid for, e.g., on-demand, pay-as-you-go, resource-pooling, etc., usually used as rationale for pricing differentiation;
- service models: a list of existing services offered in the market segment, describing how the infrastructure or its elements are used and what their functions are;
- deployment models: a list of choices by the stakeholders in the market segment on the desired model of sharing, access and ownership of the available resources, e.g., public, private, community, hybrid, etc.

The market analyst should also consider whether companies constitute a specific vertical industry. The market analyst can assume that in every vertical industry a certain value chain and value stack characterise the core business. Such knowledge will enhance transparency and comparability and highlight nuances among stakeholders in the same industry.

Figure 2 below presents an example set of vertical industries. Cybersecurity is a "horizontal" activity for such industries. They all need cybersecurity. Moreover, the supply chain of vertical industries may entail cybersecurity as an integrated part of the offering, a built-in feature of their offerings, but not their main product.

Figure 2: Vertical industries typically related to cybersecurity products, services and processes
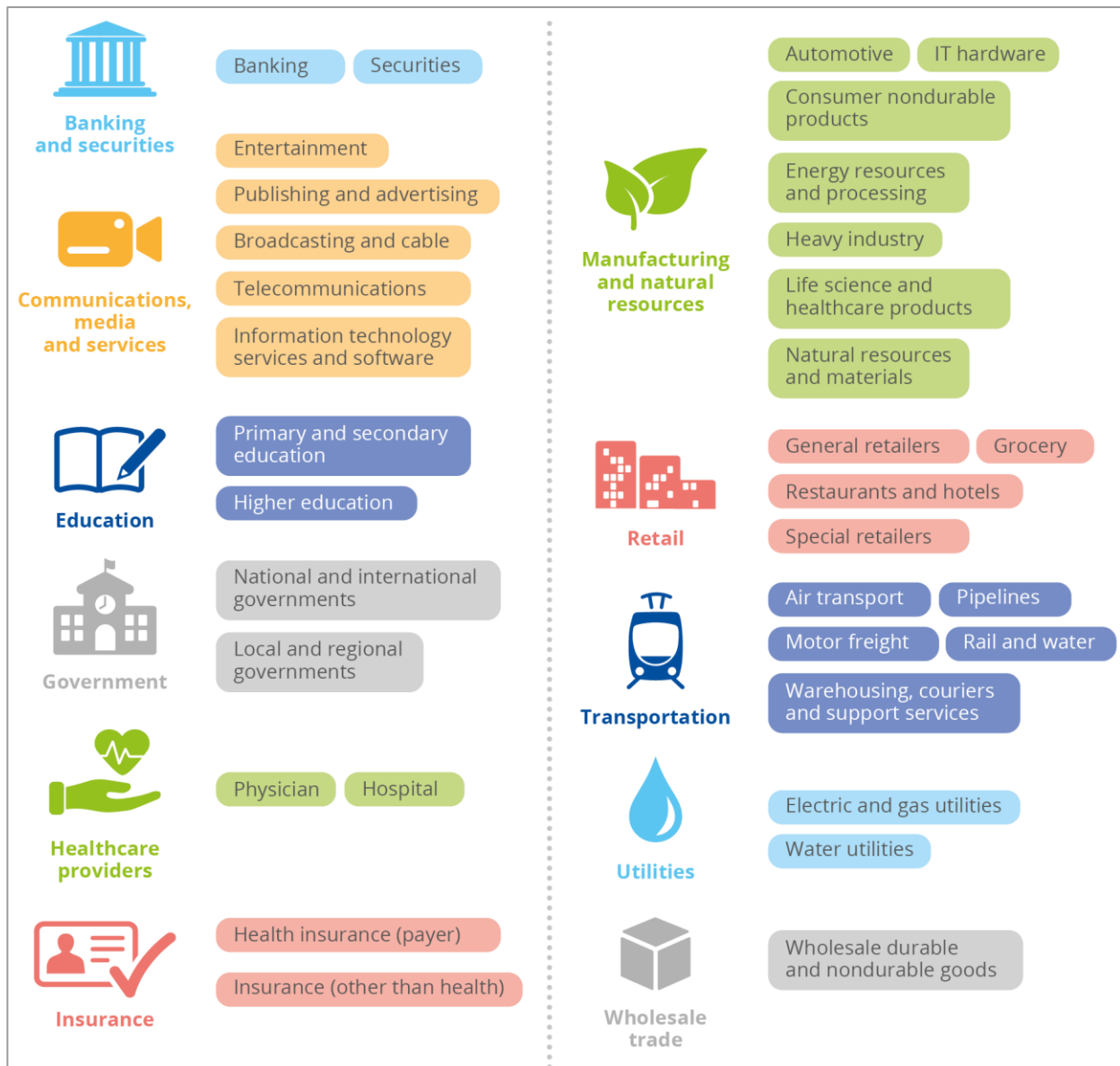
Originally published in ECSMAF, Version 1.0, the Figure above is just one example of how vertical industries can be categorised. Another example could be a categorisation inspired by the NIS Directive[38] or by the proposed NIS2 Directive[39] that list sectors and subsectors.

IDENTIFY ASSETS

A critical element in threat landscaping is identifying the assets and categories of assets to which threats can be exposed. Assets are defined as anything that has value to an individual or organisation, and therefore requires protection.[40] Assets in a cybersecurity market analysis could include infrastructure components (hardware), models, service architectures, processes and processors, networks, data and software. They may be physical assets as well as non-tangible assets (e.g., software or other intellectual property).

---

[38] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016L1148
[39] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN
[40] ENISA, AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence, p. 22, https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges.

Market analysts should consider how the assets can be attacked and protected, their robustness and resilience against an attack.

The analyst should also identify gaps in the market, where there is a need or requirement to be filled or an opportunity to exploit.

IDENTIFY THREATS

Cybersecurity threats to the market segment include ransomware, denial of service attacks, espionage, phishing and spear phishing, disinformation, extortion, data poisoning and many more.

Threats come from a variety of state-sponsored and non-state-sponsored attackers, from criminal gangs to the proverbial teenager in his/her bedroom.

Some threats are more serious than others. Spam is a nuisance, but denial of service can shut down a service for days, weeks or months. Ransomware can result in total loss of an organisation's data and its business. Ransomware attacks against health services have had huge impacts on individual patients whose records disappear into a black hole.

The market analyst should consider the types of attacks that could occur in the market segment of interest and how well prepared, how resilient that segment is against attacks. Is there a relatively high level of awareness of cybersecurity in the segment? Are there incident response plans in place?

IDENTIFY REQUIREMENTS / CHALLENGES

The market analyst needs to understand the market segment's requirements and challenges, some of which are indicated in the following paragraphs.

When identifying requirements and challenges, the market analyst needs to consider all of the links in the value chain or supply chain, especially where the supplier or buyer depends on third parties from whom they buy components or to whom they wish to sell their technology or service.

The market analyst will often ask if there are different ways of delivering or procuring a technology or service and/or note in his or her analysis the innovations found in market delivery.

The market analyst must assess the reliability of the supply chain and its compliance with all relevant legislation and regulatory structures. As the Solar Winds attack in 2020 so well showed, the analyst should also consider or evaluate the security of the supply chain and all links in it. The market analysis should also assess the feasibility: depending on the market segment and the type of survey (e.g., expert interviews with CEOs), such an in-depth study is difficult to implement.

Several kinds of supply chain attacks have been identified[41][42], all of which involve creating or taking advantage of security weaknesses in solutions that companies too often trust. They include:

- Stolen certificates. If a hacker steals a certificate used to vouch for the legitimacy or safety of a company's product, they can peddle malicious code under the guise of that company's certificate.

---

[41] ENISA, Threat Landscape for Supply Chain Attacks, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.
[42] Fortinet, Supply Chain Attacks: Examples and Countermeasures, https://www.fortinet.com/resources/cyberglossary/supply-chain-attacks.

- Compromised software development tools or infrastructure. Hackers leverage the tools for building software applications to introduce security weaknesses in the development process - even before the process is used to create an application.
- Malware preinstalled on devices. Hackers put malware on phones, USB drives, cameras and other mobile devices, and when the target connects one of those devices to their system or network, malicious code is introduced.
- Code included in the firmware of components. Digital hardware is controlled by firmware that helps it run smoothly and interface with users and other systems. Hackers can include malicious code in firmware to gain access to a system or network.

Markets are generally not static, hence, extenuating circumstances can affect the reliability of the supply chain. Brexit, for example, has affected thousands of companies on both sides of the English Channel. Another example is the judgement of the European Court of Justice curtailing the sending of European personal data for processing in the US (the "Schrems II" judgement[43]).

Another element that the market analyst should consider when identifying the market and the challenges are the pricing of the product or service, its unique selling point and the expected uptake.

Organisations need to price their product, service or process so that they at least break even or, better still, make a profit. Pricing is partly a matter of deciding how much the costs of production should be reflected in each unit, how much competitors are charging for equivalent technologies or services, how many units might be bought or sold over what period of time. The market segment, technologies and services should have a unique selling point (USP) – something that distinguishes them from competitors – some feature that the market finds attractive, if not irresistible. The USP will be a factor in driving the expected uptake.

The market analyst needs to consider how the technology or service meets a need or requirement. The analyst should consider the benefit delivered by the technology or service or market segment versus its affordability. No matter what the vendor's pricing strategy might be, if the market cannot afford the service, it will not grow. Hence, the benefit must outweigh the cost and/or be cost saving. The analyst should factor in the point that costs may change over time.

Knowing the competition is mostly relevant to individual companies, and this section of the framework explains why this is important. As mentioned above, the EU Council estimates that the cybersecurity market in Europe comprises some 60,000 companies[44]. Hence, there is a highly textured market, which the analyst needs to understand. The main goals of a competitor analysis include the following:

- Identify your strongest competitors, including competitors based outside the EU but operating within the Union;
- Assess your competitors' strategies;
- Anticipate their actions;
- Anticipate their reactions based on the actions of your own business;

- Influence their actions in a way that benefits your company.[45]

European cybersecurity companies often are competing against the biggest non-EU technology companies who have formidable cybersecurity talent for which they pay handsome salaries much higher than those offered by their smaller European rivals. Hence, the market analysis needs to take into account the availability of talent. The shortage of talent has a clear impact on market growth.

An analysis of the chosen market segment must also take into account potential **barriers** that could slow down or inhibit the exploitation of the market. We have indicated some barriers above, e.g., the challenge of recruiting cybersecurity talent. Here is a list of the most prominent barriers affecting the cybersecurity market.

Financial – Many companies – especially start-ups – are confronted by a liquidity crunch from time to time. A recent EIB-EC report highlighted the challenges that cybersecurity start-ups face in obtaining the financing they need to grow. The same report indicates that it is significantly easier to raise financing in the US compared to the EU.[46]

Technological – Companies who have developed leading technologies or services are sometimes in a race against time to get their products or services deployed before another competitor comes along with a better "mousetrap".

Regulatory – Regulatory requirements may impact the development and deployment of new technologies or services, e.g., the GDPR's requirement to protect personal data or the proposed AI Act which restricts use of surveillance technologies.

Societal (including cultural and behavioural) – A significant body of public opinion may turn against the deployment of certain technologies, e.g., facial recognition or storage of DNA.

Geographic – The deployment of some technologies may be foiled by geographic disparities, e.g., the roll-out of fibre optical cable in rural and remote areas. But what is a challenge for one technology may be a competitive advantage for another, e.g., satellite terminals.

Environmental – Some technologies, e.g., blockchain, are not kind to the environment, e.g., they consume huge amounts of energy.

Insufficient hype – To grow, markets need promotion. However, customers and clients are bombarded with information from many sources, hence, promotional materials may not be enough to make much of a dent in the target market.

Staff shortages – As mentioned above, many cybersecurity companies are constrained by a shortage of personnel and the need to pay them something approximating the salaries offered by big foreign competitors.

Asymmetric competition – European start-ups face a formidable challenge in competing with big, established, non-European companies.

Trust – A lack of trust can be a significant barrier especially in the (prospective) supply chain.

---

[45] https://www.indeed.com/career-advice/career-development/competitor-analysis
[46] European Investment Bank, with contributions from the EC and ECSO, European Cybersecurity Investment Platform, October 2022, p. 8. https://www.eib.org/attachments/lucalli/20220206-european-cybersecurity-investment-platform-en.pdf.

Identification of existing barriers against implementing/integrating cybersecurity into systems may be helpful for the identification of challenges (and opportunities). Such obstacles can be technical or procedural or knowledge based, or based on missing standards.

The market analyst needs also to consider whether the market segment, technologies or services under study are exposed to any threats or have vulnerabilities that need to be addressed. The analyst should consider whether the market segment has any dependencies, e.g., changes in policies or regulations or collaboration with other stakeholders in the market.

Threats and vulnerabilities can take many forms. Security controls are measures undertaken to mitigate the impacts and likelihood of threats to and vulnerabilities in the assets. Mitigation measures are aimed at avoiding, minimising, eliminating, sharing or transferring a risk.

Security requirements – the most appropriate way to express demand needs – will be possible and efficient for analyses focussing on the value chain. Such data, however, are usually difficult to find, especially if the market analysis scope includes stakeholders who are reluctant to be as forthcoming as they could be.

IDENTIFY VALUE STACK ELEMENTS

Segmenting the market consists of two main steps: determining the value chain and the corresponding value stack. The **value chain** is a term derived from Porter's Value Chain[47]. *Investopedia* describes the value chain as:

> "a series of consecutive steps that go into the creation of a finished product, from its initial design to its arrival at a customer's door. The chain identifies each step in the process at which value is added, including the sourcing, manufacturing and marketing stages of its production.
>
> A company conducts a value-chain analysis by evaluating the detailed procedures involved in each step of its business. The purpose of a value-chain analysis is to increase production efficiency so that a company can deliver maximum value for the least possible cost".[48]

Given the technological focus of cybersecurity, we emphasise the primary value chain elements of *operations* and *services* as well as the secondary elements of *infrastructure*, *technology development* and *procurement* – i.e., the market analyst should account for all of these elements in his or her analysis.

We can distinguish between a value chain and a supply chain. They may or may not be the same thing. If the supply chain has some kinks, if certain companies in the supply chain are less than reliable, it cannot be regarded as a value chain. In a value chain, every link (every company or organisation) delivers value.

The **value stack** describes a collection of activities/elements contributing to an organisation's value production. These activities may support a product or service in fulfilling certain standards (e.g., *quality*, *security*, *compliance*, etc.). The value stack follows the structure of the cybersecurity market value stuck elements and represents a decomposition of cybersecurity topics and technologies, services and/or processes. An example of typical cybersecurity value stack elements and their decomposition is shown in Annex 4.

---

[47] Porter, Michael, *Competitive Advantage: Creating and Sustaining Superior Performance*, Free Press, 1985.
[48] https://www.investopedia.com/terms/v/valuechain.asp

IDENTIFY MARKET SEGMENT STAKEHOLDERS

Market segment stakeholders come from both the demand side and supply side. Both need attention from the market analyst. The following paragraphs provide some guidance on identifying those different actors. The market analyst should consider (a) the number of people employed in the market segment, especially if the number is graphed over time, e.g., from now to five years in the future (such long-term forecasts however might not be easy to make); (b) the number of companies active in the selected market segment and (c) the number of stakeholders potentially at risk from malware or other attacks (and the probability and impact of risk assessment). That number could initially be relatively confined but could suddenly leap unexpectedly and highly, as happened when Stuxnet escaped into the wild, when attackers got access to the source code and started using in their own attacks. Many cyber attacks have hit thousands and millions of computers, especially where the attacker has promulgated ransomware or uses a botnet in a denial of service attack.

To assess the numbers above, the market analyst should first make a list of key market segment stakeholders across the supply chain. This list will also serve as a directory of potential stakeholders the market analyst can target in Step 4 as part of the process of deciding what to ask stakeholders to have a stronger, more empirical basis for analysing the market segment.

In this step, as in all steps, the market analyst should seek validation of his or her efforts, principally by seeking comments on the efforts from stakeholders[49]. If necessary, the market analyst may want to return to Step 2 and make some revisions.

The analyst should understand, before he or she starts their work, who will be taking decisions based on the market analysis. The decision to enter or not a particular market segment may be taken by one senior manager or it may be a collective decision. The organisation may have a decision hierarchy. That is, the analyst needs to refer to his or her manager who will need to refer to a director who will need to refer to a vice president – or some similar hierarchy of decision-making. Most likely, the market analyst will also seek the views of key stakeholders, inside as well as outside his or her organisation.

The decision-making process starts with the initiation of the market analysis. There may be various factors that need to be taken into account before a decision is made. The market analyst should understand what the decision-making process will be before he or she starts their work. The organisation undertaking the market analysis may want to circulate the draft analysis to others to have their views before taking a decision. On the other hand, the organisation may not want to share the market analysis with anyone outside a tight circle of top managers for reasons of commercial sensitivity.

To help the analyst undertake the analysis, we have added some reference questions, which are indicative only; others can be added.

Questions:

- How have you characterised the market segment? Have you done so in a way that the non-specialist can easily grasp?
- Have you identified clearly the assets of relevance to your analysis?
- Can you specify the needs and requirements of the target market?
- What threats or factors could disrupt the market segment you are analysing?
- What security controls are or can be put in place to address perceived threats?
- Who are the competitors in the market segment?

---

[49] In the instance of ENISA analyses, for instance, the Agency consults widely with stakeholders (including ENISA management and ENISA bodies), not only on the finalised market analyses, but also components thereof, such as the scoping criteria. ENISA not only consults, but also validates its analyses with stakeholders.

- Where are the points of competition, e.g., a specific technology or service?
- How do competitors' value propositions differ from yours?
- How effective are their marketing campaigns and the 4 Ps: their product, pricing, promotion and place (where they are selling)?
- Do you know who the competitors are now or might be in the coming months or years?
- Have you delineated the barriers to enter the market?
- What is the environmental impact of the selected market segment?
- Have you described the components of the value stack and value chain of relevance to your market analysis and any weaknesses or vulnerabilities in either?
- Do you know who will take the ultimate decision to enter the cybersecurity market?
- Do you know what factors the decision-maker(s) will want to know?
- Does the decision-maker have any questions beyond the details in the market analysis to help him or her make a decision?
- Has the decision-maker had any interactions with market stakeholders who have an (undue) influence on the decision-maker's conclusions? For example, well-funded big technology companies may have many times more meetings with policymakers than civil society organisations.
- Will the public be informed about the decision-making process?
- How will the decision be announced?
- Who will make the announcement?
- When will the announcement be made?
- Are there any legal obligations with regard to the decision-making process?
- Have the criteria for making a decision been made public or, if not, does the market analyst know those criteria?

STEP 4: DECIDE WHAT TO ASK STAKEHOLDERS

Two relevant actions related to this step are:

- Identify participating market stakeholder types
- Decide on questions to ask stakeholders.

IDENTIFY PARTICIPATING MARKET STAKEHOLDER TYPES

Those interested in cybersecurity products, services and processes come from a wide range of different stakeholder groups that can be categorised in various ways and at various levels of granularity. At high level, the principal stakeholder groups include government, agencies, regulators, industry, law enforcement authorities, academics, the media, civil society organisations. Each of these categories can be examined in greater granularity. So, for example: industry can be further subdivided into banking and finance, communications, media and services, insurance, manufacturing and natural resources, retail, transportation, utilities, wholesale trade, technology, etc. The cybersecurity industry comprises a wide range of developers, integrators, service providers and trade associations among others. Governments can be subdivided into education, healthcare, aviation, maritime, border security, critical infrastructure protection, counter-terror intelligence, etc. Governments include a wide range of policymakers, regulators, national authorities with cybersecurity responsibilities, computer security incident response teams (CSIRTs) as well as relevant experts within European institutions, bodies and agencies and their partners. Companies can be profiled by their turnover (revenues), profitability, number of employees, ownership, sector and location. Even internal stakeholders can be grouped, e.g., based on the structure of the organisation.

The market analyst will have some different questions for suppliers, vendors, researchers, developers and regulators – i.e., the questions developed for one segment may be different from those of another segment. Some questions may be the same, but others will be different. Different stakeholders will bring different perspectives to bear, thus, enriching the market analysis.

Identification of market stakeholder types includes types of market stakeholder dynamics (i.e., innovation power, quick rates, niche-product development, research-oriented, etc.). Some examples of stakeholder types include:

- Institutional stakeholders and other stakeholders who can influence the market;
- Consumers (demand side), including procurement officials, institutions and companies seeking cybersecurity controls against the attacks they face every day;
- Suppliers (supply side) often, but not always, companies who seek to sell their cybersecurity products, services and processes to third parties inside and outside the EU;
- Stakeholders who can grow the market;
- Internal stakeholders.

Institutional stakeholders and other stakeholders who can influence the market

These stakeholders are entitled to propose ideas for priorities for the performance of cybersecurity market analyses. They might be institutional stakeholders e.g., Member

States, the European Commission and other EU institutions, bodies and agencies (EUIBAs), industrial associations and stakeholder groups.

Policymakers and regulators, for instance, can influence the cybersecurity markets by the legislation they adopt and implement. Legislation and regulation can curtail a market, but they can also give impetus to a market. They can force non-EU actors to comply with the same rules as European entities. But the latter may gain at least a temporary advantage if they already understand and comply with European legislation, such as the GDPR.

Standards bodies, such as the ISO, CEN, CENELEC, ETSI and IEEE, can influence markets by setting standards for new technologies. For example, ISO/IEC JTC 1/SC 27 addresses information security, cybersecurity and privacy protection. ISO SC 42 addresses artificial intelligence. The market analyst might wish to join national mirror committees that track particular ISO or CEN committees.

Consumers (demand side)

Consumers are those who might buy the product or service, who procure, or who buy a cybersecurity solution. They create the **demand**. Demand volume and growth can be analysed starting from basic financial data – how many units have been sold in the past year and what are the expectations for the next year (and thereafter). However, depending on the detail of the analysis (e.g., value stack), such data might be difficult to find and collect. Hence, corresponding data sources will need to be used.

Suppliers (supply side)

Suppliers are those who can **supply** a cybersecurity product, service or process. This type includes, among others, service providers, enablers, equipment providers, integrators, vendors such as multi-domain industrial asset vendors, multi-domain vendors, single-domain specialised vendors, single-domain specialised vendors (for more details on vendors, see Annex 5).

The market analyst should consider the value-chain elements describing the technologies, services and processes for each supplier type. The level of detail for the value chain will depend on the focus of the market analysis and value stack. The analyst should map suppliers' role in the value chain and value stack and, having done so, create a market guide or landscaping report, providing an overview of the principal vendors; a map defining the market from a supply-side perspective and, as comprehensively as possible, the value chain and value stack and vendor revenues per market segment; vendor profiles rating them according to different methodologies, e.g., company overview and SWOT profiling; market share, size and forecast.

Stakeholders who can grow the market

Researchers can help to grow the market segment with their work, which will contribute to the development of new cybersecurity technologies, assessing the impact of future technology and innovation on the relevant market segment. The analyst might wish to track new patents and the state of the art referenced in journal articles and EU-funded projects.

Developers are instrumental in developing new technologies, services and processes. Their innovations may have an electrifying impact on a market segment. Developers may participate in research projects from universities, industry and governmental entities.

Investors can provide the liquidity that, especially, small companies need from time to time to get their innovations to the market. Investors can be venture capitalists, venture angels, banks and other lending institutions.

Entrepreneurs play a key role in the economy, using their skills and initiative to anticipate needs and bring good new ideas to market. An entrepreneur is an individual who creates a new business, bearing most of the risks and enjoying most of the rewards. The entrepreneur is an innovator, a source of new ideas, products, services and processes.[50]

Internal stakeholders

Internal stakeholders come from different divisions within an organisation, e.g., senior management team, the legal department, operations, research, finance department. Internal stakeholders may include working groups, comprising representatives from relevant stakeholder groups[51].

DECIDE ON QUESTIONS TO ASK STAKEHOLDERS

Once the market analyst identifies the relevant stakeholder types for the chosen market segment, he or she can prepare customised questions to ask those stakeholders[52]. The analyst should be clear about what data he or she wants to gather from the stakeholders. The analyst should consider the types of questions, e.g., avoiding open-ended question and, instead, relying on Yes/No questions, multiple choice questions or Likert (rating) scale questions, i.e., to make the questions easy and quick to answer. The analyst should rank the questions in importance. The fewer the number of questions, the more responses the analyst is likely to get. The analyst should initiate his or her questions of stakeholders by explaining the purpose of the questions and how their responses will be used.

To develop questions to ask stakeholders, the market analyst can refer to the table with scoping criteria (see Annex 3). For every criterion included in the scope (answered with "yes"), the market analyst can phrase a matching question. To use the example from the sample table in Step 2 above (see Table 2), if the scoping table criterion for the demand side about "Required demand-side capability/maturity" was marked with "Yes", the analysis will focus on the capability level of the demand-side to deploy and/or manage the procured product, service or process. The market analyst can then refer to the sub-criteria in the table:

- Capability available: demand-side possesses necessary capabilities already;
- Capability to be developed: necessary capability is not available at demand side, but will be developed;
- Capability outsourcing: demand side plans to outsource the capabilities needed to deploy/maintain the product, service or process.

In our example, all three sub-criteria were marked with "yes", so the market analyst can phrase three questions that will produce data that covers those sub-criteria chosen for the scope of the study. The respective questions could be the following:

- Does the demand side possess the necessary capability to deploy a given procured product, service or process (in the chosen market segment)?
- Can the demand side develop the necessary capability to deploy a given procured product, service or process?
- Can the demand side outsource the capability to deploy a given product, service or process?

The first two of the three questions are dependent on the previous answers being answered with "no". In developing the set of questions, therefore, the market analyst must keep in

---

[50] Adapted from https://www.investopedia.com/terms/e/entrepreneur.asp.
[51] For ENISA, for instance, the ENISA Management Team, the ENISA Advisory Group (AG), the ENISA Management Team and its Ad Hoc Working Group on EU Cybersecurity Market (https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ad-hoc-working-group-on-cybersecurity-market)
[52] Annex 6 contains example questions for stakeholders.

mind the hierarchy, dependencies and order of questions, especially if created in digital format.

When preparing the questions, the market analyst should also refer to the elements and description of the market segment. Some resources or service models may not be present in the scoping table, but may warrant additional investigation. The description may not be complete or information on emerging technologies may be unavailable to the market analyst. In these scenarios, he or she should incorporate questions not covered by the scoping table. The scoping table is a general list of criteria that aims to set general guidelines for cybersecurity market analyses across all market segments, but specific market segments may require expanding the scope of the questions.

The questions are then used as the basis to collect the data. A survey can be developed based on the questions, but other data collection tools may also be considered, including using automated means for instance to collect (additional) data. For data collection methods, see Step 5 below on *Collect the data*.

The market analyst needs to project his or her estimate of the market segment's deployment readiness. The analyst can assess the results from various open source research activities (e.g., European projects, national and international research actions/projects) in terms of their readiness and maturity levels. In doing so, he or she can identify gaps and opportunities that might influence innovation and adoption in the market segment. This task is highly prioritised within the EU (e.g., by the European Cybersecurity Competence Centre, European Innovation Council, ENISA and the latter's Research and Innovation Team), for its actions in strengthening European research and innovation.

To help the analyst undertake the analysis, we have added some reference questions, which are indicative only; others can be added.

Questions:

- Which stakeholder types do you plan to consult for their views on analysing the market segment of interest?
- Have you included among the stakeholders representatives from government, agencies, regulators, industry, law enforcement authorities, academics, the media, civil society organisations?
- Have you included developers, integrators, service providers and/or trade associations among others?
- Have you included among the stakeholders to consult those internal to your organisation, e.g., those responsible for service development and offerings, legal staff, marketing and communications experts, operations, senior management, etc.?
- Have you planned to consult with an adequate number of stakeholders
  o from the demand side?
  o from the supply side?
  o who can grow the market, such as researchers, developers and investors?
- Have you thought carefully about the questions to be addressed to the different stakeholder types to ensure their relevance? (Some questions will be relevant for all stakeholders, others will be relevant for specific stakeholder types, but not others.)

STEP 5: COLLECT THE DATA

Market analysts can gather the data they need for their analyses by a variety of means and from a variety of sources. Surveys, interviews and focus groups are examples of **primary (or empirical) research**. A literature review is an example of **secondary research**. Both methods should consider the **ethics and data protection** aspects of data collection and processing.

Some relevant actions related to this step are:

- Conduct primary research
- Conduct secondary research
- Take into account ethics and data protection.

CONDUCT PRIMARY RESEARCH

Primary research consists of the collection of data directly from stakeholders targeted by the market analysis effort (i.e., relevant market stakeholder types from the relevant vertical industry). Primary research is usually implemented through surveys, focus groups and interviews (online, by phone or mail). If the market analyst is conducting primary research, he or she will need to decide which tools to use. He or she will need to develop a questionnaire, conduct the survey and analyse the results. The different tools for primary research have some pros and cons. The tools are not mutually exclusive; in fact, they are complementary.

Surveys

If the market analyst decides to conduct a survey, he or she must be clear whom they wish to target. Is it the public or a particular demographic or geographic area? The analyst must decide if they can be conducted via telephone or online. The latter are significantly less expensive. Survey questions should be tested ex ante. Surveys require a certain number of participants for statistically meaningful results. Random surveys, e.g., responses to questions on a website, cannot be regarded as representative. If surveys are conducted across different Member States and translation of the questions are made, the analyst must ensure that translations of questions agree with the source questions. Larger surveys might be subcontracted to specialised survey agencies, holding established pools of respondents.

Interviews

The market analyst can conduct interviews in person or by phone (or communication platforms). The advantage of interviews is that the market analyst can pick to whom he or she chooses to talk. It also has the advantage of direct involvement in the collection, the possibility to steer the discussion with interviewees and the ownership of the collected data. The disadvantage is the amount of time and cost involved to conduct them, especially if they require some travel. The market analyst should conduct at least some interviews with key stakeholders, if for no other reason than as a reality check against data gathered from other sources.

Focus groups

The market analyst can explore a cybersecurity market with the help of one or more focus groups. A focus group usually comprises about 10 experts, preferably from diverse entities, who have expert knowledge of the topic or issue at hand. A cybersecurity focus group might bring together representatives from different stakeholder types, for instance, a cybersecurity

developer, a procurement department, a cybersecurity company, a public prosecutor's office, an academic, a civil society organisation, an enabler, such as a legal expert – or some combination thereof. Usually, the group focuses on a limited number of questions for discussion, lasts less than a day, tries to reach a consensus and makes some recommendations in response to the question(s) discussed. Focus groups are good for primary research, but are time-consuming to organise and may require payments to the participants. A focus group requires an animator and someone to take notes. Focus groups may be a useful complement to other data-gathering strategies. For example, focus groups can be used to test how questions in surveys are understood. They can also be used to discuss the results of surveys and/or interviews.

Observation

The market analyst might wish to see how consumers or other stakeholders react in particular situations or where they are subject to the same stimuli. Market analysts have to be careful with respect to the methodology - introducing stimuli and any elements of deception (e.g., untrue information) would carry a specific set of ethics and data protection concerns. Passive observation could be the way to go, e.g., stakeholders' publicly known reactions to existing, publicly known stimuli. Such observation could be online or in person (e.g., how data subjects react to deepfakes). For cybersecurity research, such observation would most likely need to be online. If the analyst is gathering personal data, he or she will need the data subject (the person)'s consent for the observation.

CONDUCT SECONDARY RESEARCH

Secondary research is based on already existing data, including open source intelligence (OSINT). 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. The advantage of this method is its low costs, its efficiency and ownership of collected data. A disadvantage is that the publicly available information might be limited or inaccurate or arcane or not specific enough regarding the vendor's product, service or process or the buyer's interest in knowing who sells the products, services or processes that would fulfil their needs and requirements.

In the instance of secondary research, the market analyst will need to identify various data sources, such as news stories, journal articles, scientific studies, "grey literature", such as government reports, research deliverables (e.g., from EU-funded Horizon Europe projects). The analysts will need to extract the salient data points from his or her secondary research and, in due course, validate his or her research outputs (the market analysis) by means of colleagues, peers and/or stakeholders.

Online communities

Social media may offer a useful market research tool to get immediate feedback on customers' experiences and beliefs and to ask consumers about potential product improvements. If your social accounts do not have hundreds of thousands (if not millions) of followers, do not expect social media to be a viable source of market research.[53] The reliability or validity of data from social media is questionable for various reasons. Social media users are not representative of the public as a whole. Online communities may be subject to manipulation and disinformation.

The market analyst can research social media in several ways:

---

[53] Beaulac, Hugh, How to Use Social Media for Market Research, CXL, 18 Feb 2019, updated 12 Mar 2021. https://cxl.com/blog/social-media-market-research/

- Qualitative content analysis (number of likes/comments/shares). The number of Likes can be a vanity metric, but assessing the engagement rate of consumers on social media may suggest the attractiveness of a marketing message or product.
- Social listening. Passively gather feedback from your customers or monitor opinions about your brand or competitors.
- Polls or questions. Ask questions directly in social media feeds, encouraging users to share thoughts and feelings.[54]

The market analyst should consider which social media will yield the most useful results. As one example, around 97% of B2B and B2C companies use one of the largest online platforms. [55]

Use of automated means

The use of automated means to collect and process information can be considered, including web-crawlers and Machine Learning (ML)/Artificial Intelligence (AI) based text analysis. For instance, ML can be used for pre-filtering large amount of web-based information that is then reviewed by the analyst. When automatic means are used, important related propaedeutic actions include the definition of the areas to search (e.g. common information channels/blogs/newsfeed) and the identification of the key words to use for the search.

Contracted market research

Research can be contracted to external market analysis companies. They provide "turnkey" market analyses in response to market research questions. Though this method leverages existing skills and data collection infrastructure, the market analyst or her team need 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 by performing a scoping exercise, as described above. The downside of contracted research is cost. The upside is that the cost of contracted research is sometimes shared by several clients.

TAKE INTO ACCOUNT ETHICS AND DATA PROTECTION

When planning and executing data collection activities, the market analyst should take into account the ethical and data protection requirements of each method of data collection.

Ethical issues include such things as respect for persons and for human dignity; fair distribution of benefits and burden; the rights and interests of the participants; transparency with regard to the purpose and methods of the activity; the need to ensure participants' free informed consent (with particular attention to vulnerable categories of individuals such as children, patients, discriminated people, minorities, persons unable to give consent, etc.), avoidance of bias. Moreover, the methodologies used in the cybersecurity market analysis should not result in discriminatory practices or unfair treatment. When conducting interviews, the analyst may wish to ask the interviewee to review a written information sheet and to sign an informed consent form (i.e., that the interviewee understands the purpose of the interview and consents to be interviewed).

Among **data protection issues** with which the analyst may need to contend are the following: the legal basis for processing; compliance with data processing principles; pseudonymisation and where feasible, anonymisation; enabling data subject rights, e.g., some experts might wish for anonymity, while others are okay with attribution; repurposing of personal data; the transfer of exports of EU data to non-EU countries; national rules on

---

[54] Ibid.
[55] Ibid.

cold-calling, e.g., when conducting online surveys, etc. These are just a few examples. The GDPR is a key reference.

To help the analyst undertake the analysis, we have added some reference questions, which are indicative only; others can be added.

Questions:

- How are you planning to collect data? Are you conducting interviews, surveys, focus groups, etc.?
- Are you conducting a credible review of journal articles, government reports, third-party analyses, social media, etc., for findings of relevance to the market analysis?
- Do you expect to collect sufficient data to make a credible market analysis?
- Do you expect to be able to cite in the market analysis a credible list of sources for your analysis?
- Are you in compliance with the relevant ethical and data protection frameworks?

STEP 6: ANALYSE THE DATA

This step consists of extracting relevant and valuable information from the data collected. The main actions in this step are:

- Process the data collected
- Identify interesting findings
- Examine contextual factors
- Identify trends
- Assess the sustainability, innovation and evolution of the market
- Compare views.

PROCESS THE DATA COLLECTED

The market analyst will need to process the data collected from various sources and in various forms. For example, interview data will be in the form of notes or transcripts. The output of focus groups and workshops will be reports agreed by the participants. Computers may tabulate some or all of survey data, especially from online surveys, but some telephone surveys may result in responses to a combination of multiple choice type questions as well as unstructured subjective views. In other words, the market analyst may draw on qualitative and quantitative data and need to process it to generate his or her key findings but also to document the evidence for those key findings. The analyst will need to structure and "clean" the data to fix or remove incorrect, corrupted, incorrectly formatted, duplicate or incomplete data within a dataset. When combining multiple data sources, there are many opportunities for data to be duplicated or mislabelled. If data is incorrect, outcomes and algorithms are unreliable, even though they may look correct. The market analyst may benefit from a template for the data cleaning process so so that he or she know they are doing it the right way every time.[56]

Despite best efforts at collecting data from a variety of sources, the market analyst may still find some holes or gaps in the data collected and in the resulting analysis. The analyst can (perhaps) bridge the gap by making some informed assumptions or collect views of a group of experts, e.g., in a focus group aimed at making some assumptions based on scarce evidence.

Processing the data collected inevitably means summarising and synthesising the data so that it is coherent and "tells a story". For example, incident response reports should describe how an attacker penetrated the target, the vulnerability exploited by the attacker, the consequences and impact of the attack, the remedial measures taken or that should be taken, who is responsible for what, etc. So: a story. Or, as another example, the market analyst may want to know how big the potential market is for some new software for detecting attacks somewhere in the supply chain. Hence, the analyst will need to posit the market need and demand for such software that might open up a new, as yet non-existent market. The market analyst may need to conduct interviews and host focus groups to get a feel for the likely demand for the software. The analyst's market analysis report will need to say what data was collected, how and when it was collected, and the findings. To make the case for developing a new market, the analyst will need tell a story, underpinned by evidence, and when there is a lacuna in the evidence, to say what assumption led to the conclusions.

Processing data takes time, especially if there is a serious need for cleaning. The analyst needs to be well aware of the time and complexity of data processing. He or she should be

---

[56] https://www.tableau.com/learn/articles/what-is-data-cleaning

guided by five characteristics of data quality, namely: the validity, accuracy, completeness, consistency and uniformity of the data, i.e., the degree to which the data is specified using the same unit of measure. [57]

The analyst may also consider using for the data collection some automated means such as web-crawlers and ML/AI based text analysis, which might be useful for instance for pre-filtering information or for identifying trend detection.

IDENTIFY INTERESTING FINDINGS

In conducting the analysis, the analyst needs to keep in mind to whom he or she is going to send the analysis and what their expectations of the analysis might be.

The analyst should analyse the data and identify any interesting points or priorities, for instance:

- Gaps between demand and supply
- Incentives driving market entry
- Attractiveness of market entry
- Regulatory and policy compliance
- Contextual factors
- Trends (see section on Identify Trends)

Gaps between demand and supply

Gaps between supply and demand may create opportunities, depending on which side of the fence the market analyst stands. If demand outstrips supply for a new product, service or process, the vendor can price his or her offering higher than in a competitive market with alternatives. Conversely, if supply outstrips demand, the vendor may find he or she needs to lower the price of their offering, perhaps to uneconomic levels.

The market analyst needs to consider where and why there are gaps in the market. Gaps could appear anywhere in the supply chain. The market analyst needs to be aware that his or her forecast could be completely undone by a failure or weakness in the supply chain, including some stakeholder in the chain who decides to increase significantly the price of their offering. For example, a shortage of chips may be caused by the collateral damage of war or simply bad planning or a shortage of a precious mineral such as palladium, manganese, cobalt or lithium used in smart phones. The analyst should contemplate how the gap could be filled and the likely impact of the gap on the growth in the market segment.

Gaps between supply and demand may arise from the fact that a vendor may need a steady supply of a component but may want to minimise how many such components it must carry in its inventory versus not being able to meet the demand. In the cybersecurity sector, gaps in supply and demand may also arise because of a shortage of talent. Thus, the analyst should also consider the labour demands in the market segment of interest.

Incentives driving market entry

Developers and vendors of new and emerging technologies and services are driven to the marketplace by various incentives, among which are these:

- Profit – Almost always the principal incentive;
- Transferability – Technologies developed in a government or university research lab can be spun out to the private sector. The research for one application may be transferred to one or more other applications;

---

[57] Ibid.

- Adaptability – The technology results can be adapted across different applications;
- Reputation – Stakeholders invest in an interesting market segment to enhance their reputation, even if a profit is not likely in the near term;
- Caution – Many experts are concerned about the impact of quantum computing on cybersecurity, hence, many entities – governments, universities, tech companies – are conducting research even though the pay-off may be a decade or more away;
- Shared interests – Stakeholders may be motivated by shared interests, like those needed to build a 5G network or those needed to agree extended reality standards.

The market analyst needs to specify what are the principal drivers for cybersecurity research, innovation and exploitation in the market segment of his or her analysis. We expect certification to be a major driver in the marketplace. For example, much of the Cybersecurity Act is devoted to cybersecurity certification. Cybersecurity certification may play a more important role in some domains than others.

Attractiveness of market entry

The market analyst needs to consider the costs, revenues and profits expected from the market segment over time. The market analyst should cite the evidence for his or her estimates and how confident he or she is in those estimates.

Regulatory and policy compliance

The market analysis should provide some contextual information on the legislative and regulatory environment. The market analyst should alert his or her readers to the status of prospective legislation that could have an impact on the cybersecurity market such as the proposed AI Act or Cyber Resilience Act.

These pressures on the supply side will include compliance with the legislation such as the EU's General Data Protection Regulation, the Cyber Security Act, the Digital Services Act, the Digital Markets Act, the NIS 2 directive and the e-Privacy regulation.

On the demand-side, the buyers of cybersecurity products, services or processes also face regulatory or policy pressures, e.g., in adequately securing their network or complying with standards.

EXAMINE CONTEXTUAL FACTORS

The market analyst should take contextual factors into account in his or her analysis. There are two classic methodologies for identifying and analysing contextual factors. First is the SWOT analysis focusing on the strengths, weaknesses, opportunities and threats. Second is the PESTLE methodology to analyse the impact of contextual factors that may be political, economic, social, technology, legal or environmental (PESTLE) (more information on PESTLE factors is provided below).

SWOT analysis

A SWOT analysis – which focuses on the strengths, weaknesses, opportunities and threats – is a widely used methodology in governmental and non-governmental institutions, associations and the private sector. Among other things, it serves policy objectives – e.g., how strong is the EU in a particular market segment, where does it have opportunities to extend its sovereignty and autonomy – as well as competitor analysis – e.g., what threats does the EU face, where is it vulnerable. It is also a useful methodology for scoping a market analysis, especially when it used in question mode. Below are examples of SWOT-

based questions for market analysis conducted by an EUIBA, an international organisation or a European association.

Strengths

- What are the EU's strengths in the selected market segment?
- Are there some national or EU champions in the selected market?
- How is our technology or service better than that of our competitor?
- What are the prospects for further developing our strengths in the selected market?

Weaknesses

- What weaknesses do we (does the EU) have in the market segment?
- Does the EU / do we have some strategic vulnerabilities, i.e., our weakness in the selected market segment has some knock-on effects in other markets?
- Will our weakness increase our dependency on non-European third parties?

Opportunities

- Do "we" see some opportunities for Europe / for our institution in developing and deploying a new technology or service or process in the cybersecurity market?
- How is it an opportunity? Is it a gap in the marketplace worth exploring?
- Does the opportunity require some support from the EU or national governments?
- Does the opportunity come with any conditions?
- Is the opportunity one about which we can talk openly or does it require confidentiality until the product or service is deployed?

Threats

- Does Europe / our institution face a threat in our chosen market segment? How serious is it?
- What is the nature of the threat? Is it technological, financial, economic or other?
- Is there a perceived gap in the market that could be subject to an attack? Or is there a gap that could be addressed with a new cybersecurity product or service?
- What is the origin of the threat?
- What can we do to mitigate the threat?
- What might happen if we don't respond to the threat?

PESTLE factors

Market analysts typically consider multiple perspectives to gain an overview of key trends. One of the most frequently applied measurement tools to analyse how external factors (Political, Economic, Social, Technology, Legal, Environmental)[58] affect the operations of an organisation or a specific market segment is abbreviated PESTLE. These factors help public and private organisations understand potential impacts, take better decisions, allocate resources more efficiently and introduce changes to generate improvements in impacted areas. They also help identify current and future opportunities and risks and how to best manage them.

A PESTLE analysis typically includes the following steps:

- Identifying the key events within the six external factors;

---

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

- Analysing possible impacts on the organisation or market segment;
- Categorising opportunities and threats; and
- Tracking trends.

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

The *political factor* of the PESTLE methodology aims to assess how new government policies and changes in legislation affect a specific market segment or an organisation's operations. Typical examples are tax, employment, environmental and other laws (see also legal factors below). The political factor encompasses aspects such as the general political climate of a country, the degree of government stability, its regulations, international relations and posture. Terrorist attacks usually prompt demands for more surveillance and politicians may accede to such demands even though they may know that increased surveillance does not automatically lead to a reduction in cybercrime. An example is the current geopolitical crisis.

The *economic factor* assesses the key determinants of an economy's performance such as inflation rates, exchange rates, cost of production, economic growth, disposable income of consumers and the unemployment rate. These determinants may have a direct or indirect impact on organisations 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. The economic factor can impact the way organisations price their products, services or processes. An example of an economic or financial contextual factor is the increasing cost of cybercrime and cyber attacks, with far-reaching costs, such as those caused by the WannaCry ransomware in 2017 or the shutdown of the Colonial Pipeline network in the eastern US in 2021 following a ransomware attack against the computerised equipment managing the pipeline.

The *social factor* refers to the demographic characteristics, cultural attitudes and customs of the target populations. Typically, this includes for instance 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. An example of a social contextual factor affecting the cybersecurity market is the public's reaction against facial recognition in public spaces.

The *technology* factor pertains to innovations in technology that may affect the operations of organisations 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. Artificial intelligence is an example of a technology that has had a transformative impact on the cybersecurity market. Defenders employ AI in anomaly detection to guard against all kinds of attacks, while attackers have begun to employ AI in viruses (Stuxnet is a classic example and one of the first of an AI-driven virus). AI is helping defenders to speed up reaction times, when time is of the essence when the organisation is experiencing an attack.

The *legal factor* concerns an organisation's compliance with relevant laws that could affect its position in the market. For instance, in the context of cybersecurity market analysis, the market analyst should endeavour to analyse how changes in the data protection legislation may impact the demand and the supply of certain products, services or processes.

The *environmental factor* concerns the impact on the environment of a cybersecurity product, service or process. Often environmental factors have been overlooked. For example, blockchain technology might be good at the confidentiality and privacy of transactions, but it burns huge amounts of energy. Many of our infrastructures have

environmental impacts, such as water delivery systems and energy networks. Such infrastructures are constantly combatting attacks with as strong cybersecurity as they can manage. Successful cyberattacks against infrastructure may cause huge environmental damage, e.g., disruption to water networks, oil spills or black-outs. To counter attacks, defenders need to understand the vulnerabilities in environmental and infrastructure networks.

IDENTIFY TRENDS

Cutting across contextual factors or even animating them are cybersecurity market trends. They are one of the main elements to understand and estimate market developments. Market trends emerge from a variety of factors. They may be of a generic nature or sector specific. The relevance of market trends for a specific analysis requires a multi-level assessment to cover these dimensions.

Market analysts can foresee trends in technology research, but environmental factors and economic market characteristics may also help identify trends within the scope of the cybersecurity market analysis and in the context of supply-side and demand-side research.

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.

The maturity of particular cybersecurity markets can be analysed through the penetration of cybersecurity products in the value chain of an organisation, the ratio of cybersecurity spending in IT investments, the number of incidents impacting their business, level of cybersecurity capability, etc. The maturity is indicated by the number of iterations a technology has experienced.

In the following subsections, we provide examples of trends in the cybersecurity domain.

Rise in cybercrime and cyber attacks

Estimates of the cost of cybercrime and cyber attacks vary significantly, but all estimates show a rise in cybercrime and cyberattacks. If the market analyst can illuminate the costs of cybercrime and cyber attacks in the chosen market segment, so much the better. The market analyst must make a considered judgment regarding how susceptible (or not) a new technology or service might be to cyber attacks.

Criminals are innovators. They are interested in new technologies if they will support their malign intents. Blockchain, for example, was helpful in disguising their transactions and, especially, for money laundering. Criminals have played with deepfakes for advancing pornography and social engineering. They have also begun to use artificial intelligence. The market analyst will need to make an estimation of how criminal use of new technologies might impact the market segment chosen for analysis.

Cybercrime as a service has also been facilitating the growth in cyber attacks, so that anyone can get tailor-made tools and lists of potential victims at a fraction of the cost of developing such tools themselves.

Growth in the attack surface

The Internet of Things (IoT) already numbers billions of devices in use and that number is expected to grow rapidly in the next few years. The IoT includes the chips in your toaster, fridge, oven and other appliances, but also the SCADA devices in critical infrastructure and

driverless vehicles, where the risk of manipulation keeps cybersecurity experts awake at night. The IoT is greatly expanding the cyber attack surface.

Growth in the type of cybercriminal and cyber attacker

Not only is the attack surface growing, the range of cybercriminals and cyber attacks has also been growing, partly because malware and the instruments for deploying it are declining in cost and expertise.

So cybercriminals and cyber attackers range from state-sponsored attackers to attackers who free-lance for government agencies on one day and on their own account the next. They include organised crime gangs, like the mafia, to discontented individuals and braggards who want to show off their expertise in taking down big companies or government agencies.

ASSESS THE SUSTAINABILITY, INNOVATION AND EVOLUTION OF THE MARKET

The market analyst should include in his or her analysis study some assessments or predictions about the sustainability of the market segment and how it might evolve over the next five years or more and what innovations might arise during that time to propel or undermine the market. Sustainability means more than a growing number of customers: it also means its environmental sustainability and, particularly, the UN Sustainable Development Goals.[59]

COMPARE VIEWS

The analysis should highlight any views that either support or are at variance with the analyst's finding. He or she should bring those other views to the attention of his or her senior managers or whoever is funding the market analysis. Views that support our market analysis are always welcome, of course, but even other views may be welcome in showing the need for more in-depth research. More conservative market analyses may also be welcome in terms of injecting a note of caution into decisions to invest in or grow a particular market. Contrary views are not always genuine; hence, the analyst should determine who funded and sponsored contrary studies and what might have been their motive in doing so.

To help the analyst undertake the analysis, we have added some reference questions, which are indicative only; others can be added.

Questions:

- What findings are interesting for the addressees of your analysis?
- Do the data collected show any gaps between demand and supply?
- What specific contextual factors are relevant for your market analysis?
- Which trends could affect your market forecasts, either for selling or procuring products, services or processes?
- Have you searched whether there are other market analyses that have already been conducted in your area of interest?

---

[59] https://sdgs.un.org/goals

STEP 7: DISSEMINATE THE RESULTS

The organisation conducting the analysis will decide on whether to make the market analysis public.

The three main actions in this step are:

- Identify the tools for presenting the results
- Visualise the results with good graphics
- Assess the effectiveness of the dissemination activities.

IDENTIFY THE TOOLS FOR PRESENTING THE RESULTS

In presenting the market analysis, the analyst should consider who the decision-makers are, who will make the ultimate decision to promulgate (or not) the results of the market analysis. The decision-maker may have some strategic or tactical considerations of which the analyst is unaware in the decision to promulgate those results.

The market analyst should consider how he or she should present the results of the market analysis to the aforementioned decision-makers. There are various ways of doing so – a report, a slide presentation, a video, a webinar, online, etc. Various tools can be employed, none mutually exclusive.

VISUALISE THE RESULTS WITH GOOD GRAPHICS

The target audience will absorb better the findings of the market analysis if they are presented in a visually and graphically pleasing way. No matter how great the market analysis is, if it is not presented in a user-friendly format, and if the target stakeholders are baffled by the results, the analysis will have been for naught. Think carefully about visualising the results of the analysis and how to present them. Remember the adage: a picture is worth a thousand words.

ASSESS THE EFFECTIVENESS OF THE DISSEMINATION ACTIVITIES

The market analyst will want to know how colleagues, management and stakeholders have received his or her analysis and, especially, how successful he or she has been in disseminating the results of the analysis. As noted above, there are various tools that can be used to disseminate the results; some will be more successful, more effective than others. For future reference, for new market analyses, the analyst will want to learn lessons, to learn which dissemination activities work best. The analyst should assess the effectiveness of the various activities within a month or so of submitting his or her results while those results are reasonably fresh in the minds of the target stakeholders.

Just as there are different means of dissemination, there are different ways of measuring their effectiveness. For example, if the analyst's organisation has released a press release about the analysis, then the analyst can monitor how many news outlets (traditional media, newspapers, magazines, websites) have picked up the press release. Publishing the press release on the organisation's website, the analyst can see if there have been more site visits and click-throughs. He or she can convene a focus group to understand the views of a cross-section of stakeholders about the analysis and how it has been presented.

CONCLUSIONS AND WAYS FORWARD

In this section, we draw some brief conclusions and suggestions about the way forward.

First, this cybersecurity market analysis responds, in part, to an obligation on ENISA by the Cybersecurity Act (CSA)[60], which was referenced in the Introduction above. Art. 8 par. 7 of the CSA says that "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". The ECSMAF provides guidance on the things that should be taken into account in conducting cybersecurity market analyses. It contributes to the implementation of the CSA: it supports a strong EU cybersecurity market; it supports the regulatory oversight of the market; it supports cybersecurity certification, as provided in the CSA. It also supports the EU's December 2020 Cybersecurity Strategy for the Digital Decade[61].

Second, this cybersecurity market analysis framework is a guidance targeting several different cybersecurity stakeholders, including market researchers and strategists and other cybersecurity analysts. We have made it as readable and accessible as possible to stakeholders.

SCENARIOS AND FORESIGHT

The analyst might wish to develop scenarios indicating technology adoption, application and its impacts as well as its threats and opportunities. Drawing scenarios helps the analyst and stakeholders understand the challenges facing the development of the market segment, the requirements for mitigating risks, reducing threats relating to the deployment, operational and societal issues of technology adoption.

The market analyst, together with colleagues and/or stakeholders, can create a scenario of what they would like the market segment to look like in five years, for example. The construction of the scenario (as well as the market analysis itself) can be accompanied by other foresight techniques such as *horizon scanning* or *Delphi exercises*. Constructing a desired, but reasonably realistic scenario, is followed by *backcasting*, i.e., what steps do we need to take to arrive at the desired scenario? The market analyst should bring together a diverse group of stakeholders to participate in the scenario construction exercise to avoid missing any important perspectives. At the outset of that exercise, the market analyst can present his or her findings and views of where the market segment could or should be in the chosen time frame. The participants can express their points of view about what steps should be taken to arrive at the desired scenario and what hurdles might have to be crossed to get there. The market analyst should then draft the scenario based on the discussion and then run the scenario by those participating in the exercise for their comments before drafting a new final version reflecting those comments as well as the actions to be taken to arrive at the desired scenario.[62]

---

[60] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881.
[61] Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN
[62] There are hundreds of articles on writing scenarios. Here is one, which can be used as a guide to construction of scenarios with increasing stakeholder consultation. Wright, David, Bernd Stahl and Tally Hatzakis, "Policy scenarios as an instrument of policymaking", *Technological Forecasting and Social Change*, Vol. 154, May 2020. https://www.sciencedirect.com/journal/technological-forecasting-and-social-change/vol/154/suppl/C.

A cybersecurity market analysis can benefit from scenarios and foresight, which help us map the desired future and the ways forward (the steps) to get there. The section on scenarios and foresight could form part of Step 7 or it could come even earlier as part of Step 5. As we mentioned in the Introduction, the market analyst does not need to follow the framework slavishly; he or she can pick from the detailed table of contents which bits he or she might want to use and set aside other parts. The section on scenarios and foresight is a case in point; the analyst might wish to engage in scenario construction and foresight as an aide to market analysis or at the conclusion, that is, the market analysis can serve as an input to the scenario construction.

THE WAY FORWARD

This is the second version of the framework, ECSMAF Version 2.0 (V2.0). It is an evolution of the ECSMAF Version 1.0 (V1.0)[63] with the lessons learned from the pilots, i.e. the ENISA EU Cybersecurity Market Analysis - IoT in Distribution Grids[64] and Cloud Cybersecurity Market Analysis[65].

It is entirely possible that it will be followed by subsequent versions, especially based on the lessons learned from other pilot analyses that may be conducted in the future and if we receive feedback from stakeholders about how we can improve it and how they can use it to improve the EU's position in the cybersecurity domain. Doing so is not only to vitalise the EU cybersecurity market, but also to contribute to the EU digital sovereignty.[66]

To help the analyst undertake the analysis, we have added some reference questions, which are indicative only; others can be added.

Questions:

- Which would be the best tool(s) that you have already available or you could easily procure for presenting the results?
- Which visualisation elements can you use for presenting the results?
- Do the tool(s) and visualisation elements you intend to use have the results of your analysis reaching the target audience?
- Have you considered constructing a scenario of where your organisation would like to be in (say) five years?
- Have you contemplated which stakeholders you could invite to a brainstorming session for constructing the scenario?

---

[63] ENISA Cybersecurity Market Analysis Framework (ECSMAF) - Version 1.0, https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf
[64] https://www.enisa.europa.eu/publications/eu-cybersecurity-market-analysis-iot-in-distribution-grid
[65] https://www.enisa.europa.eu/publications/cloud-cybersecurity-market-analysis.
[66] On the concept of EU digital sovereignty see for instance: European Parliament, *Digital sovereignty for Europe*, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.

ANNEX 1 – ABBREVIATIONS

Abbreviation	Description
AG	Advisory Group
AHWG	Ad Hoc Working Group
AI	Artificial Intelligence
AM	Access management
AM	Audit management
ANEC	European Association for Coordinating Consumer Representation in Standardisation
AST	Application security testing
BCM	Business continuity management
BEUC	European Consumer Organisation
B2B	Business to business
B2C	Business to consumer
CASB	Cloud access security brokers
CCO	Corporate compliance & oversight
CEN	Comité européen de normalisation
CENELEC	European Electrotechnical Committee for Standardization
CERT	Computer Emergency Response Team
CSA	Cybersecurity Act
CSaaS	Cybersecurity as a Service
CSPM	Cloud security posture management
CSIRT	Computer Security Incident Response Team
CWPP	Cloud workload protection platform
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
DLP	Data loss prevention
DMZ	Demilitarized zone
DNA	Deoxyribonucleic acid
DRM	Digital risk management

DSA	Digital Services Act
ECCC	European Cybersecurity Competence Centre
ECCG	European Cybersecurity Certification Group
ECSMAF	ENISA Cybersecurity Market Analysis Framework
ECSO	European Cyber Security Organisation
ELM	Enterprise legal management
EOS	European Organisation for Security
ETSI	European Telecommunications Standards Institute
EUIBAs	EU institutions, bodies and agencies
EU TIC Council	European Union Testing, Inspection and Certification Council
GRC	Governance, risk management and compliance
GDPR	General Data Protection Regulation
IAM	Identity and Access Management
IaaS	Infrastructure as a Service
ICT	Information and communications technology
IDPS	Intrusion detection and prevention systems
IEEE	Institute of Electrical and Electronics Engineers
IGA	Identity governance and administration
IoT	Internet of Things
ISF	Information Security Forum
ISO	International Organization for Standardization
ISO/IEC JTC 1/SC 27	ISO International Electrotechnical Commission Joint Technical Committee 1 Special Committee 27
JRC	Joint Research Centre
KMaaS	Key management as a service
ML	Machine Learning
NAC	Network access control
NASDAQ	[US] National Association of Securities Dealers Automated Quotations stock exchange
NDR	Network detection and response
NIS	Network and Information Security Directive
NLO	National Liaison Officer
OSINT	Open Source Intelligence
PaaS	Platform as a Service
PAM	Privileged access management
PESTLE	Political, Economic, Social, Technological, Legal and Environmental dimensions (analysis method)
R&D	Research and development

SaaS	Software as a service
SASE	Scure access service edge
SCADA	Supervisory control and data acquisition
SCCG	Stakeholder Cybersecurity Certification Group
SIEM	Security information and event management
SME	Small and medium-sized enterprise
SOAR	Security orchestration, automation and response
SOC	Security operations centre
SPD	Single Programming Document
SWOT	Strengths, Weaknesses, Opportunities and Threats (analysis method)
USP	Unique selling point
UTM	Unified threat management
VA	Vulnerability assessment
VPN	Virtual Private Network
VRM	Vendor risk management
WAF	Web application firewall

ANNEX 2 – SCORING PRIORITY MARKET SEGMENTS

The following table is an example of how priorities can be established on the basis of votes by different stakeholders, such as members of the ENISA Ad Hoc Working Group.

Proposed market segment	Supply			Demand			ENISA relevance	Total
	Big companies	SMEs	EU	Big companies (ESPs)	SMEs	EU		
Cloud computing	High	Low	Medium	High	Medium	High	High	1 st
IoT cybersecurity	Medium	Medium	High	Medium	Medium	High	Medium	2nd
Managed Security Service Providers (MSSP)	Medium	Medium	Medium	Medium	Medium	Medium	Low	3rd

High relevance Medium relevance Low relevance

ANNEX 3 – CRITERIA FOR SCOPING THE MARKET ANALYSIS

Here is a set of criteria for scoping a market analysis. ENISA used these criteria to set the scope of a cloud cybersecurity market analysis. However, almost all of the criteria are relevant for any cybersecurity market analysis.

Table 3: Examples of criteria for scoping the market analysis

Scoping criteria categories	Scoping criteria
Demand-side	• Assessment of generic company data for the demand side; • Role of procured service for the business; • Required demand-side capability or maturity for deploying the procured product; • Role of the product in risk mitigation; • Demand-side presence in various geographies; • Demand-side requirements to be met by the procured product; • Identification of gaps in products available to meet demand-side requirements; • Investment plan for financing procurement of the product; • Market barriers towards deployment of the service.
Supply-side	• Supplier financial figures; • Assessment of supply-side company data; • Presence in different geographic spaces of the supplier who delivers the product; • Business role of the product in the supplier supply-chain; • Capabilities required to deploy the product; • Role of the product in threat reduction; • Assessment of product requirements; • Gaps, emerging requirements; • Investment strategies to finance development of the product; • Market trends and barriers.
Research and development (R&D)	• R&D financial figures; • R&D organisational details; • Assessment of relevant contemporary research activities in market area; • Assessment of efficient funding instruments; • Market drivers in the related market area; • Market trends barriers; • Importance of skills; • Innovative research topics in related technology areas.
Regulation	• Type, size and areas of influence of the organisation; • Market segments, areas, sectors under regulatory supervision; • Regulatory instruments used; • Cybersecurity threats the exposure to which will be reduced via regulatory activities; • Assessment of transition plans to new regulatory instruments; • Market drivers for regulatory compliance; • Market barriers for regulatory compliance; • Foreseen incentives to support transition by market players; • Analysis of existing cyber security standardization activities and the involved stakeholder communities (this may give information on emerging market segments)

ANNEX 4 – EXAMPLES OF CYBERSECURITY VALUE STACK

The structure and content typical cybersecurity value stack elements and their decomposition is shown in the table below. The presented material is derived from work undertaken by ENISA, the European Cyber Security Organisation (ECSO) and the EC's Joint Research Centre (JRC).

Table 4: Structure and content of the typical cybersecurity value stack elements

Value Stack group	Value Stack	Value Stack elements
R&D and education	**Education:** This market consists of offerings related to cybersecurity education.	Cybersecurity academia / research
		Cybersecurity professional education
	R&D: This market consists of 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 comprises 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 comprises 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 comprises encryption software, enterprise data loss prevention (DLP) software and tokenisation 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 (PAM) software and user authentication software.	Access management software
		Identity governance and administration software
		Privileged access management software
		User authentication software
		Other identity and access management SW
	Infrastructure protection SW: This market consists of networks and endpoints (including servers, laptops, mobile devices, 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 comprises software products in the form of –platforms, usually hosted, 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 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 consists of cybersecurity products within enterprise network equipment market such as firewall and next generation firewall	Firewall equipment, intrusion detection and prevention systems, network access control equipment, network detection and response, zero trust network access

	solutions, unified threat management (UTM) products, intrusion detection and prevention systems (IDPS), network access control (NAC), network detection and response (NDR).	
	Hardware security: This market 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 and systems: This market consists of physical hardware used to recognise biometric signals.	Hardware biometric security module
		Software biometric security module
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	These activities include 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 (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 consists of cybersecurity solutions design & architecture development.	Security design, engineering and architecture development

	Integration services: This market consists of integration, planning, scheduling and testing.	Implementation and integration, interoperability testing
	Development: This market consists of cybersecurity development, implementation and testing.	Implementation support (technical assistance/expert support services)
Managed services	**Managed response services:** This market comprises cybersecurity operations and technology maintenance services that include incident management and response.	Managed detection and response (MDR)
		Incident response
	Cybersecurity device management: This market 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 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
	Virtualised cybersecurity services: This market 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 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 consists of any 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 consists of services related to the creation of certificates and their maintenance. Though usually this activity is being performed by/on behalf of national or non-profit organisations, numerous companies offer this know-how.	Services related to the assessment and implementation of assurance levels for product certification (e.g., component criticality assessment, risk and threat assessment, identification of attacker potential, formulation of requirements, gap analysis, identification of product evaluation levels, identification of controls, testing, etc.).
	Service and process certification services: This market consists of services related to the cybersecurity certification service and process, such as development,	Services related to the assessment and implementation of assurance levels for service and process certification (e.g., criticality assessment, risk assessment, identification of attacker potential,

	operations, production processes and services.	formulation of requirements, audit, gap analysis, identification of controls, etc.)
	Professional certification services: This market primarily consists of the infrastructure (human, technical, documents) needed to obtain professional cybersecurity certificates (note: though it has overlaps with cybersecurity training above, we regard it as a separate element due to its market size and importance).	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.).
	Accreditation services: This market consists of the services that lead to an accreditation of an organisation to offer and perform cybersecurity-related certification efforts (see above mentioned services).	Services related to the accreditation of cybersecurity certification (accreditation of testing infrastructures/labs, accreditation of processes and skills).

The structure of value stack may vary, depending on the sector in scope. The table below shows the cybersecurity related value stack elements in the area of cloud computing, as they have been used within the ENISA Cloud Cybersecurity Market Analysis[67].

Table 5: Value stack elements in the area of cloud cybersecurity

Value-stack group	Value-stack elements	Comments
Cloud Software Security	Cloud testing tools and services	
	Secure web gateways	
	VM backup and recovery	
	Cloud application discovery	
	Cloud security posture assessment	
	Cloud management platforms	
	Cloud workload protection	
	Cloud data backup	
	Cloud data protection gateways	
	Security-as-a-service	
	Software defined perimeter	
	Container security	
	Micro-segmentation (SW defined segmentation)	
	Secure Software Development tools and practices	
	SASE (secure access service edge)	
	Application Audit / logging	
	Security orchestration, automation and response (SOAR)	
Data security	Data loss prevention	
	Data encryption	
	Disaster recovery as a service	
	(IaaS) Container encryption	
	Data Audits/ logging	

---

[67] https://www.enisa.europa.eu/publications/cloud-cybersecurity-market-analysis.

Value-stack group	Value-stack elements	Comments
Identity Management	Identity-as-a-Service, Identity and Access Management	
	User awareness	
	Multi-factor authentication	
	Password policy	
	Key management as a service (KMaaS)	
	Identity proofing services	
	Role- and attribute based access and control	
	Audit / logging	
Operational cybersecurity	Cloud security assessments	
	Security rating service	
	Penetration testing	
	Security information and event management (SIEM)	
	Cyberthreat Intelligence and threat hunting	
	Cloud monitors / continuous monitoring	
	Forensics	
	Vulnerability management	
Network security	VPN- Network encryption	
	Firewall-as-a-Service	
	DMZ	
	Intrusion detection	
	Network logging	
Cloud Hardware security	Secure tokens	
	Hardware availability/ recovery	
	Hardware redundancy	
	Hardware security policy (e.g. testing)	

ANNEX 5 – EXAMPLES OF VENDORS

Some examples of vendors 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 are 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 are 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 are 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 larger vendors. They emerged in developing cybersecurity market segments where they leverage

innovative, state-of-the-art, cybersecurity technologies to ensure differentiation.
Below are 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.

ANNEX 6 – EXAMPLE QUESTIONS FOR STAKEHOLDERS

ENISA formulated the following questions for stakeholders for its cloud cybersecurity market analysis[68]. They may serve as a model or template for questions pertinent to other cybersecurity markets. Some questions may be more relevant than others, hence, the market analyst should feel free to adapt the questions he or she thinks most relevant to their market study. The analyst may have other questions of particular relevance to their market segment.

DEMAND

- In which countries in the EU are you present?
- Indicate number of employees.
- Indicate approximate annual revenue (for NGO or public administration, please put 0).
- Indicate main sector of activity.
- Indicate main subsector of activities.
- Indicate ownership structure.
- What % of digital assets do you have in the cloud? (i.e., percentage of total digital assets)
- What % of sensitive data (finance, accounting, employee, customer intelligence, IPR, health or payment etc.) is stored in the cloud?
- What service model of cloud do you use?
- What deployment model for cloud services do you use?
- How many different cloud providers do you have (including public, private)?
- What are the main cloud attributes that you use?
- Which of these categories of measures have you already implemented or plan to implement in the context of cloud cybersecurity? (i.e., implementations might be within purchased services)
- Which compliance requirements are the most relevant?
- Which business or other requirements must be taken into account?
- What are the most relevant cybersecurity threats for your environment?
- What threats do you aim to reduce with cloud security solutions?
- Have you experienced an impactful incident in the last 12 months?
- Which type of impact was it?
- What was the overall impact of incidents?
- Were any of incidents subject to mandatory reporting to a regulatory body, government, data subject, etc.?
- Were any cloud infrastructure vulnerabilities reported to you by your provider during last year?
- Did you need to take any action by your side?
- Could you please provide some examples of such actions?
- What are the most relevant challenges for your environment?

---

[68] https://www.enisa.europa.eu/publications/cloud-cybersecurity-market-analysis

SUPPLY

- Indicate number of cloud customers.
- Indicate approximate annual revenue of cloud business.
- Indicate total value-added cloud business (= Revenues minus the price paid for materials and services).
- Indicate customer sectors of activity for entire cloud business.
- Indicate any other sector.
- Indicate activities in subsectors of banking, communications or media, education, government, healthcare, insurance, manufacturing, retail, transportation and/or utilities.
- Indicate activities in wholesale subsectors.
- In which countries in the EU are you present?
- Indicate geographical areas of customers.
- Indicate investment plan for cybersecurity.
- Indicate current implementation strategy for cybersecurity offerings.
- Indicate percentage in revenues for investments in research, development and innovation.
- Indicate ownership structure.
- Which are the service models offered?
- Indicate available certifications, attestations (e.g., audit reports, such as SOC2) for SaaS, PaaS, IaaS.
- Which deployment model for cloud services do you support?
- What are the three most important cloud attributes in your offerings (by means of income)?
- Which of these categories do you already implemented or plan to implement in the context of cloud cybersecurity?
- Indicate detailed Identity and Access Management (IAM) functions, antivirus and end point protection functions, incident detection and response functions, value-added cybersecurity functions, infrastructure security and security policy enforcement, cloud hardware security.
- Which compliance requirements are the most relevant?
- Which business or other requirements must be taken into account?
- What are the most relevant cybersecurity threats for your environment?
- What threats do you aim to reduce with cloud security solutions?
- Did you experience one or more impactful incidents in the last 12 months?
- What was the overall impact of the incident?
- Were any of the incidents discovered subject to mandatory reporting to a regulatory body, government, data subject, etc.?
- What are the most relevant cybersecurity challenges for your environment?
- How many vulnerabilities have you handled last year?
- How many of those vulnerabilities were found in systems of your providers?
- How many of them took more than a week or more to fix?
- Indicate events or incidents that might impact your overall market.
- Indicate other important effects on market (e.g., deployment, regulation, network effect, bottleneck)?
- Do you think there are gaps and niche areas in the market?
- Indicate what you think are the most important cybersecurity research topics.
- What are the main technology drivers for the cybersecurity of cloud computing? Name up to three (e.g., AI, 5G/Edge).
- What are the main business drivers for the cybersecurity of cloud computing? Name up to three.

R&D

- Indicate the total yearly budget available for research projects.
- Indicate the number of research staff in your organisation.
- Indicate the main source of research budgets/grants.
- In which countries or geographical areas in the EU do you have a physical presence?
- In which sectors does your organisation conduct research? For example, in banking, communications or media, education, government, healthcare, insurance, manufacturing, retail, transportation and/or utilities.
- Indicate activities in wholesale subsectors.
- Indicate the average number of staff participating in a project.
- Do you collaborate on a regular basis with third-party organisations?
- Indicate ownership structure of your organisation.
- Indicate the number of projects in cybersecurity in the past year.
- Indicate the most important research topics for you in cybersecurity.
- Indicate the developments that you think will be most impactful for cybersecurity (both negative and positive impact).
- What are the most relevant cybersecurity threats in your opinion?
- What do you consider to be the most important instruments for research funding?
- What do you regard as the most important market, financial, economic or societal drivers promoting research and/or innovations in the EU?
- What barriers do you consider for research uptake?
- What technological barriers have you encountered?
- Does your organisation suffer from a shortage of skills?
- Indicate ease of finding proper funding for cybersecurity research.
- Do you know about any newcomers or companies with great innovation value?
- Do you think there are gaps and niche areas in the market?
- Name the three most important issues that research on cybersecurity must solve.

REGULATORY

- Indicate the size of the population in your area of responsibility.
- Indicate the countries or geographical areas influenced by your activities.
- Indicate the subject of cybersecurity-related regulatory activities in which your organisation is involved.
- Indicate sectors that fall in the regulatory supervision of your organisation, e.g., in banking, communications or media, education, government, healthcare, insurance, manufacturing, retail, transportation and/or utilities.
- Indicate activities in wholesale subsectors.
- Indicate the type of your organisation.
- Indicate the role of your organisation in regulatory work.
- Indicate which regulatory instruments are most consequential for you.
- Do you have a plan to transition to an EU-approved cybersecurity certification scheme?
- What are the most relevant cybersecurity threats in your opinion?
- What threats or vulnerabilities do you aim to reduce by with an EU-approved cybersecurity certification schemes?
- What are the most relevant challenges to be addressed through regulatory work in your opinion?
- How many cybersecurity vulnerabilities have been reported to your organisation in the last year?
- Can manage these vulnerability reports with your actual resources?
- Have dedicated funds been allocated to support companies in transitioning towards the use of the regulatory compliance instrument chosen?

- Indicate other markets, financial, economic, societal or legal drivers for promoting regulatory compliance.
- What are the main regulatory barriers?
- What are the technological barriers encountered?
- What may be the impact of data localisation requirements and the ensuing need to invest in local infrastructure?
- Do you see opportunities from the regulatory framework (i.e., the drive to have services that are compliant with the GDPR, financial regulation, etc.)?
- Indicate activities subsectors of government.

FURTHER READING

ENISA, AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence, December 2020.
https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

ENISA, Threat Landscape for Supply Chain Attacks, July 2021.
https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

ENISA, Foresight Challenges: A study to enable foresight on emerging and future cybersecurity challenges, November 2021.
https://www.enisa.europa.eu/publications/foresight-challenges

ENISA Single Programming Document 2022–2024, January 2022.
https://op.europa.eu/en/publication-detail/-/publication/168b7270-d7e6-11ec-a95f-01aa75ed71a1/language-en

ENISA, Risk Management Standards, March 2022.
https://www.enisa.europa.eu/publications/risk-management-standards

ENISA Cybersecurity Market Analysis Framework (ECSMAF), Version 1.0, April 2022.
https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf

ENISA, EU Cybersecurity Market Analysis - IoT in Distribution Grids, April 2022.
https://www.enisa.europa.eu/publications/eu-cybersecurity-market-analysis-iot-in-distribution-grid

ENISA, Cloud Cybersecurity Market Analysis, March 2023.
https://www.enisa.europa.eu/publications/cloud-cybersecurity-market-analysis

ENISA Threat Landscape Methodology, July 2022.
https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology

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