TLP - CLEAR

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA Technology and Innovation Radar Methodology

APRIL 2026

About ENISA

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

CONTACT
For contacting the authors please use radar@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS
ENISA

ACKNOWLEDGEMENTS
Greta Nasi, Nico Abbatemarco, Benedetta Burston (Bocconi University)

ISBN 978-92-9204-790-0, DOI 10.2824/2390334

Table of Contents

Introduction

1.1 Context of the Technology and Innovation Radar on Cybersecurity

In line with its strategic objective, the European Union Agency for Cybersecurity (ENISA) has commenced the development of a **technology and innovation radar (TIR)** on cybersecurity as part of its 2025–2027 single programming document. Among other things, the initiative aims to systematically measure the impact of new and emerging technologies on cybersecurity by identifying key trends, assessing their technological maturity and mapping their trajectory from research to market adoption.

The TIR on cybersecurity is positioned within the broader **ENISA foresight methodology** and provides a structured approach for anticipating cybersecurity developments. Starting from ENISA's foresight framework, several methodological pathways are available, ranging from horizon scanning and Delphi surveys to trend radars. The TIR represents one of these possible approaches, selected for its ability to integrate both qualitative and quantitative evidence in a dynamic, visual and frequently updated format. By embedding the TIR within this overarching foresight system, ENISA ensures methodological coherence and continuity with its previous foresight exercises, creating a unified analytical chain from early signal detection to policy-relevant insight.

A core element of this initiative is the establishment of an evidence-based methodological framework that will allow ENISA to accurately identify cybersecurity trends and patterns, including both mature innovation ready for adoption as well as early-stage developments that can warrant continued monitoring. Through a combination of structured data analysis, expert validation and stakeholder consultation, the radar offers a dynamic view of the technology landscape relevant to cybersecurity, grounded in real-world evidence and strategic foresight, ensuring a structured connection between research, innovation and market adoption. Additionally, the framework will contribute to ENISA's broader role under the Cybersecurity Act by providing strategic insights to EU policymakers, research institutions and industry stakeholders.

The purpose of the following document is to outline a comprehensive methodology for identifying and analysing technology signals that are relevant to the cybersecurity landscape. It describes the main stages that should be followed and explains how these variables can be assessed and validated through a structured process. Furthermore, the document explores how the resulting data can be integrated into a set of visualisation formats, to support decision-making, foresight and stakeholder engagement.

NB: In order to reach this methodology, a comprehensive desk-research was carried out on existing TIRs/tools and related frameworks. The most important findings are found in Annex 0.

.

Methodology

2.1 General References

The methodology adopts a **signal-based direction** as the central analytical unit. A signal can be a trend, a tool or a platform outlining an emerging cybersecurity trend. This choice reflects current **industry and foresight best practices,** where signals of change serve as detailed evidence of emerging trends. Alternative foresight directions, such as pure megatrend analysis, scenario modelling or expert-driven Delphi exercises, were considered; however, the signal approach was preferred because it allows higher temporal resolution, traceability and quantification of technological momentum. It also facilitates direct connection with ENISA's data-driven monitoring capabilities and the upcoming public radar dashboard.

As such, the primary objective of the radar is to **anticipate and evaluate technological developments that may significantly impact the cybersecurity landscape through the mapping of signals**. In foresight practice, a signal is commonly understood as a **tangible manifestation of novelty** – an observable indicator of emerging change.

Signals are often weak in their early stages, but they offer early glimpses into developments that could, over time, evolve into significant trends or disruptions. The radar serves as a mechanism for detecting such signals, tracking innovation trajectories and synthesising insights into actionable intelligence for policy and strategic planning.

At the same time, the radar also monitors stronger, more mature signals – technological applications that are already showing clear evidence of adoption or market traction. These are systematically evaluated for their adoption readiness, enabling stakeholders to distinguish between technologies that are still emerging and those that are approaching mainstream deployment.

By combining foresight on weak signals with grounded assessments of strong ones, the radar provides both **early warning and short-term strategic insight**, supporting a balanced view of the evolving cybersecurity technology landscape.

The radar is targeted at a **multi-stakeholder audience** comprising primarily EU policymakers, cybersecurity agencies, research and development (R & D) programme managers and institutions involved in technology foresight, regulation or innovation planning. The outputs are also expected to benefit the research community and industry stakeholders involved in cybersecurity innovation.

The following section sets out the methodology to be followed to develop the TIR. **Figure 1** illustrates its six overarching steps, providing an overview of the entire process. A detailed overview of the methodology is presented in **Annex 1**.

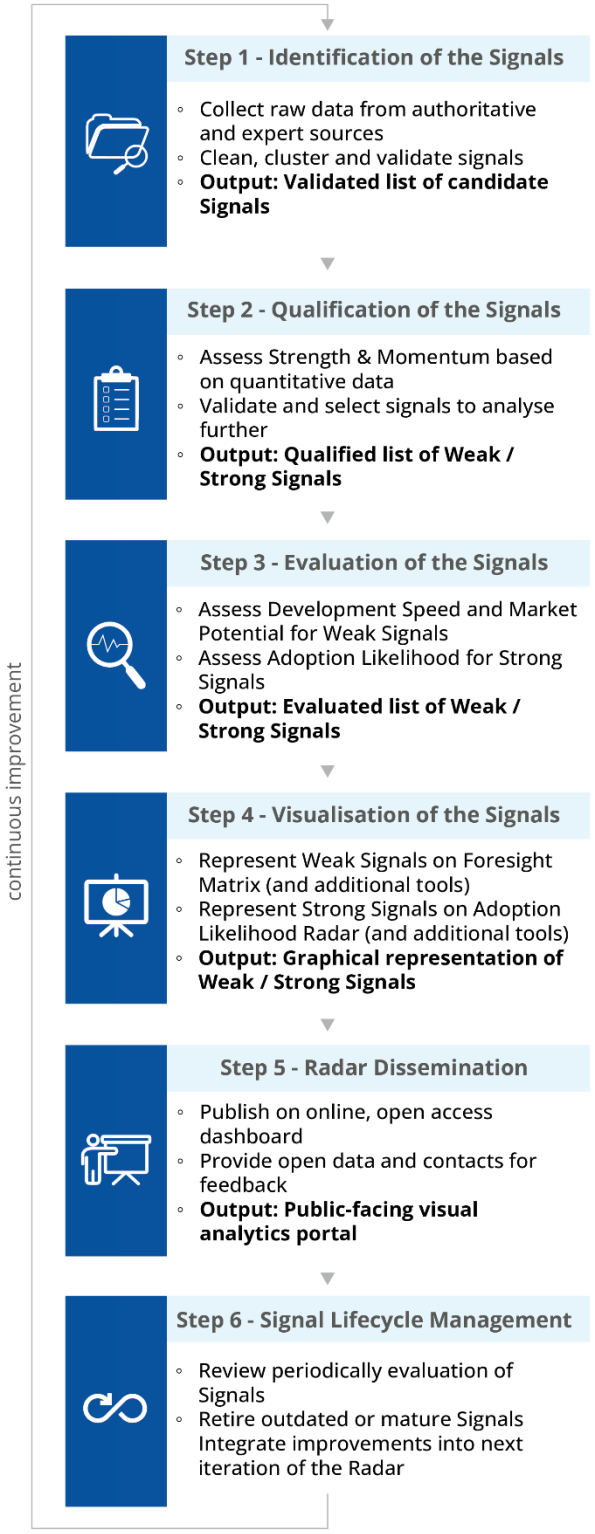


Figure 1 High-level representation of the methodological steps of the TIR

The effective implementation of the radar requires a **structured governance system** ensuring coordination, accountability and continuity across all phases of the methodology. The governance model establishes clear **roles, responsibilities and decision-making** flows, combining ENISA's internal management structure with external expert engagement.

Annex 2 provides a proposal of how governance can be managed across the different phases of the methodology, illustrating the key actors involved, their main functions and the corresponding outputs. Nevertheless, the governance structure remains to be tested and decided within ENISA.

2.2 Identification of the signals

The first operational phase focuses on identifying signals that are relevant to cybersecurity. This step always begins with the structured collection of inputs (Section 2.2.1) from multiple authoritative sources (Section 2.2.2) and, when necessary, may be complemented by stakeholder consultations (Section 2.2.3). Once gathered, these signals undergo a data cleaning and consolidation process to eliminate duplicates, resolve overlaps and clarify ambiguous entries (Section 2.2.4). Leveraging different types of sources supports risk mitigation: by combining inputs from diverse yet complementary environments, the process reduces dependency on any single knowledge domain or institutional perspective.

Each signal is subsequently classified through a multi-dimensional and structured clustering approach (Section 2.2.5). This structured categorisation enables consistent tracking and facilitates comparative analysis across different sections of the radar. The final step in this phase (Section 2.2.6) involves the first validation and screening of signals, ensuring that only those with sufficient relevance and evidence progress to the next stage of analysis.

By the conclusion of this phase, the project should have established a clearly defined analytical perimeter and a coherent technology landscape (see Figure 2). The following subsections describe each of these steps in detail, outlining how they are implemented.

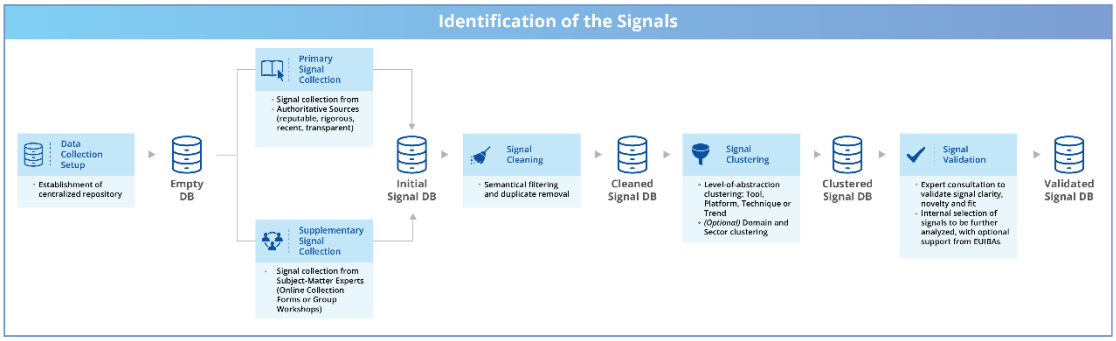


Figure 2 Detailed representation of the methodological steps of the signals' identification

NB: DB = database; EUIBAs = European Union institutions, bodies and agencies.

2.2.1 Data Collection Set-up

Establishing a structured data collection set-up is essential to ensure consistency, traceability and quality assurance in the identification of signals. This process begins with the creation of a

centralised signal input repository, which may take the form of a structured spreadsheet or a collaborative database environment, depending on available resources and team preferences.

To enable systematic documentation and validation, each signal entry should include a minimum set of metadata fields, including:

- **signal name;**
- **short description;**
- **technology readiness level (TRL),** either specified in the source or derived through best-available estimation;
- **current adoption level**, derived through best-available estimation, according to Rogers' diffusion of innovation theory (innovators, early adopters, early majority, late majority, laggards);
- **type of source**, for example market report, policy paper, white paper, expert interview;
- **title of document / name of interviewed expert;**
- **publication date / interview date;**
- **author / publishing organisation / expert's affiliation;**
- **domain,** if specified in the source;
- **sector,** if specified in the source.

This set-up ensures that all collected signals are well documented and ready for subsequent processing, such as filtering, clustering and integration into the radar's analytical framework.

2.2.1.1 Primary Signal Collection

Unlike structured statistical exercises, the signal collection process does not follow a strict mathematical or rigid procedure, as reports on emerging technologies are typically published on an ad hoc basis and rarely provide uniform coverage across all specific technological applications. Consequently, it is not feasible to define a definitive, exhaustive and fully reproducible source list.

Instead, the methodology adopts a principle-based approach, relying on inputs from **authoritative sources**. The selection of sources is guided by the need to ensure the quality, strategic relevance and credibility of the signals identified. In particular, the goal is to source content from globally recognised entities that are well positioned to detect, assess or comment on technological innovation trends relevant to cybersecurity. To guide source selection, the following key criteria are applied.

- **Reputation and impartiality.** The entity producing the report should be broadly recognised for its subject-matter expertise and independence. The entity should be one commonly cited in policymaking and in the development of enterprise-level strategies.
- **Methodological rigour.** Reports should demonstrate the use of robust analytical or empirical methods.
- **Recency.** Only reports published within the last one to two years should be considered, to ensure signals reflect the current state of innovation.
- **Transparency.** The source should be clear about the data or evidence base used to generate its findings or forecasts.

These criteria were selected based on established and published references in foresight and evidence appraisal (e.g. the UN Environment Programme's 2021 planetary action annual

report ([1]); the European Commission's 2020 strategic foresight report ([2]); the Organisation for Economic Co-operation and Development's (OECD) strategic foresight toolkit ([3])), which consistently highlight credibility, trustworthiness, transparency, methodological rigour and timeliness as key attributes of authoritative sources for this type of exercise.

Table 1 provides an overview of the main archetypes of entities whose outputs are considered suitable for primary signal collection. For each type, examples are provided alongside a justification of their relevance to the radar's objectives. A suggested list of authoritative sources is also presented in **Annex 3**.

Table 1 Examples of data sources for the primary signal collection

TYPE OF SOURCE	EXAMPLES	REASON FOR NEED
Market analysts and consultancies	Gartner, International Data Corporation, Forrester, McKinsey, Boston Consulting Group	Provide insights on technology market trends, adoption forecasts, competitive dynamics and vendor landscapes; help identify which technologies are commercially viable and gaining traction.
International organisations and standards bodies	OECD, International Telecommunication Union, International Organization for Standardization, World Economic Forum (WEF), ENISA	Offer global policy perspectives, standardisation roadmaps and regulatory context that shape adoption readiness and compliance fit.
Universities and research centres	University of Oxford, Harvard University, Fraunhofer Society, Massachusetts Institute of Technology (MIT), Joint Research Centre (JRC)	Deliver rigorous academic studies, technical assessments and early-stage foresight analyses on emerging or disruptive technologies.
Industry associations, information-sharing and analysis centres and technical alliances	European Telecommunications Standards Institute (ETSI), Institute of Electrical and Electronics Engineers, Cloud Security Alliance, European Cyber Security Organisation (ECSO)	Issue white papers, best practice guides and frameworks that track developments within specific sectors or technologies, often bridging industry and regulation.
Regulatory and legal institutions	Commission reports, national cybersecurity agencies, ENISA	Provide guidance on current and upcoming regulations, certification schemes and compliance obligations critical to assessing regulatory alignment.
Investment banks and venture funds	Goldman Sachs, JP Morgan, PitchBook, Atomico, CB Insights	Offer data on funding flows, start-up ecosystems and investment theses that indicate where capital is driving technological growth and innovation hotspots.
Think tanks and policy institutes	RAND Corporation, Chatham House, Carnegie Endowment for International Peace, European Policy Centre	Provide strategic scenarios, geopolitical assessments and long-range policy analyses that enrich foresight and risk context.
Tech news outlets and trade publications	Wired, The Register, TechCrunch, Dark Reading	Highlight the most recent developments, emerging applications and shifts in market sentiment that may not yet appear in formal studies, offering early signals of change.
Technology companies and integrators	IBM (International Business Machines), Cisco, Microsoft, Palo Alto Networks	Publish security landscape reports, technical white papers and deployment roadmaps grounded in direct operational data and global client experience.

These sources are typically heterogeneous in both format and language, ranging from structured technology landscape analyses to high-level executive outlooks. As a result, processing them requires either manual review to preserve nuance and ensure proper contextual interpretation or

([1]) United Nations Environment Programme, 'UNEP in 2021: Planetary action: Climate, nature, chemicals & pollution', 2022, https://wedocs.unep.org/handle/20.500.11822/37946.
([2]) European Commission, '2020 strategic foresight report', European Commission website, https://commission.europa.eu/strategy-and-policy/strategic-foresight/2020-strategic-foresight-report_en.
([3]) OECD, *Strategic Foresight Toolkit for Resilient Public Policy: A comprehensive foresight methodology to support sustainable and future-ready public policy*, OECD Publishing, Paris, 2025, https://doi.org/10.1787/bcdd9304-en.

the use of advanced analytical tools capable of extracting meaning from unstructured data (e.g. an approved machine learning or AI-based engine, appropriately trained ([4])).

In either case, the task should be conducted by a team of trained analysts or domain experts who carefully examine the full content of the selected documents. Given the inherently qualitative nature of this work, expert judgement and discretion are indispensable to the process, ensuring a robust human-in-the-loop approach to interpreting and consolidating the signals.

2.2.1.2 Supplementary Signal Collection

This step consists of the structured elicitation of signals from subject-matter experts, building on participatory foresight methods widely used across EUIBAs. Expert input offers a valuable complement to a literature-based collection by surfacing emerging developments that may not yet be formally documented but are known within practitioner or research communities.

To ensure feasibility in terms of time and resource consumption, this phase should preferably be conducted online or in a hybrid context. Two formats are envisioned.

- **Online collection forms.** Experts provide individual inputs via a structured submission form such as EU Survey ([5]). This method allows for asynchronous participation and can reach a broad range of contributors without placing limits on the number of responses.
- **Online group workshops.** Experts are engaged through real-time, facilitated breakout discussions. This format enables collective sense-making and allows for clarification and debate. To ensure productive engagement, each breakout group should be limited to approximately 10–20 participants.

In both cases, the composition of the expert pool is critical. One possible approach would be to establish a dedicated ad hoc working group (AHWG). The membership of the AHWG will be composed of up to 30 leading experts selected through an open call, based on the requirements and competencies outlined. These members will bring together a balanced mix of expertise relevant to the radar. In forming the group, ENISA will consider a range of factors to ensure a representative and effective composition. This includes geographical diversity, gender balance and a well-rounded representation of key stakeholder groups. These stakeholders span both the supply side, such as technology vendors, integrators and service operators, and the demand side, including end users, critical infrastructure and public entities. Stakeholders from the conformity assessment community (including conformity assessment bodies-CABs, auditors, certification bodies and testing laboratories) and academic experts with deep knowledge of network and information security will also be considered. Alternatively, ENISA could adopt a more flexible, ad hoc approach by engaging specific stakeholder categories through targeted surveys rather than broader, generic consultations.

Before participating, experts should receive a guidance document outlining the objectives, scope and process of the signal collection exercise. Whether via an online form or interactive session, the activity should be structured around a guided foresight prompt that invites experts to identify technological applications or innovations they consider novel, emerging or strategically significant for the near-term future of cybersecurity. This prompt is designed to elicit candidate signals

([4]) Comparable tools are already being piloted within other EUIBAs, for example GPT@JRC, which is currently being tested as a full-scale pilot project under the Commission's ICT governance framework.
([5]) See, for example, the open public consultations implemented with EU Survey and the Better Regulation Portal.

grounded in real-world use cases, field experience or horizon scanning that experts may have conducted within their own organisations.

The output of this process is captured in raw form, using the same structured template introduced in Section 2.1.1. At this stage, no formal cleaning or filtering is applied: ambiguous, duplicate or inconsistent entries are retained as submitted, to be systematically addressed during the dedicated consolidation phase.

While inherently qualitative and subjective, this method offers unique value by surfacing practice-based signals that may not yet appear in published data sources. It also supports the identification of context-specific innovations, for instance those shaped by particular sectors, jurisdictions or regulatory priorities, which often remain underrepresented in more structured scanning approaches. Finally, the participatory nature of the process contributes to the credibility and ownership of the results, reflecting the perspectives of professionals embedded in the cybersecurity innovation ecosystem.

NB: The rationale above does not challenge the governance proposal presented in Annex 2 with the layers. It is possible that some members of the AHWG can be part of the operational management layer and of the expert and validation layer.

2.2.2 Signal Cleaning

Once candidate signals have been collected, they undergo a data cleaning and consolidation process. The primary objective of this step is to harmonise the dataset, eliminate redundancies, resolve ambiguities and prepare the signals for classification and subsequent comparative analysis.

The cleaning process, to be conducted either manually or supported by text analysis tools (e.g., natural language processing or machine learning engines), begins with a comprehensive review of all entries in the central repository. Duplicate or overlapping signals are identified and consolidated. These may include semantically identical or near-identical applications expressed using different wording across sources (e.g., ‘zero trust security’ and ‘zero trust architecture’) or recurring concepts drawn from multiple documents.

Where variations are minor and conceptually aligned, the signal is rewritten into a single, harmonised formulation. In cases where differences in terminology reflect distinct scopes, technical layers or contextual uses, the entries may be retained as separate but linked signals and flagged for domain-specific validation in the following clustering stage.

During this process, any vendor-specific signals (e.g., ‘Vendor X’s threat intel platform’) are excluded, unless they can be generalised into a widely adopted class of technology (e.g., threat intel platform).

2.2.3 Signal Clustering

Following the cleaning phase, the consolidated signal set undergoes a structured and multi-dimensional clustering process aimed at grouping signals under a coherent set of thematic categories. This clustering operates on two levels: the first and compulsory level focuses on the level of abstraction (e.g., trends, techniques, tools or platforms), while the second, optional level, organises signals by elements such as domain or sector. This dual approach enhances the interpretability of the data and facilitates communication with stakeholders by aligning emerging technological applications with familiar domains of cybersecurity policy and practice.

2.2.3.1 Level of Abstraction Clustering

To ensure comparability and avoid inconsistencies, a compulsory clustering criterion is introduced: the **level of abstraction**. This ensures that signals of different conceptual depth are not compared or evaluated on unequal terms. In practice, signals related to emerging cybersecurity developments may span a broad abstraction spectrum: from strategic approaches to specific technical solutions. To maintain analytical clarity and support systematic monitoring, this methodology adopts a four-tier taxonomy that distinguishes among the following:

- **Tools.** Concrete software products or utilities that implement or automate specific tasks within the development and operations life cycle (e.g., a network protocol analyser).
- **Platforms.** Foundational ecosystems or run-time environments that provide infrastructure, services and integration capabilities for building, deploying and scaling applications (e.g., security orchestration, automation and response).
- **Techniques.** Systematic methods, patterns or approaches used to design, test and evolve software systems (e.g., post-quantum cryptography).
- **Trends.** Emerging shifts in cybersecurity paradigms, frameworks or ecosystem practices that influence how technologies are applied (e.g., zero trust architecture).

To facilitate accurate attribution, analysts are instructed to apply the decision tree described in Figure 3.

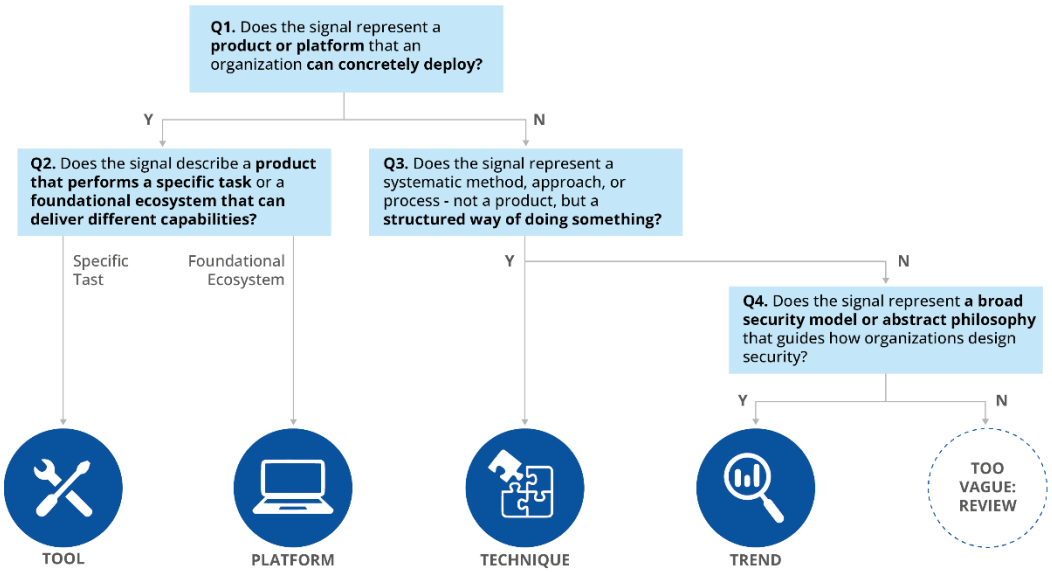


Figure 3 Decision tree for level of abstraction signal clustering

Ambiguous or excessively broad signals (e.g., 'AI in cybersecurity') need to be re-expressed with greater precision and detail (e.g., 'machine learning for behavioural threat detection') to ensure they fit within the intended scope and can be meaningfully assessed.

The level-of-abstraction clustering is considered compulsory as it directly informs the structure and interpretability of the radar's main visualisation (see Section 2.5). However, additional clustering categories can be applied in parallel to support more detailed analysis and tailor outputs to specific stakeholder needs. As an example, a signal can be clustered by domain or by sectoral relevance. These secondary lenses are valuable for tailoring visualisations and analyses to specific user groups but must always be applied in addition to, not in place of, the abstraction-based clustering. It is clear that the clustering ambiguity will need to be addressed on a case-by-case basis.

2.2.3.2 Domain/Sector Clustering

The specific labels to be used for this exercise (e.g., the list of potential domains for domain clustering or sectors for sector clustering) could reference different frameworks or standards. For a first run of the radar, it is suggested to start with the domain and sector labels defined in the JRC Cybersecurity Taxonomy published by the Commission in 2022 ([6]). While other established standards/projects, such as those developed by ECSO ([7]) or the National Institute of Standards and Technology (NIST) ([8]), may alternatively be used, to ensure consistency across editions and support longitudinal analysis, it is strongly recommended to select one clustering standard at the outset and apply it consistently over time, introducing changes only when clearly justified.

2.2.4 First Signal Validation and Selection

Once signals have been cleaned and clustered, a validation step is required to ensure the quality, clarity and novelty of the resulting list before proceeding to the evaluation phase.

The preferred approach for this validation is a structured expert consultation. The expert panel should be established through a transparent and systematic selection process, which could align with the AHWG, as previously outlined in Section 2.2.1.2. In any case, where feasible, it is advisable that the same group of experts involved in the initial collection phase (or a subset thereof) should also participate in this validation exercise to maintain continuity and context.

Experts are invited to review each signal and assess it against a defined set of criteria, including:

- **clarity and precision of formulation;**
- **novelty and degree of innovation;**
- **fit with the abstraction levels and clustering taxonomy.**

Based on their assessment, experts may be asked to propose revisions (e.g., clearer wording), flag redundancies or recommend the removal of items that are outdated or insufficiently distinct. Special attention should be given to signals previously flagged as ambiguous or borderline cases during the cleaning and clustering phases.

The validation process may be carried out in different formats, depending on resource and time availability, including:

- **a facilitated workshop (online or in person);**

([6]) European Commission, 'JRC Cybersecurity Taxonomy', European Commission website, https://cybersecurity-atlas.ec.europa.eu/cybersecurity-taxonomy.
([7]) ECSO, *A Taxonomy for the European Cybersecurity Market – Facilitating the market defragmentation – WG2 – Market deployment, investments, and international collaboration*, ECSO, 2021, https://ecs-org.eu/ecso-uploads/2022/10/605de1e3a768a.pdf.
([8]) NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, NIST, 2018, https://doi.org/10.6028/NIST.CSWP.04162018.

- **a virtual review round with shared documents;**
- **a structured online consultation with form-based feedback.**

The final outcome of this step is a validated and coherent list of emerging technological signals, forming the analytical foundation of the TIR and serving as the entry point for subsequent variable assessment and scoring activities.

In this step, the team and experts also have the opportunity to define the specific focus of the radar, using the clustering categories established in the previous phase. For example, one edition may take a broad view and include cybersecurity signals across all sectors, while another may be tailored to a specific context (e.g., the energy sector). In such cases, only the signals tagged with the corresponding cluster (e.g., 'energy' in the sector clustering) will be selected for further evaluation.

As the final part of this initial validation step, the ENISA working team defines the focus domains of the radar, selecting the signals to be further analysed in the following phases based on ENISA priorities (e.g., whether to pursue a general-purpose, sector-specific or domain-specific analysis). Upon the decision of the strategic oversight entities (e.g., the ENISA Management Board or management team), a consultation with the relevant EU entities may be conducted to help define the focus. This consultation would provide an additional layer of institutional review, ensuring that the selected signals are consistent with broader European strategic and policy objectives.

2.3 Qualification of the Signals

Following the identification of the candidate signals, the next operational phase focuses on qualifying the signals by assessing their **strength** and **momentum**. Unlike the first phase, which emphasises manual interpretation of heterogeneous sources, this method leverages structured bibliographic databases and reproducible procedures to ensure coverage, comparability and transparency (despite the importance still played by analysts in interpreting the results).

This assessment is performed in two main steps. First, signals are subjected to a structured evaluation using established and reputable research data sources such as scientific publication databases, patent repositories and news/trend analysis tools (Section 2.3.1).

Next, the preliminary results of this analysis are validated through a dedicated expert workshop (Section 2.3.2). In this step, participants are invited to reflect on the scores produced by data-driven methods, provide contextual interpretation and contribute qualitative insights. This expert dialogue helps refine and finalise the qualification of each signal.

The output of this phase is a finalised list of weak and strong signals to be included in the radar (see Figure 4). This distinction provides the basis for subsequent decisions on how each signal should be represented within the radar. Depending on their strength, different evaluation or visualisation pathways are followed to evaluate signals in the next stages of the methodology.

This phase also introduces the possibility of applying a fast-track process (Section 2.3.3), which enables a more streamlined and accelerated evaluation procedure under specific conditions. The objective of this option is to ensure the timely handling of cases where urgency or resource optimisation is critical, while maintaining consistency with the overall framework.

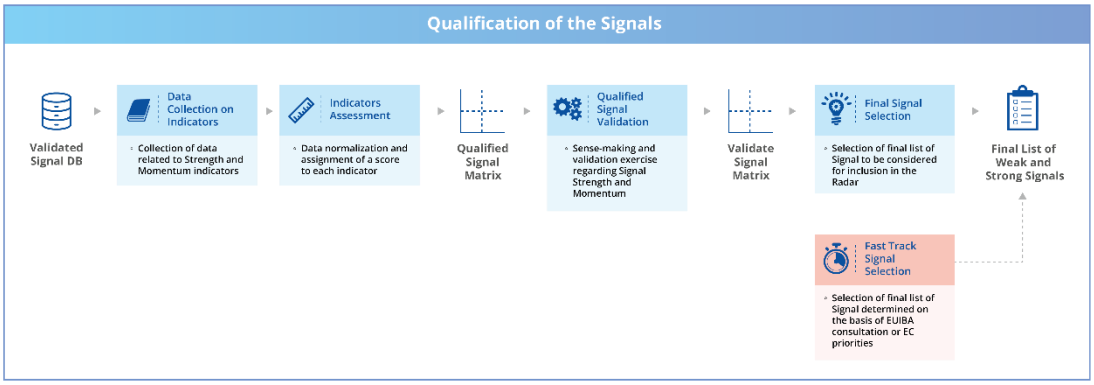


Figure 4 Detailed representation of the methodological steps of the qualification of signals

2.3.1 Signal Monitoring

Once a curated list of signals has been consolidated and validated, a structured monitoring phase is launched to assess their **strength** and **momentum**. These two variables synthesise established practices commonly found across European and international technology monitoring efforts and use a combination of patent/article analysis, more specifically, the following.

- **Strength** refers to the overall maturity and visibility of a technological application within expert, academic and technical ecosystems. It reflects both its development readiness (e.g. TRL) and its recognition across authoritative sources such as strategic reports, policy publications and technical reviews. It is meant to signal how robust and established the technology is from a scientific, technical and expert standpoint.
- **Momentum** refers to the extent to which a technological application is gaining traction in strategic discussions, media or research communities. It is used as a proxy to capture perceived importance or momentum. It serves as a proxy for the perceived momentum or importance of a technology, independent of its current maturity.

The following subsections present a way to operationalise the assessment of these two variables.

2.3.1.1 Introducing Strength and Momentum

To ensure objectivity, we suggest that these two variables be assessed through quantitative indicators derived from trusted data sources. The methodology follows precedent from recent foresight initiatives at the EU level, which emphasise the use of evidence-based signal monitoring over purely qualitative evaluation (see, for example, EIC, 2022[9]; JRC, 2020[10]; OECD, 2023).

Specifically, the indicators proposed for each variable are described in Table 2 below.

[9] EIC Work Programme 2022 - European Innovation Council - European Commission
[10] JRC Statistical Audit of the Global Innovation Index 2020 | Knowledge for policy

Table 2 Indicators used to evaluate signal strength and momentum

INDICATOR	STRENGTH	MOMENTUM
TRL (strength) / current adoption level (momentum)	Estimation of how mature the signal is according to TRL.	Estimate of how adopted the signal is across organisations, according to Rogers' Diffusion of Innovations.
Mentions in authoritative sources	Absolute number (count) of mentions that the signal receives from authoritative sources.	Year-on-year (YoY) change in mentions that the signal receives from authoritative sources.
Academic publications	Absolute number (count) of peer-reviewed scientific articles related to the signal.	YoY change in peer-reviewed scientific articles related to the signal.
Patent filings	Absolute number (count) of inventive activity and intellectual property generation surrounding the signal.	YoY change in inventive activity and intellectual property generation surrounding the signal.
News or search trends	Absolute number (count) of news items mentioning the signal and/or search trends related to the signal.	YoY change in news items mentioning the signal and/or search trends related to the signal.

Importantly, this integration of multiple quantitative sources also enables continuity between phases: for example, TRL scores, adoption estimates and mentions in authoritative sources, already gathered during the initial signal identification phase, are reused as part of the scoring for this step, improving consistency and reducing redundant effort.

2.3.1.2 Collecting the Data

To streamline collection and reduce resource demands, the use of established EU-level data infrastructures to collect the data needed for the indicators is strongly recommended. In particular, TIM analytics ([11]), the automated text and data mining platform developed by the JRC, could represent a robust solution capable of providing the vast majority of the quantitative inputs required for signal qualification in the initial edition of the radar.

TIM analytics aggregates data from multiple relevant sources, which align directly with the indicators selected to measure strength and momentum (see Table 3).

([11]) European Commission, 'TIM analytics', European Commission website, 8 February 2024, https://knowledge4policy.ec.europa.eu/text-mining/topic/tim_analytics_en.

Table 3 Sources from TIM analytics that can be leveraged by the radar

SOURCE	RELATED INDICATOR	DESCRIPTION
Scopus ([12])	Academic publications	Comprehensive coverage of academic journals, preprints, books and conference proceedings including over 25.5 million open-access documents.
PATSTAT ([13])	Patent filings	PATSTAT contains bibliographical and legal event patent data from EU Member States, extracted from the European Patent Office's database.
Europe Media Monitor (EMM) ([14])	News items or search trends	The EMM software analyses both traditional and social media. EMM gathers about 300 000 news articles per day in up to 70 languages.

A critical enabler of this process is the construction of accurate, specific and standardised keyword sets for each signal. These keyword sets must reliably capture the technological application and its common variants or synonyms to ensure high-quality data retrieval.

To support this step, analysts are encouraged to use the signal name and short description already collected during the identification phase as a foundation for keyword construction.

For example, if the identified signal is 'XDR (extended detection and response), and its description refers to 'advanced, integrated cybersecurity platforms for endpoint and network detection', a preliminary set of keywords might include:

- **'XDR'**
- **'Extended Detection and Response'.**

Boolean logic is applied to structure the queries in a precise way. For example, a Scopus search might use the following query string, adding the year of reference of the radar and the previous one (for the YoY calculation):

TITLE-ABS-KEY (('Extended Detection and Response' OR 'XDR') AND PUBYEAR = 2025)

However, the quality and reliability of this step depend heavily on the consistency of keyword usage across analysts and over time. To ensure reproducibility and traceability, the selection of keywords should not rely solely on the discretion of individual analysts. Instead, a dictionary search approach could be implemented as a preliminary step.

This would involve the construction of a controlled keyword dictionary, which could be initially created and expanded using generative AI tools and embedding-based methods. Once validated, preferably by the ENISA Core Radar Team, the dictionary would be frozen for the current edition of the radar, and all queries should be generated directly from it. The dictionary and query formulation can be periodically reviewed and updated as part of a controlled versioning process, but any future modification to the dictionary should be justified, documented and revalidated, since such changes may affect the resulting scores and are essential for maintaining traceability and comparability over time.

([12]) https://www.scopus.com/pages/preview.
([13]) https://www.epo.org/en/searching-for-patents/business/patstat.
([14]) European Commission, 'Europe Media Monitor (EMM)', Knowledge for policy website, 23 May 2018, https://knowledge4policy.ec.europa.eu/online-resource/europe-media-monitor-emm_en.

An example of a dictionary-based query could be:

TITLE-ABS-KEY ((‘Extended Detection and Response’ OR ‘XDR’ OR ‘Advanced threat detection platform’ OR ‘Integrated threat detection and response’) AND PUBYEAR = 2025)

The analyst then extracts the absolute values for each indicator and normalises them using the ordinal 1–5 scale described earlier. These normalised values are combined to generate composite scores for each signal along the two dimensions of interest. The output of this process is a preliminary qualification of each signal, expressed as a score on both strength and momentum axes. These scores are then fed into the expert workshop described in the next step, where they are reviewed, contextualised, and, if needed, adjusted.

Although Scopus, PATSTAT and the EMM represent the primary recommended data sources for the first edition of the radar, alternative databases and platforms may be integrated into future iterations. In particular, sources such as the ‘Cooperating real-time sentient objects: architecture and experimental’ evaluation and the Community Research and Development Information Service, the latter already available within the TIM analytics infrastructure, can be monitored from the outset, even if not immediately relevant to the selected indicators. Doing so allows for early data collection that may support future analytical needs, aid in the validation of expert judgement or help identify significant discrepancies between data-driven insights and observed developments in the cybersecurity landscape.

Table 4 Example of normalised values for signal strength

	SCORE 1	SCORE 2	SCORE 3	SCORE 4	SCORE 5
TRL	Estimated TRL 1–2, experimental stage with basic research.	Estimated TRL 3–4, prototype development with early validation.	Estimated TRL 5–6, technology validated in tests.	Estimated TRL 7–8, technology ready for full validation.	Estimated TRL 9, mature technology with proven performance.
Mentions in authoritative sources	Values in the bottom 20th percentile of the dataset.	Between 21st and 40th percentile.	Between 41st and 60th percentile.	Between 61st and 80th percentile.	Above 80th percentile.
Academic publications	Values in the bottom 20th percentile of the dataset.	Between 21st and 40th percentile.	Between 41st and 60th percentile.	Between 61st and 80th percentile.	Above 80th percentile.
Patent filings	Values in the bottom 20th percentile of the dataset.	Between 21st and 40th percentile.	Between 41st and 60th percentile.	Between 61st and 80th percentile.	Above 80th percentile.
News items or search trends	Values in the bottom 20th percentile of the dataset.	Between 21st and 40th percentile.	Between 41st and 60th percentile.	Between 61st and 80th percentile.	Above 80th percentile.

On the other hand, momentum seeks to understand whether a given signal is gaining traction, holding steady or losing relevance across scientific, policy and public discourse. To evaluate this,

the approach leverages a set of YoY indicators. Say a yearly timeframe is suggested, as it is a reasonable span for both the work of the analysts and the speed of tech evolution. These indicators provide insight into whether attention towards a given signal is accelerating, stagnating or declining.

Because these values are expressed in percentages, they require normalisation to fit the ordinal scoring system for the other axis of the matrix. This is achieved by defining thresholds that reflect the magnitude and direction of change. For example, a significant increase, such as a YoY growth above 20 % in patent filings or scientific articles, would correspond to the highest score, signalling strong upward momentum. Steady growth (e.g., between 10 % and 20 %) would be scored as 4. Signals indicating a moderate change in attention (greater than 5 % but less than 10 %) receive a neutral score of 3, while those showing a small change (greater than 0 % but less than 5 %) a score of 2. Finally, signals exhibiting negative growth would be assigned the lowest score of 1. This method allows for consistent comparability across signals, while still being sensitive to early signs of acceleration or decline. A recap of how momentum indicators could be normalised to an ordinal scoring scale is proposed in Table 5.

Table 5 Example of normalised values for signal momentum

	SCORE 1	SCORE 2	SCORE 3	SCORE 4	SCORE 5
Current adoption level	Innovators	Early adopters	Early majority	Late majority	Laggards
Mentions in authoritative sources	≤0 % YoY change	0 to 5 % YoY change	6 % to 10 % YoY change	11 % to 20 % YoY change	≥20 % YoY change
Academic publications	≤0 % YoY change	0 to 5 % YoY change	6 % to 10 % YoY change	11 % to 20 % YoY change	≥20 % YoY change
Patent filings	≤0 % YoY change	0 to 5 % YoY change	6 % to 10 % YoY change	11 % to 20 % YoY change	≥20 % YoY change
News items or search trends	≤0 % YoY change	0 to 5 % YoY change	6 % to 10 % YoY change	11 % to 20 % YoY change	≥20 % YoY change

As a final result, strength and momentum can be calculated as composite scores based on the formulas below.

Strength = (0.50 × TRL score) + (0.125 × authoritative mentions score) + (0.125 × academic publications score) + (0.125 × patents score) + (0.125 × news/trends mention score)

Momentum = (0.5 × current adoption level score) + (0.125 × authoritative mentions YoY score) (0.125 × academic publications YoY score) + (0.125 × patents YoY score) + (0.125 × news/trends mention YoY score)

The rationale behind the first formula is that TRL and current adoption level are well-established and standardised measures of how mature a technology is, especially in public-sector and EU-funded innovation frameworks. They directly reflect how close a given signal is to market deployment or operational use. Given their central role in evaluating implementation feasibility, we

assign them half the total weight (50 %), making them the anchor metric for the two dimensions. As for the four additional indicators, they complement TRL and current adoption level by tracking how a signal is performing in different contexts – industry, scientific, R & D, media and user. These are all important, but individually they are less directly correlated with actual technical deployability and rush to adopt. As such, they are given equal and smaller weights (12.5 %), together composing the remaining 50 %.

As for the second formula, this aims to capture velocity rather than volume: how quickly a signal is gaining attention and investment across multiple fronts. Since each of the four indicators tracks a different kind of momentum, they are treated as equally important components of the overall trend. Assigning equal weights (25 %) reflects a balanced view of market dynamics and avoids overemphasising any one dimension.

Once composite scores for strength and momentum have been calculated, each signal is plotted on a two-dimensional matrix, with strength on the X-axis and momentum on the Y-axis (see Figure 5). This positioning allows for a comparative evaluation of the signals' current maturity and perceived trajectory. Based on their relative placement, signals are grouped into four macro-categories, each reflecting a distinct development profile.

- **Emerging signals (low strength, high momentum).** Signals that are gaining visibility and traction but are not yet technically mature. These may represent promising developments still in early stages of technological readiness.
- **Early signals (low strength, low momentum).** Signals that remain weak on both axes. These may be speculative, overhyped or still too immature to warrant immediate strategic attention but could evolve over time.
- **Latent signals (high strength, low momentum).** Signals that are technically solid but have not yet achieved broad attention or uptake. These may benefit from targeted policy or market interventions to unlock their value.
- **Leading signals (high strength, high momentum).** Signals that are both mature and gaining widespread traction. These typically represent high-priority areas for strategic monitoring, investment or adoption.

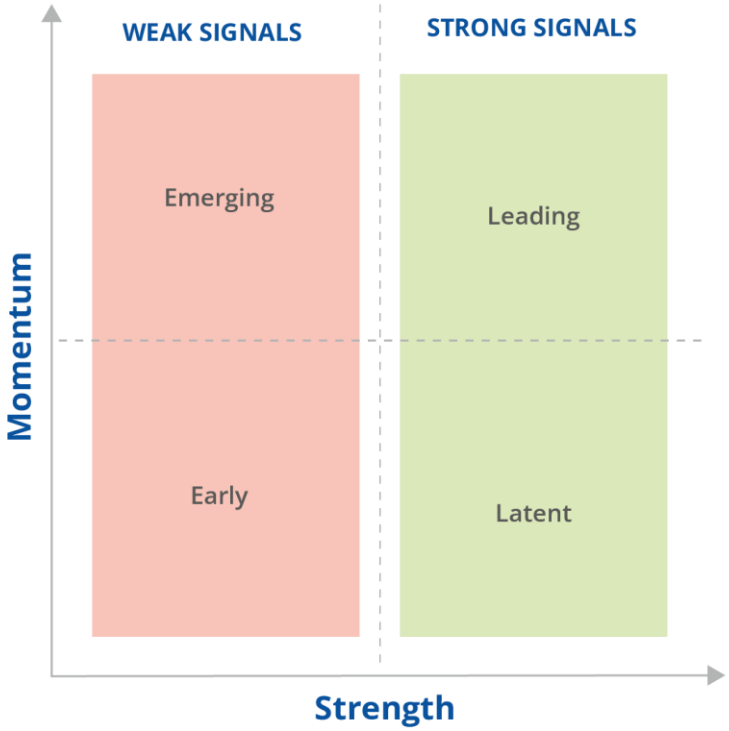


Figure 5 Visualisation of the strength/momentum matrix

The assessment methodology and calculation formulas proposed in this section are intended to serve as a structured reference for the first edition of the TIR. While no single standard exists for foresight exercises of this kind, and future iterations may warrant adjustments to indicators, scoring thresholds or weighting models, these should not be altered arbitrarily. Unless substantive feedback is received or context-specific requirements emerge, methodological stability should be preserved across editions. This continuity will enhance the comparability of results over time and enable the progressive development of a consistent and robust longitudinal dataset underpinning the radar.

2.3.2 Final Signal Validation and Selection

The second and final step in the qualification of signals involves an expert sense-making and validation process. This phase plays a critical role in ensuring that the most strategically relevant and technologically credible signals are ultimately selected for inclusion in the TIR.

To ensure objectivity and avoid self-referential bias, this workshop should ideally involve a new group of experts, distinct from those consulted during the initial validation phase. For example, the ENISA Advisory Group could play this role.

To guide this process, a double-diamond methodology may be used. This approach allows the group to first diverge, exploring a broad range of views and perspectives on the signals, and then

converge, reaching consensus on the most relevant and actionable entries. This method supports both creative exploration and structured decision-making, enabling a rigorous yet inclusive form of validation.

The process begins by inviting each participant to submit a curated list of three to five technological signals they believe merit close monitoring. For each submitted signal, experts are also asked to provide a preliminary evaluation of its strength and momentum, based on their individual expertise and access to relevant information. To ensure consistency between the overall methodology and the experts' assessments, clear guidelines and criteria defining these two indicators will be provided in advance. Once collected, all inputs are aggregated into a central repository, forming the basis for the subsequent sense-making and validation exercises.

Following the initial expert input, workshop facilitators present the draft qualification matrix developed during the preceding monitoring phase. This matrix is presented with a transparent overview of how each signal was assessed in terms of strength and momentum, based on the underlying quantitative indicators. The expert-submitted signals are then systematically compared against the matrix to identify consistencies, discrepancies and potential gaps.

If new signals are introduced during this process, they are treated as 'wild cards'. These are not integrated into the current edition of the radar but will be carefully documented and carried forward into the feedback and iteration cycle of signal evaluation for future consideration.

A structured sense-making discussion follows, enabling participants to collectively interpret the preliminary scores, assess their alignment with real-world technological and market trends, and adjust them where appropriate. At this stage, potential areas for indicator weight fine-tuning may also be highlighted and considered for implementation in future editions to ensure coherence between the analytical model and expert judgement.

However, such adjustments should be considered only when they are the following.

1. Clearly justified and necessary to improve validity.

2. Approved by the majority of participants: this step ensures not only validation of the scoring framework, but also contextual interpretation of outliers and potential refinements to signal definitions or clustering. At the end of this phase, a critical decision must be taken regarding which signals advance to the formal data collection process and, ultimately, are reported in the yearly iteration of the radar. This step requires careful consideration, as it defines the scope of the signals to be publicly showcased. Depending on the governance structure established for the radar (e.g., whether an AHWG, a dedicated expert task force or an internal coordination team is in place), the responsibility for this selection may rest with a different group than the ones involved in earlier validation activities. It is recommended that the ENISA Management Board lead this decision, to ensure strategic alignment, a clear division of roles and to preserve both methodological rigour and institutional accountability across phases.

The final output of this process is a validated and prioritised set of signals, each qualified across the two dimensions.

2.3.3 Fast Track Signal Selection

In certain cases, it may be necessary to accelerate the assessment of specific technological signals, particularly when these are identified as strategically relevant on the basis of the

consultation with EUIBAs and possible Commission priorities. In such instances, a fast-track procedure may be initiated to ensure timely analysis and alignment with emerging policy or strategic needs. This approach allows the signal to bypass the regular identification and qualification stages defined in the standard methodology and proceed directly to the evaluation phase.

However, this acceleration comes with a trade-off. Skipping the additional stages of collection, validation and qualification means that the analytical depth is reduced. The signal will not benefit from the same degree of contextual analysis, benchmarking against other technologies or supporting evidence. Consequently, while fast-track assessments provide quick and targeted insights, they lack the comparability and comprehensiveness of the standard workflow.

In addition, this implies that, at a minimum, the entity requesting the fast track must provide key baseline information, including an estimate of the signal's strength and its level of abstraction clustering (e.g. whether the object(s) of analysis is a trend, technique, tool or platform). Additional contextual data, such as the sector and domain of application, should also be supplied when relevant, depending on the specific purpose and scope of the fast-track request.

The fast track should therefore be used selectively and clearly marked in the final reporting outputs to distinguish it from signals that have gone through the full methodological pipeline.

The fast-track mechanism should follow a structured yet streamlined procedure designed to ensure methodological consistency while accommodating urgent analytical needs. The process begins with a **trigger or request** justified by a condition of strategic relevance or urgent need. Upon activation, the **requesting entity** provides **a baseline dataset** containing a minimum set of information on the signal, including its name and description, an estimated TRL and current adoption level, its level of abstraction and its sectoral and domain pertinence. Following this submission, the **core team** conducts **an initial screening** to verify the absence of duplication with existing signals, assess the coherence of the proposal with the current taxonomy and analytical scope, and confirm that the data meet the minimum quality threshold. The outcome of this step determines whether the signal is deemed eligible for fast-track processing.

If eligible, the signal then undergoes a **rapid expert validation**, completed within approximately 10 days. This stage relies on a **micro-panel** of three to five experts, drawn from the AHWG or the broader advisory pool, who participate either through a short EU Survey consultation or a focused one-hour virtual session. Experts provide quantitative estimates of the signal's strength and momentum (on a 1–5 scale) and qualitative comments regarding its strategic impact. Their inputs are consolidated to derive average scores and a short analytical profile. Once validated, the signal is integrated directly into the radar pipeline, advancing to the evaluation phase without undergoing the full identification and qualification process. To ensure transparency, fast-track signals are explicitly marked with a distinct visual label (Fast-track) and incorporated into the public dashboard, where they remain subject to full validation during the next regular update cycle.

2.4 Evaluation of the signals

The third phase of the methodology focuses on evaluating the qualified signals against a broad set of adoption-related variables. This evaluation is divided into two distinct but parallel streams, depending on the strength of the signal as identified in the preceding qualification step: one path for weak signals and another for strong signals (see Figure 6).

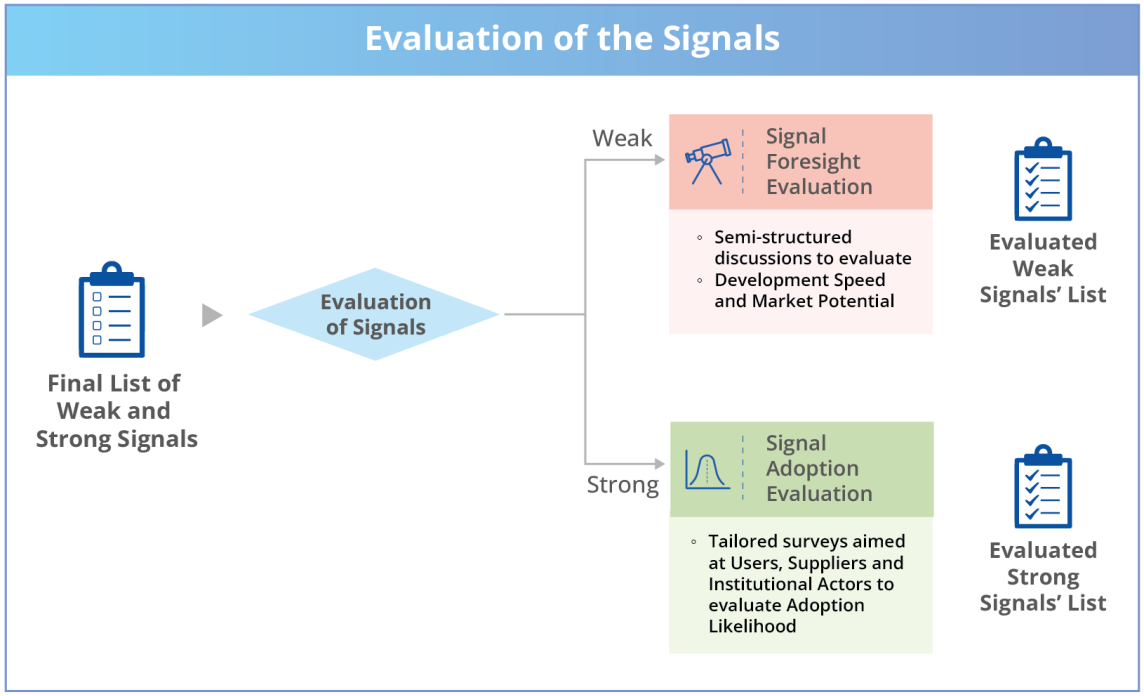


Figure 6 Detailed representation of the methodological steps of the evaluation of the signals

Weak signals play a valuable role in shaping the foresight landscape and informing future iterations of the radar. These signals are thus assessed through the involvement of foresight experts with the goal of estimating their future development speed and market potential (Section 2.4.1). This enables early monitoring and horizon scanning, helping stakeholders remain alert to early-stage developments that may later evolve into disruptive trends.

In parallel, strong signals are evaluated through established models of technology adoption (Section 2.4.2). The framework, adapted from the Unified Theory of Acceptance and Use of Technology (UTAUT[15]), is extended to include the perspectives not only of end users, but also technology suppliers and institutional stakeholders (e.g., regulators, standards bodies). This multi-stakeholder approach ensures a more representative understanding of each signal's adoption readiness across the European cybersecurity ecosystem.

The following subsections describe in detail the respective methodologies and tools used for assessing weak and strong signals.

2.4.1 Weak Signal Assessment

The assessment of weak signals is designed to capture early insights into technologies that, while currently underdeveloped or lacking in visibility, may possess disruptive potential in the medium-to-long term. These signals do not feature in the main radar visualisation but contribute

[15] Unified theory of acceptance and use of technology - Information Systems Theories

significantly to the foresight ecosystem by enabling long-range monitoring and preparatory analysis.

This step is carried out through semi-structured interviews with a panel of foresight experts, ideally members of the AHWG or the ENISA Advisory Group, conducted either individually or collectively within a workshop. The goal is to position each weak signal along two key dimensions: **development speed** and **market potential**. These two variables allow for an early-stage classification that can guide further monitoring, support strategic anticipation and inform future editions of the radar.

2.4.1.1 Development Speed

The theoretical framework behind development speed is the Technological Innovation Systems (TIS) framework (Markard & Truffer, 2008). The TIS framework is a well-established analytical approach used to understand the dynamics that drive the development, diffusion and use of emerging technologies within a specific socio-technical context. Its core purpose is to identify the structural conditions and functional processes that influence how a technology evolves from early innovation to widespread adoption. In the context of foresight and technology assessment, the TIS framework is particularly valuable because it highlights non-linear, systemic factors, such as actor networks, institutional support, market formation and knowledge development, that shape the trajectory of technological emergence. These dimensions align closely with the strategic foresight goal of understanding not only whether a technology is advancing, but also how and why it may succeed or stagnate depending on the surrounding innovation ecosystem.

More specifically, the TIS framework is structured around a set of seven core functions that capture the key processes necessary for the successful development and diffusion of a technology. These functions help assess the performance of an innovation system and identify potential barriers or enablers. Briefly, they are the following.

- **Knowledge development and diffusion.** This refers to the generation of scientific, technical and practical knowledge about the technology, along with the exchange of that knowledge among actors in the system (e.g., through publications, conferences, collaborations).
- **Entrepreneurial experimentation.** This function captures the activities of start-ups, firms or institutions that experiment with the technology in real-world settings, testing business models, use cases and prototypes.
- **Development of positive externalities.** Captures network effects, spill overs and synergies that emerge as more actors become involved, which in turn reinforce the innovation system (e.g., industry consortia, knowledge sharing platforms).
- **Guidance of the search.** This involves the direction and prioritisation of technological development, often shaped by policy goals, societal needs or strategic visions (e.g., national strategies, regulatory roadmaps).
- **Market formation.** Refers to the creation of early markets, demand signals or procurement mechanisms that incentivise the adoption of the emerging technology, even if it is not yet competitive with incumbents.
- **Resource mobilisation.** Encompasses the allocation and availability of financial, human and infrastructural resources needed to support the innovation process, such as funding schemes, skilled labour or infrastructure.

- **Creation of legitimacy.** Relates to the social acceptance and political support of the technology, including activities that reduce resistance or scepticism and build trust among users, regulators and other stakeholders.

Together, these functions provide a systemic view of how technologies mature within their ecosystems and offer practical guidance for identifying where policy or institutional support may be needed to accelerate their progress.

2.4.1.2 Market Potential

As for the second variable, market potential, this estimates the likely future spread and relevance of the signal across the cybersecurity landscape. It is based on three sub-dimensions.

- **Sector penetration**: whether the signal is likely to remain confined to one specific sector (e.g., finance), expand across two or three sectors or become widely adopted across all sectors.
- **Domain usefulness**: assesses the relevance of the signal across cybersecurity domains. A signal relevant to only one domain receives a lower score than one spanning multiple domains.
- **Type of adopter**: experts consider whether the signal will be relevant only to highly specialised users (e.g., critical infrastructure), to larger institutions (e.g., large enterprises, public authorities) or also to smaller actors (e.g., small and medium-sized enterprises (SMEs), individual users). The broader the relevance, the higher the score.

2.4.1.3 Weak Signal Evaluation

To evaluate the developmental trajectory of weak signals, a semi-structured discussion framework is proposed. The framework is designed to guide expert dialogues around the potential evolution and impact of each weak signal and is divided into two main sections, each targeting a distinct dimension of potential evolution. During these dialogues, participants assess each signal by expressing their opinions on the indicators specified for the two variables. The degree of convergence or divergence among participants' views can then be used to assign indicative values to the framework's indicators, capturing both the diversity and direction of expert opinion. Experts are asked to evaluate the development speed and market potential of each weak signal with a time horizon consistent with the radar's publication cycle (e.g., one year if the radar is updated annually). The goal is to capture realistic short-term expectations about the signal's uptake potential. Moderators play a central role in guiding the discussion and ensuring that all dimensions of each weak signal are explored in a balanced and comparable way. Their task is not to lead participants towards consensus, but to stimulate reflection, clarify assumptions and capture differing viewpoints.

Here are a few example questions that can be used to lead and structure the dialogue around each weak signal.

Section 1: Development speed

1. Knowledge development and diffusion
    a. Is new knowledge or research emerging around this signal?

   b. Is knowledge about this signal increasingly being shared, for example through collaborations, open data or conferences?
2. Entrepreneurial experimentation
   a. Are start-ups, innovators or research teams increasingly experimenting with this signal?
   b. Can you think of any concrete pilots, prototypes or early use cases that stand out?
3. Development of positive externalities
   a. Does this signal connect or create synergies with other technologies or sectors?
   b. Do you see it contributing to broader learning, knowledge sharing or innovation in the cybersecurity ecosystem?
4. Guidance of the search
   a. Have you come across this signal in strategic documents or discussions, for instance in policies, roadmaps, or organisational strategies?
   b. Do you see active encouragement from key actors such as funders, regulators or standard-setting bodies?
5. Market formation
   a. Do you see any early markets or niche applications forming around this signal?
   b. Do you think there are relevant barriers preventing broader market uptake at this stage?
6. Resource mobilisation
   a. What kinds of financial support do you see available, for instance venture capital, public funding or other investments?
   b. Beyond money, do you think there are enough skills, infrastructure or organisational capabilities to sustain its development?
7. Creation of legitimacy
   a. How do institutional or influential stakeholders (e.g., government agencies, large organisations associations) view this signal?
   b. Do you sense broad acceptance of this signal or is it still something that is viewed with caution or uncertainty?

Following the discussion, moderators are expected to translate the group's insights into a 1–5 scale, reflecting the perceived level of each construct (see Table 6 for a proposed scoring scale). This approach helps capture qualitative judgements in a comparable, structured format while maintaining the depth of the conversation.

Table 6 Suggested scoring table to evaluate development speed.

	SCORE 1	SCORE 2	SCORE 3	SCORE 4	SCORE 5
Knowledge development and diffusion	Little or no new knowledge generated or shared.	Early studies or isolated initiatives, limited diffusion.	Steady research activity, some knowledge exchange.	Broad and coordinated learning, regular collaboration.	Established knowledge base with continual diffusion.

Entrepreneurial experimentation	No visible pilots or experiments.	Small-scale tests.	Exploratory tests.	Tested pilot examples showing real-world use.	Multiple pilots or prototypes underway.
Development of positive externalities	No spill over effects.	Minimal synergies with related areas.	Moderate spill overs enhancing other domains.	Noticeable cross-sector or knowledge benefits.	Strong benefits across ecosystems.
Guidance of the search	No strategic direction or reference to the signal.	Mentioned occasionally, unclear priorities.	Recognised in some strategies or policies.	Clear guidance and targeted initiatives.	Strong, aligned direction from key actors.
Market formation	No visible market or demand.	Early interest, niche applications forming.	Initial product / service and early adopters.	Growing market with limited participants.	Growing market with many participants.
Resource mobilitisation	No funding, skills or infrastructur e available.	Small-scale or short-term resource access.	Basic investment and capability development.	Funding and skill base supporting growth.	Diverse, long-term resource flows and capacity.
Creation of legitimacy	No awareness or resistance dominates.	Early advocacy, mixed perceptions.	Growing recognition and reduced resistance.	Broad acceptance from key stakeholders.	Embedded in norms or policy.

The resulting values are aggregated to compute a composite score with equal weights for each of the constructs. By averaging the scores across these seven areas, each signal receives a total development speed score.

Development speed

$$DS = \frac{1}{7}\sum_{j=1}^{7} X_{ds_j}$$

whereX_{ds_j} = score for construct j (1–7 = knowledge development and diffusion, entrepreneurial experimentation, development of positive externalities, guidance of the search, market formation, resource mobilisation, creation of legitimacy).

Section 2: Market potential

1. Sector penetration
    a. In your view, which sectors or industries are currently showing the most interest or activity related to this signal?
    b. Beyond those initial domains, do you see potential for this signal to expand into new sectors?
2. Domain usefulness

   a. What specific cybersecurity functions could benefit most from this signal?
   b. Could this signal enable new capabilities or change the way certain cybersecurity functions are currently performed?
3. Type of adopter
   a. Who do you think are the most likely early adopters of this signal, for instance specialised organisations, large institutions or a wider user base?
   b. Over time, do you expect adoption to remain concentrated among a few expert users or to spread more broadly to SMEs and the general public?

Similar to the previous case, following the discussion, moderators are required to translate the group's insights into a 1–5 scale (see Table 7 for a proposed scoring scale).

Table 7 Suggested scoring table to evaluate market potential.

	SCORE 1	SCORE 2	SCORE 3	SCORE 4	SCORE 5
Sector penetration	A very specific niche.	A specialised sector.	Two to three sectors.	Broadly cross-sectoral (many sectors).	Ubiquitous (relevant across most sectors).
Domain usefulness ([16])	One to two function only.	Three to four functions.	Five to six functions.	Seven to eight functions.	All (or almost all) core cybersecurity functions.
Type of adopter	Highly specialised actors	Large private or public organisations only.	Large organisations and selected SMEs.	Most SMEs and some individual users.	Widely usable across all adopter types, including the public.

By averaging the scores across these three questions, each signal receives a market potential score, which complements the development speed score from Section 1.

Market potential

$$\mathrm{MP} = \frac{1}{3}\sum_{j=1}^{3} \mathrm{X}_{\mathrm{mp_j}}$$

where: $\mathrm{X}_{\mathrm{mp_j}}$ = score for construct j (1–3 = sector penetration, domain usefulness, type of adopter).

In future iterations of the radar, the weights of the indicators for both development speed and market potential may be adjusted, depending on the feedback received from the first round. This

([16]) The numerical thresholds used here are based on the 15-domain structure of the European Cybersecurity Taxonomy; however, they may need to be adjusted if an alternative domain classification is applied, such as the six categories outlined in the NIST 2.0 framework.

would allow certain variables to be prioritised over others, recognising that not all factors carry the same relevance.

This step concludes by assigning a clear scoring for the two variables associated with each signal, providing a structured summary of the discussion outcomes that can be compared and tracked over time in a dedicated visualisation tool, which is described in the following methodological phase.

2.4.2 Strong Signal Assessment

The evaluation of strong signals requires a methodology more related to 'technology acceptance' than weak signals, as these technologies are expected to populate the main visualisation of the TIR. For this purpose, a structured survey instrument grounded in the UTAUT framework is proposed. The survey is tailored to capture adoption-related perspectives from different types of stakeholders, including technology users, technology providers (suppliers and R & D entities) and institutional actors (such as regulators or standards development organisations). While developed as a distinct instrument, it could be integrated into existing ENISA initiatives, such as the market assessment framework and the NIS survey framework, to ensure coherence and synergy between initiatives.

This assessment enables a comprehensive and multi-perspective analysis of the readiness and likelihood of adoption for each strong signal, based on real-world feedback from the cybersecurity ecosystem.

The evaluation focuses on five core constructs derived from the UTAUT ([17]) model (Venkatesh et al., 2003):

- **performance expectancy**: the degree to which a stakeholder believes that using the signal will help them achieve performance gains;
- **effort expectancy**: the perceived ease of use or implementation of the signal;
- **social influence**: the perceived social pressure or endorsement from influential actors or organisations to use the signal;
- **facilitating conditions**: the availability of resources, infrastructure or regulatory support enabling the use of the signal;
- **behavioural intention**: the stakeholder's expressed willingness to adopt, promote or support the signal.

2.4.2.1 Strong Signal Evaluation

Each construct is operationalised through a set of tailored statements specific to the respondent's stakeholder category. As for the weak signal assessment, respondents will rate each statement on a five-point Likert scale (ranging from 'strongly disagree' to 'strongly agree'), enabling structured and comparable scoring across stakeholder groups.

While the underlying constructs remain consistent, the survey questions are adapted to reflect the context and viewpoint of each stakeholder group. Users are asked to evaluate how a given technology impacts their individual workflows and usability perceptions. Suppliers and R & D entities are asked to evaluate the implementation ease, client demand and strategic intent to

([17]) Technology Acceptance Lab, 'Unified Theory 1 & 2 & Extension (UTAUT)' Technology Acceptance Lab website, https://acceptancelab.com/unified-theory-utaut.

support or scale the technology. Institutional actors (e.g. regulators, standardisation bodies) are asked to assess the feasibility for governance, alignment with policy goals and societal value.

This multi-actor triangulation allows for a more accurate and inclusive picture of how adoption may unfold across the ecosystem.

Performance expectancy

1. Users
    a. 'Using [SIGNAL] helps my organization meet its strategic security objectives.'
    b. '[SIGNAL] makes it easier for the security staff to meet efficiency goals or KPIs.'
    c. '[SIGNAL] makes it easier for the security staff to meet quality goals or KPIs.'
2. Suppliers
    a. 'Our clients achieve measurable security performance improvements when using [SIGNAL].'
    b. '[SIGNAL] adds clear efficiency to our customers' security operations.'
    c. 'Offering [SIGNAL] enhances our company's reputation or competitiveness in the market.'
3. Institutional actors
    a. 'Using [SIGNAL] contributes to better performance or resilience in the overall cybersecurity domain.'
    b. 'Using [SIGNAL] supports achievement of public or institutional policy objectives.'
    c. 'Using [SIGNAL] strengthens the strategic capabilities of the ecosystem we oversee.'

Effort expectancy

1. Users
    a. 'Our existing systems can integrate [SIGNAL] without major technical challenges.'
    b. 'Our staff can learn to use [SIGNAL] with minimal additional training.'
    c. 'Adopting [SIGNAL] would not require extensive changes to our current workflows.'
2. Suppliers
    a. 'We can deploy [SIGNAL] for clients using standard, well-tested processes.'
    b. 'Supporting and maintaining [SIGNAL] for customers requires limited ongoing effort.'
    c. 'Integrating [SIGNAL] into our existing product or service portfolio is technically straightforward.'
3. Institutional actors

a. ‘Current regulatory frameworks can accommodate [SIGNAL] without major revisions.’
b. ‘Clear standards or guidelines exist that make it straightforward to oversee or regulate [SIGNAL].’
c. ‘Monitoring or enforcing compliance for [SIGNAL] would not require disproportionate effort.’

Social influence

1. Users
    a. ‘Competitors in my industry are already adopting or experimenting with [SIGNAL].’
    b. ‘Our key partners or suppliers encourage us to adopt [SIGNAL].’
    c. ‘There is growing recognition within my sector that [SIGNAL] will soon become a standard practice.’
2. Suppliers
    a. ‘We see increasing client demand or inquiries for [SIGNAL].’
    b. ‘Industry associations, consortia, or major clients are promoting [SIGNAL].’
    c. ‘Our competitors are developing or offering similar solutions based on [SIGNAL].’
3. Institutional actors
    a. ‘There are visible government or EU initiatives promoting skills and capacity for [SIGNAL].’
    b. ‘Public opinion or political priorities are creating momentum to regulate or endorse [SIGNAL].’
    c. ‘Stakeholders within our policy domain are actively calling for guidance or standards on [SIGNAL].’

Facilitating conditions

1. Users
    a. ‘My organization has the budget, tools, and infrastructure to implement [SIGNAL].’
    b. ‘Our staff have the knowledge and technical support needed to use [SIGNAL] effectively.’
    c. ‘We can access external expertise or vendor support to deploy and maintain [SIGNAL].’
2. Suppliers
    a. ‘Our organization has the technical infrastructure to deliver and maintain [SIGNAL] for clients.’
    b. ‘We have the training materials, support teams, and documentation ready to assist customers with [SIGNAL].’
    c. ‘We have established partnerships or supply chains that facilitate deployment of [SIGNAL].’
3. Institutional actors

a. ‘Our organization has the expertise required to assess and govern the use of [SIGNAL].’
b. ‘We have adequate resources and capacity to oversee or support the deployment of [SIGNAL].’
c. ‘We can collaborate effectively with other institutions to support the responsible rollout of [SIGNAL].’

Behavioural intention

1. Users
    a. ‘My organization plans to continue/pursue using [SIGNAL] next year.’
    b. ‘We are likely to invest further in [SIGNAL] or similar technologies.’
    c. ‘We consider [SIGNAL] an important part of our future digital or cybersecurity strategy.’
2. Suppliers
    a. ‘My organization plans to continue offering [SIGNAL] as part of our portfolio.’
    b. ‘We intend to promote [SIGNAL] to a wider customer base in the near future.’
    c. ‘We plan to invest in improving or expanding our [SIGNAL]-related capabilities.’

3. Institutional actors
    a. ‘Our organization plans to develop new or updated policies relevant to [SIGNAL].’
    b. ‘We intend to encourage or facilitate wider adoption of [SIGNAL] within our remit.’
    c. ‘We are likely to allocate future resources or initiatives to support [SIGNAL].’

In the survey design, questions should be structured in a matrix format to ensure consistency and comparability across all weak signals. Rather than asking respondents to answer multiple questions for a single signal before moving to the next, each question is posed sequentially for all signals. For example, respondents would first be asked to evaluate their organisation’s position on Question 1 across the full list of signals, and only then proceed to Question 2 and so on. This approach facilitates clearer benchmarking, reduces respondent bias and aligns responses along common dimensions (see Figure 7 for an example representation).

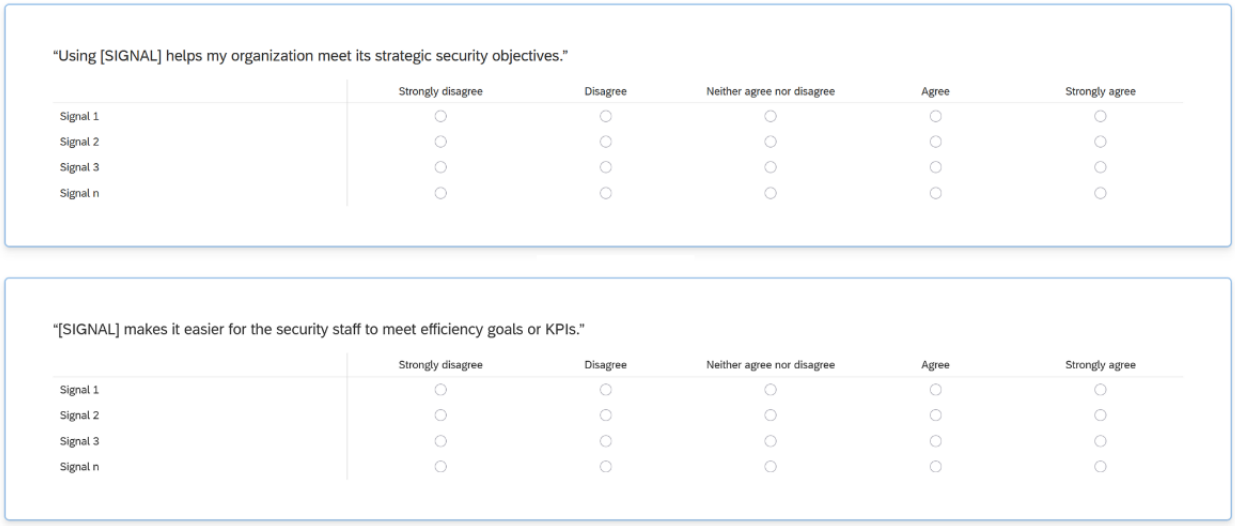


Figure 7 Example representation of the strong signal evaluation survey.

The survey responses are aggregated to compute a composite score with equal weights for each of the five constructs, for each type of respondent. Each of the 15 items contributes equally to the overall score.

User adoption likelihood score

$$ALS_{user} = \frac{1}{15}\sum_{j=1}^{5}\sum_{k=1}^{3} X_{u_{jk}}$$

Supplier adoption likelihood score

$$ALS_{supplier} = \frac{1}{15}\sum_{j=1}^{5}\sum_{k=1}^{3} X_{s_{jk}}$$

Institutional actor adoption likelihood score

$$ALS_{institutional} = \frac{1}{15}\sum_{j=1}^{5}\sum_{k=1}^{3} X_{i_{jk}}$$

where: $X_{x_{jk}}$ = score for stakeholder group x(u = user, s = supplier, i = institutional actor), construct j(1–5 = performance expectancy, effort expectancy, social influence, facilitating conditions, behavioural intention), and item k(1–3).

These are then combined into a single adoption readiness score for each signal, reflecting its perceived maturity and adoption likelihood. This composite score determines the positioning of the strong signal on the radar visualisation.

Overall adoption likelihood score

$$ALS_{overall} = \frac{1}{3}(ALS_{user} + ALS_{supplier} + ALS_{institutional})$$

In future iterations of the radar, weights may need to beadjusted to the evaluation framework, depending on the outcomes of the first round. This would allow certain variables to be prioritised over others, recognising that not all factors carry the same relevance.

Importantly, the scoring mode accommodates different levels of stakeholder input. Where full triangulation is not feasible, partial data (e.g. users only or users and suppliers) may still offer useful insights. However, the ideal case is to collect responses from all three groups to ensure balance and robustness.

This step concludes by assigning a clear overall score for the adoption likelihood associated with each signal, providing a structured summary of the survey results that can be compared and tracked over time in a dedicated visualisation tool, which is described in the following methodological phase.

2.5 Visualisation of the signals

2.5.1 Linking Visualisation Types to Strategic Foresight Purposes

In addition to categorising visualisation types by their structural format, it is essential to assess how each supports different foresight functions. Drawing from ENISA's foresight challenges report, visualisation tools can be aligned with three core strategic intentions:

(a) diagnosis, which focuses on assessing the current state and identifying early signals;
(b) prognosis, which anticipates plausible or probable future developments;
(c) prescription, which informs actionable strategies or policy interventions.

These intentions can further be differentiated by their orientation, either responsive, aimed at mitigating or preparing for foreseeable developments, or normative, aimed at guiding efforts towards a preferred future.

Each visualisation model supports a different mix of these functions. This mapping helps ENISA determine not only which visual tools to use, but also how to sequence and combine them to meet the methodological demands of different use cases.

2.5.2 Mapping Visualisation Types to Foresight Intentions and Orientations

VISUAL TYPE	DIAGNOSIS	PROGNOSIS	PRESCRIPTIVE (RESPONSIVE)	PRESCRIPTIVE (NORMATIVE)
Radar chart	x		x	x
Matrix model	x		x	
Technology cycle		x	x	
Linear index	x		x	x

2.5.3 Visualisation Proposals

While the document outlines the methodological foundations, the **visualisation component** remains a key deliverable of the project. The TIR visualisations are designed to transform analytical results into an intuitive interface for stakeholders. To date, two general visualisation concepts have been developed, but the final deliverable envisages **at least four distinct prototypes**, each tailored to cybersecurity-specific examples (e.g., encryption technologies, threat-intelligence automation). These visualisations will demonstrate how the radar can dynamically present weak and strong signals, show movement across foresight cycles and enable user interaction – an essential element for future operational use.

There are four distinct but complementary visualisations: one focused on strong signals, which serves as the main decision-support tool, and another dedicated to weak signals, which supports foresight and early-stage monitoring (see Figure 8).

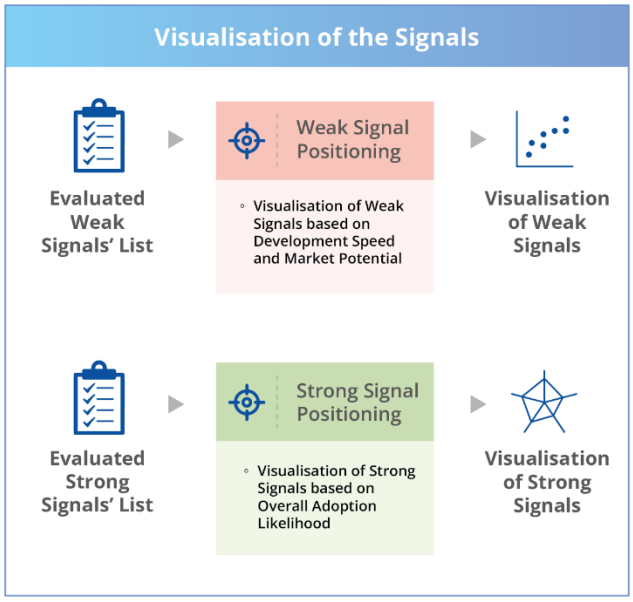


Figure 8 Detailed representation of the methodological steps of the visualisation of the signals.

The weak signal chart (Section 2.5.4) highlights emerging technologies with lower maturity or uncertain relevance but potentially disruptive trajectories, enabling stakeholders to anticipate and track early developments that may shape future cybersecurity landscapes.

In parallel, the strong signal radar (Section 2.5.3) captures technologies with high levels of maturity, presenting them in a structured and comparative way to inform strategic planning, policy and investment.

These two visualisations together ensure that the radar remains both operationally useful in the short term and strategically forward-looking over time.

Over time, other visual formats such as heatmaps, comparative dashboards or multi-dimensional matrices may also be employed to track dynamics or highlight contrasts across technologies. This would be especially beneficial to strengthen the analytical power of the radar, particularly as more data points and feedback are collected across successive editions.

2.5.4 Weak Signal Visualisation

Each weak signal is positioned on a dedicated foresight chart that visualises its innovation potential along two critical axes: development speed and market potential, as explained in Section 2.4.1. The first axis captures the signal's technological development speed and maturity, reflecting how actively the technology is being advanced, studied or prototyped. The second axis reflects the signal's systemic potential, its ability to generate widespread impact across sectors, functions or adopter groups once matured. This two-dimensional positioning helps distinguish between signals that are simply evolving rapidly and those that may reshape the cybersecurity ecosystem more broadly.

This visualisation (see Figure 9) is inspired by the JRC methodology for assessing high-potential innovations ([18]), but has been adapted to focus on market potential rather than internal management or project execution aspects. To capture the different expectations towards weak signals, the following four categories have been created.

- **Transition ready.** These weak signals show both rapid development and growing market potential. They are closest to becoming strong signals, as technological foundations are consolidating and interest across sectors is visibly increasing. While not yet widely adopted, they exhibit momentum and alignment with future market or policy trends. Early policy discussions can help anticipate their impact and integration.
- **Tech consolidation.** These signals demonstrate high development speed but still limited market traction. They are advancing in terms of research, experimentation and ecosystem support, but their commercial or user uptake remains uncertain. With greater visibility or clearer use cases, they could evolve into emerging strong signals.
- **Market consolidation.** These signals show growing market interest despite relatively limited technological development. Early adopters or niche actors are beginning to explore them, indicating that they may soon attract more structured development and support.
- **Exploration.** These represent speculative weak signals, where both technological development and market recognition remain low. They often highlight novel or disruptive ideas with limited current evidence but high exploratory or visionary value. Their future evolution depends on whether development efforts and market attention converge over time.

([18]) For more information regarding the JRC Innovation Radar visualisation, please see https://innovation-radar.ec.europa.eu/methodology.

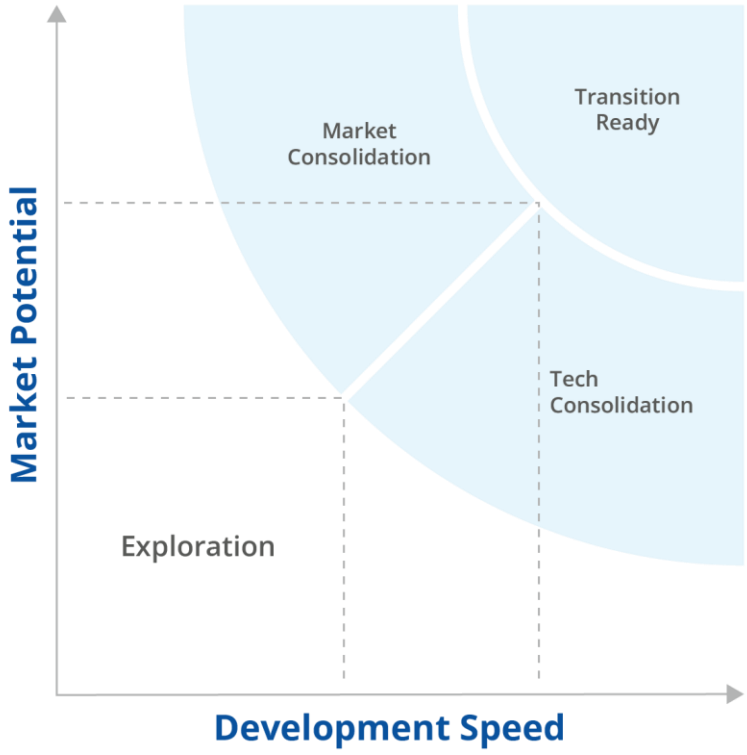


Figure 9 Main data visualisation for weak signals.

Together, these categories enable a more nuanced understanding of early-stage technologies – beyond binary weak/strong labels – by offering a visual prompt to guide strategic monitoring. Signals that are already moving fast but have limited systemic potential may require targeted experimentation, while signals that appear slower but with high systemic implications may merit early research investment or ecosystem coordination. In this way, the matrix becomes a key foresight tool, helping stakeholders identify not only which signals to watch, but also why and how they might matter in the future.

2.5.5 Strong Signal Visualisation

The primary visualisation output of the methodology is the radar chart, which serves as the central tool for communicating the positioning of strong signals. The radar is divided into five concentric adoption zones ([19]), each representing a different level of overall adoption likelihood, from early-stage exploration to near-mainstream deployment (see Figure 10).

- **Recognise.** Signals in this zone are currently not recommended for adoption. This may be due to immaturity, unresolved risks, lack of regulatory clarity or misalignment with current cybersecurity needs. Stakeholders are advised to monitor cautiously, but avoid active investment or deployment until further validation is available.
- **Observe.** Signals in this zone are worth watching and exploring, but not yet ready for scaled deployment. Early pilots or proofs of concept may be underway, and stakeholders are

([19]) The four adoption zones are once again inspired by the Thoughtworks Technology Radar and are commonly used across similar tools aimed at evaluating emerging technologies.

encouraged to investigate potential use cases, evaluate technical feasibility and monitor developments, particularly where alignment with a future strategy is expected.

- **Trial.** Signals in this zone are suitable for controlled experimentation in real-world conditions. While not yet fully mainstream, they have demonstrated sufficient maturity and promise. Stakeholders are encouraged to initiate pilot projects, collect evidence and build internal readiness for future scaling.
- **Plan.** Signals in this zone have proven potential and are approaching operational relevance. They are no longer purely experimental but require strategic planning for broader deployment. Stakeholders should focus on developing integration roadmaps, securing resources and aligning governance or procurement mechanisms to support upcoming adoption.
- **Implement.** Signals in this zone are considered mature and strategically relevant to wide adoption. They have proven value in cybersecurity operations, have passed through trial phases successfully and are supported by a growing ecosystem. Stakeholders should actively pursue integration, scale-up and long-term deployment.

This format enables intuitive reading of a technology's maturity for and proximity to widespread implementation, offering stakeholders a clear view of what is gaining traction within the cybersecurity ecosystem.

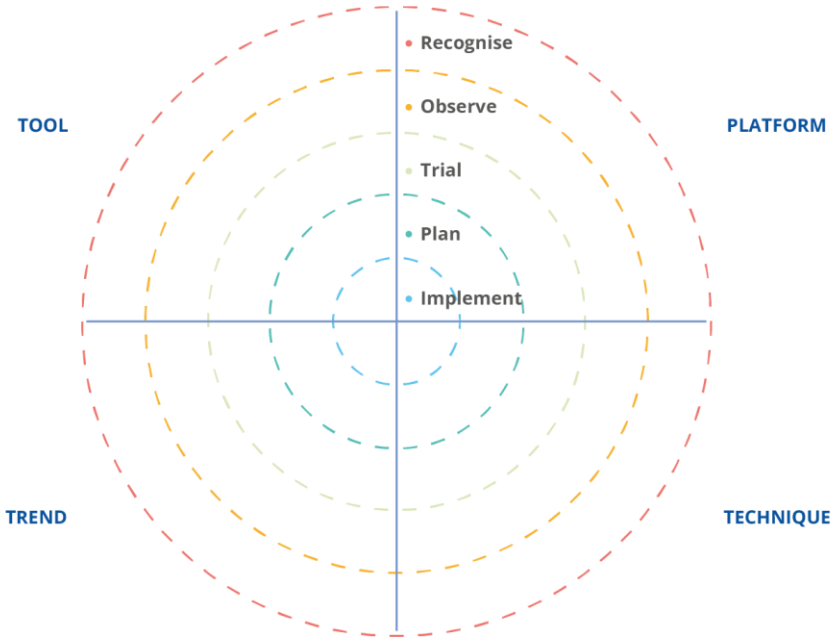


Figure 10 Main data visualisation for strong signals.

In addition to the core radar visualisation, complementary visualisations may be developed to deepen the analytical insights and tailor outputs to specific stakeholder needs. For example, data can be segmented by sector, geography or organisational size, allowing for a detailed view of where and by whom a technology is being adopted. Similarly, adoption readiness scores can be differentiated across stakeholder groups, such as users, suppliers and institutions, revealing how perceptions and preparedness vary across the ecosystem.

2.6 Data Visualisation

The visualisations generated through this methodology will be disseminated via a dedicated public dashboard, ensuring open access to the radar's findings and promoting transparency and stakeholder engagement across the EU cybersecurity community. This tool will allow users to explore the signals, their classification and associated indicators in a transparent and user-friendly format (see Figure 11).

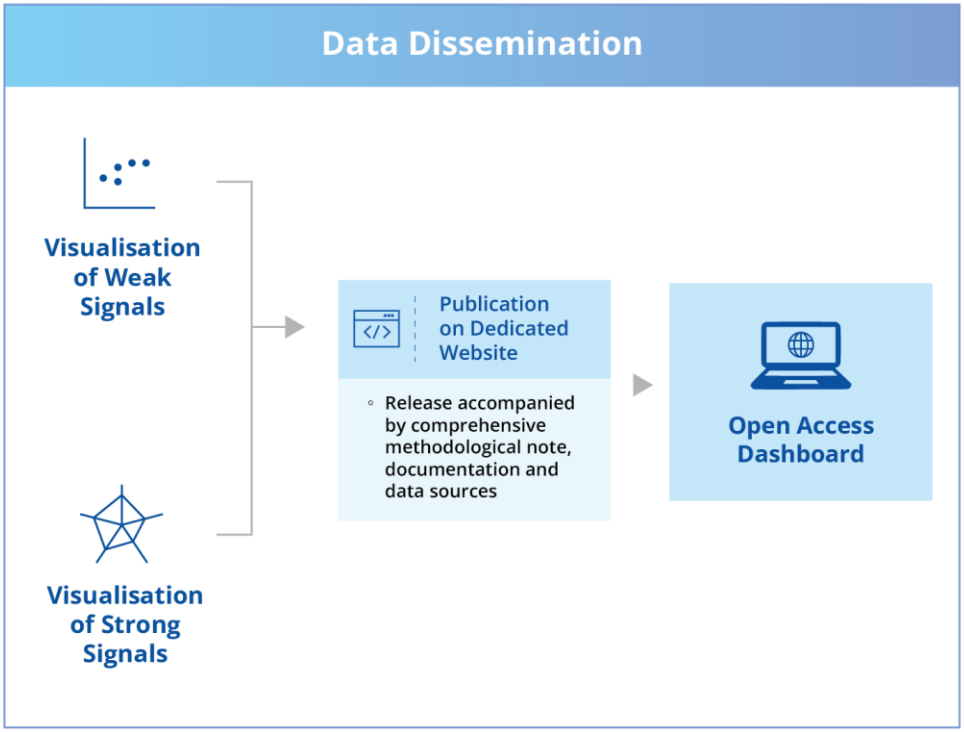


Figure 11 Detailed representation of the methodological steps of the data dissemination.

Each release of the data through the dashboard will be accompanied by a comprehensive methodological note, clearly detailing how the signals were identified, how each indicator was measured or estimated and the steps taken to ensure data consistency and analytical robustness. This documentation will also outline any known limitations or assumptions applied during the process.

To ensure accountability and foster stakeholder trust, the data sources underpinning the radar will be made publicly accessible via the same dashboard.

To support continual improvement and engagement, the website will also include a dedicated feedback channel, including a clear point of contact for questions, suggestions or methodological clarifications. Stakeholders will be encouraged to share their perspectives, propose additional sources or signal discrepancies, thereby contributing to the iterative development and relevance of future radar editions.

The technical format of the tool (e.g., PowerBI or equivalent) will be defined at a later stage of the radar project.

2.7 Signal Life Cycle Management

The radar is designed as a dynamic monitoring tool, continually evolving in line with technological and market developments. With each new edition, the status of all included signals will be systematically reviewed and updated to ensure the tool remains focused on relevant and emerging cybersecurity signals.

As part of this update cycle, signals that no longer exhibit sufficient strength and momentum will be removed from the radar. The threshold for this removal will be assessed on the use of the radar over a three-year period. This ensures that the analysis does not become diluted by outdated or stagnant entries and continues to reflect the most pressing and promising developments in the cybersecurity landscape.

Conversely, signals that have reached technological maturity and demonstrate readiness for widespread adoption will also be phased out of the radar. While no longer considered emerging, these signals are acknowledged as having moved beyond the foresight scope of the radar and are therefore tracked through other operational or implementation-focused mechanisms, if necessary.

This life cycle management approach preserves the radar’s role as a forward-looking instrument, ensuring it remains focused, agile and strategically aligned with current and future cybersecurity challenges.

Bibliography

Bergek, A., Jacobsson, S., Carlsson, B., Lindmark, S., & Rickne, A. (2008). Analyzing the functional dynamics of technological innovation systems: A scheme of analysis. Research Policy, 37(3), 407-429. https://doi.org/10.1016/j.respol.2007.12.003

Bergek, A. (2019). 'Technological innovation systems: a review of recent findings and suggestions for future research,' Chapters, in: Frank Boons & Andrew McMeekin (ed.), Handbook of Sustainable Innovation, chapter 11, pages 200-218, Edward Elgar Publishing.

European Commission, Joint Research Centre. (2020). Science for policy handbook (M. Matusiak & M. Gagliardi, Eds.). Publications Office of the European Union. https://doi.org/10.2760/25354

European Commission, Joint Research Centre. (2022). European cybersecurity taxonomy (EUR 31224 EN). Publications Office of the European Union. https://doi.org/10.2760/13202

European Commission Joint Research Centre. (2024). Materialising the future: Horizon scanning for emerging technologies and breakthrough innovations in the field of advanced materials for energy (FUTURINNOV workshop report, 13 May 2024). Publications Office of the European Union. JRC Publications Repository

European Union Agency for Cybersecurity (ENISA). (2025). ENISA Single Programming Document 2025-2027: including multiannual planning, work programme 2025 and multiannual staff planning. Luxembourg: Publications Office of the European Union. https://www.enisa.europa.eu/sites/default/files/2025-02/17_02_2025_ENISA %20Single %20Programming %20Document %202025-2027.pdf

Hekkert, M. P., Suurs, R. A. A., Negro, S., Kuhlmann, S., & Smits, R. E. H. M. (2007). Functions of Innovation Systems: A new approach for analysing technological change. Technological Forecasting and Social Change, 74(4), 413-432. https://doi.org/10.1016/j.techfore.2006.03.002

Hendrix, T. (2019). TECHNOLOGY FORESIGHT OF PATENT MANAGEMENT: AN OVERVIEW ON BIG DATA FOR REPOSITORY FIELDS. Jurnal Bisnis dan Manajemen. 20. 175-193. 10.24198/jbm.v20i2.327.

Joanny, G., Giraldi, J., Perani, S., Fragkiskos, S., Rossi, D., & Eulaerts, O. (2020). Weak signals in Science and Technologies 2019: Analysis and recommendations. *[Proposed change: Integrate 'Guidance of the Search' under Development Speed or justify its separation.]*

Lopatka, M., Pólvora, A., Manimaaran, S., & Borissov, R. (2022). Identification of Emerging Technologies and Breakthrough Innovations (Working Paper 1/2022). European Innovation Council & Publications Office of the European Union.

Markard, J., & Truffer, B. (2008). Technological innovation systems and the multi-level perspective: Towards an integrated framework. Research policy, 37(4), 596-615.

OECD. (2019). Strategic foresight for better policies. OECD Publishing. https://doi.org/10.1787/9789264311817-en

OECD (2022) OECD Strategic Foresight Toolkit for Resilient Public Policy Strategic Foresight Toolkit for Resilient Public Policy (EN)

OECD (2023), OECD Science, Technology and Innovation Outlook 2023: Enabling Transitions in Times of Disruption, OECD Publishing, Paris, https://doi.org/10.1787/0b55736e-en.

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) (Text with EEA relevance)

Robinson, D. K., Winickoff, D., & Kreiling, L. (2023). Technology assessment for emerging technology: Meeting new demands for strategic intelligence. Organisation for Economic Co-operation and Development.

Thoughtworks. (2025, April). Technology Radar, Vol. 32: An opinionated guide to today's technology landscape. https://www.thoughtworks.com/content/dam/thoughtworks/documents/radar/2025/04/tr_technology_radar_vol_32_en.pdf

United Nations Environment Programme. (2021). Foresight briefs: Horizon scanning and foresight methodologies. UNEP. https://wedocs.unep.org/handle/20.500.11822/37387

Venkatesh, V., Morris, M. G., Davis, G. B. et al. (2003) User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, Vol. 27, No 3, pp. 425-478, 2003, Available at SSRN: https://ssrn.com/abstract=3375136

Annex 0: Desk Research – Tools and Frameworks reviewed

Introduction

This annex summarises the technology foresight, radar and evaluation frameworks analysed during the desk research phase to inform the development of the ENISA TIR. The review covered 11 reference models spanning public, private and academic contexts, complemented by a methodological clustering exercise mapping their visualisation and evaluation logic.

Tools and frameworks

#	Framework	Origin	Core focus	Evaluation dimensions	Visualisation type	Update frequency
1	Thoughtworks Technology Radar	Thoughtworks	Software development and engineering practices	Maturity, adoption, impact, risk	Quadrant-ring radar chart	Biannual
2	Zalando Technology Radar	Zalando	Internal technology adoption and alignment	Adoption, architecture fit, maintainability	Quadrant-ring radar chart	Rolling
3	DEVO (Digital Enterprise Value and Organization) Lab High Impact Technology Radar	SDA Bocconi School of Management / MIT	Emerging digital technologies and business impact	Impact, distance, speed	Multi-quadrant radar	Annual
4	Dresner Wisdom of Crowds	Dresner Advisory	Business intelligence and analytics market insights	33 vendor evaluation criteria	Comparative index/bar charts	Annual

5	Gartner Hype Cycle	Gartner	Technology maturity life cycle	Five maturity phases	Time-based curve	Annual
6	Gartner Magic Quadrant (MQ)	Gartner	Vendor landscape and competitiveness	Vision, execution	2x2 matrix	Annual
7	McKinsey Tech Trends Outlook	McKinsey	Cross-sector technology foresight	Innovation, investment, adoption	Bubble/bar charts	Annual
8	IDC (International Data Corporation) MarketScape	IDC	ICT vendor competitiveness	Capabilities, strategies	2x2 matrix	Annual/biennial
9	Forrester Wave	Forrester	Comparative vendor benchmarking	Offering strength, strategy, market presence	2x2 mMatrix	Annual/biennial
10	NASA (National Aeronautics and Space Administration) TRL Framework	NASA	Technology readiness and maturity	Nine readiness levels	Linear scale/index	Continual
11	BMW (Bayerische Motoren Werke) Tech Trend Radar	BMW Group	Mobility foresight	Relevance, speed, knowledge gap	3-layer radar	Annual

Common methodological features

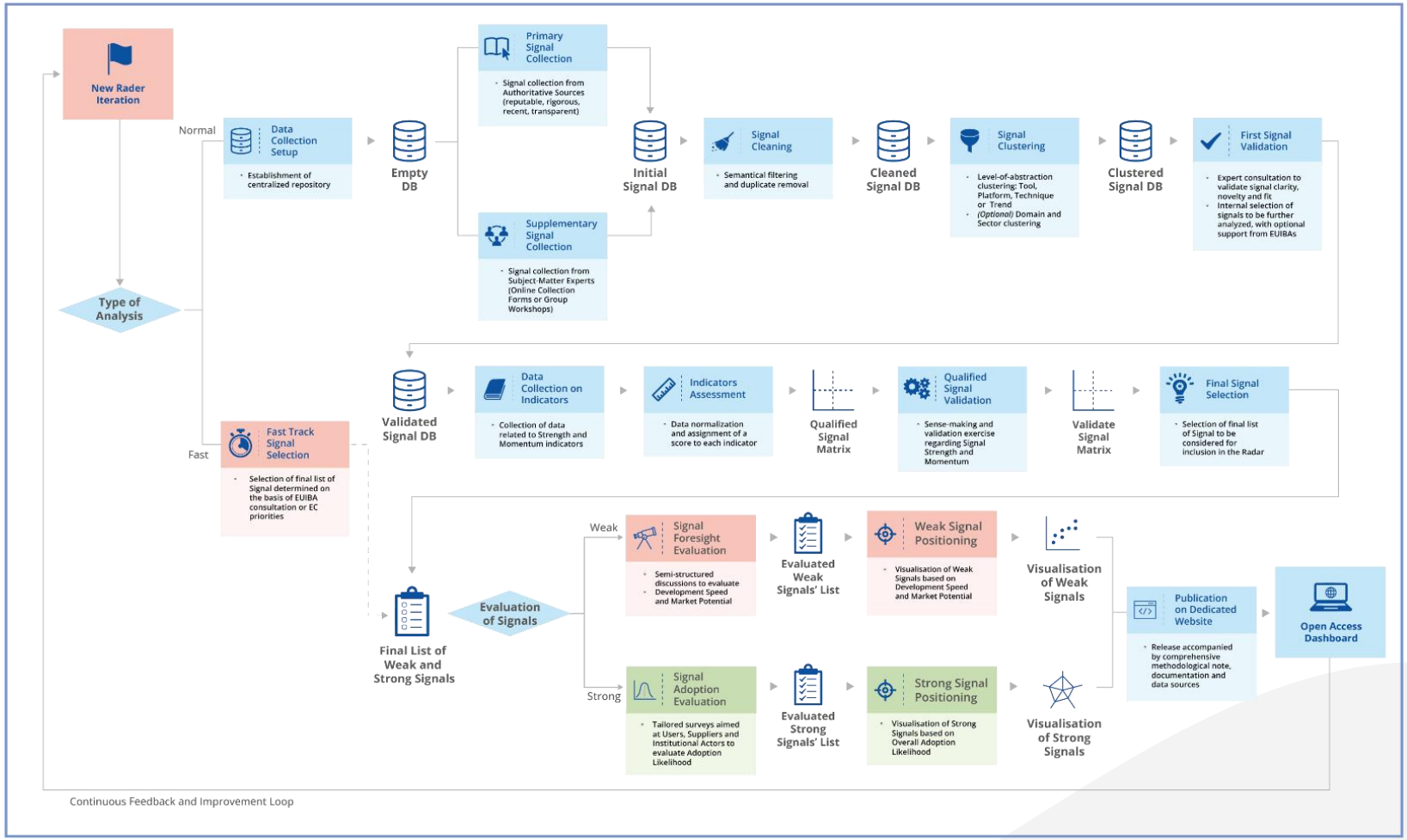
Category	Description
Structured Taxonomy	Frameworks classify technologies into clusters for comparability and filtering.
Multi-criteria scoring	Combination of maturity, adoption, impact and risk dimensions; qualitative or quantitative.
Expert validation	Iterative expert engagement and peer review ensure reliability and consensus.
Regular cadence	Periodic updates (biannual to annual) ensure relevance and trend consistency.
Actionability	Insights guide adoption, investment or policy priorities.
Visual transparency	Use of radar charts, matrices, cycles or indices for intuitive communication.

Clusterisation of frameworks

Cluster	Representative models	Foresight function	Strengths	Limitations
Radar charts	Thoughtworks, Zalando, DEVO, BMW	Diagnostic + prescriptive	Visual maturity overview	Limited time dimension
Matrix models	Gartner MQ, IDC, Forrester, McKinsey	Prescriptive (investment)	Supports prioritisation	Oversimplifies multidimensionality
Technology cycles	Gartner Hype Cycle	Prognostic (timing)	Captures evolution over time	Perception-based
Linear indices	NASA TRL, Dresner	Diagnostic benchmarking	Easy comparability	Reduces complexity

Annex 1. Complete methodology flowchart

The flowchart below illustrates the overall generic process underpinning the radar methodology. It visually summarises the sequence of phases and feedback loops that guide the identification, qualification and evaluation of signals and the overall dissemination of the tool. This representation aims to clarify how the different methodological components connect and tries to ensure a coherent understanding of the workflow across all actors involved.


New Rader Iteration
Type of Analysis
Normal
Data Collection Setup
Establishment of centralized repository
Empty DB
Primary Signal Collection
Signal collection from Authoritative Sources (reputable, rigorous, recent, transparent)
Supplementary Signal Collection
Signal collection from Subject-Matter Experts (Online Collection Forms or Group Workshops)
Initial Signal DB
Signal Cleaning
Semantical filtering and duplicate removal
Cleaned Signal DB
Signal Clustering
Level-of-abstraction clustering: Tool, Platform, Technique or Trend
(Optional) Domain and Sector clustering
Clustered Signal DB
First Signal Validation
Expert consultation to validate signal clarity, novelty and fit
Internal selection of signals to be further analyzed, with optional support from EUIBAs
Validated Signal DB
Data Collection on Indicators
Collection of data related to Strength and Momentum indicators
Indicators Assessment
Data normalization and assignment of a score to each indicator
Qualified Signal Matrix
Qualified Signal Validation
Sense-making and validation exercise regarding Signal Strength and Momentum
Validate Signal Matrix
Final Signal Selection
Selection of final list of Signal to be considered for inclusion in the Radar
Fast
Fast Track Signal Selection
Selection of final list of Signal determined on the basis of EUIBA consultation or EC priorities
Final List of Weak and Strong Signals
Evaluation of Signals
Weak
Signal Foresight Evaluation
Semi-structured discussions to evaluate Development Speed and Market Potential
Evaluated Weak Signals' List
Weak Signal Positioning
Visualisation of Weak Signals based on Development Speed and Market Potential
Visualisation of Weak Signals
Strong
Signal Adoption Evaluation
Tailored surveys aimed at Users, Suppliers and Institutional Actors to evaluate Adoption Likelihood
Evaluated Strong Signals' List
Strong Signal Positioning
Visualisation of Strong Signals based on Overall Adoption Likelihood
Visualisation of Strong Signals
Publication on Dedicated Website
Release accompanied by comprehensive methodological note, documentation and data sources
Open Access Dashboard
Continuous Feedback and Improvement Loop

Annex 2. Suggested Governance Structure

The following two tables provide a summary of the proposed governance structure for the radar. They outline the key roles and responsibilities established to ensure effective management throughout all phases of the methodology. Together, these tables offer a clear overview of how decision-making, validation and oversight are organised to maintain the quality, consistency and continuity of the radar process. The currently proposed governance structure envisions teams to be consolidated into three layers:

- a strategic oversight layer, consisting of the ENISA Management Board and, optionally, people from EUIBAs;
- an operational layer, consisting of the ENISA Core Radar Team;
- an expert and validation layer, consisting of the AHWG and the ENISA Advisory Group.

The allocation of tasks presented below remains to be further tested on the provisional use cases of the project.

	(Optional) Fast-Track Signal Selection	Step 1 – Data Collection Setup	Step 2 – Primary Signal Collection	Step 3 – Supplementary Signal Collection	Step 4 – Signal Cleaning	Step 5 – Signal Clustering	Step 6 – First Signal Validation and Selection
ENISA Core Radar Team	• /	• Prepare Database for Data Collection	• Perform Primary Signal Collection on Authoritative Sources	• Conduct Supplementary Signal Collection (online or hybrid)	• Perform Signal Cleaning	• Perform Signal Clustering	• Conduct First Signal Validation workshop • Propose First Signal Selection
Ad-Hoc Working Group (or alternative Experts' Team)	• /	• /	• /	• Participate to Supplementary Signal Collection (online or hybrid)	• /	• /	• Participate to First Signal Validation workshop
ENISA Advisory Group (or secondary Experts' Team)	• /	• /	• /	• /	• /	• /	• /
ENISA Management Team	• Confirm Signal for Fast-Track	• /	• /	• /	• /	• /	• Confirm First Signal Selection
EUIBA	• Propose Signal for Fast-Track	• /	• /	• /	• /	• /	• *(Optional)* Participate to First Signal Selection
Industry and Other External Stakeholders	• /	• /	• /	• /	• /	• /	• /

Annex 3: Suggested Authoritative Sources

The following table presents a selection of authoritative sources that may be considered for inclusion in the ENISA radar. This list is not intended to be exhaustive or definitive at this stage; rather, it serves as a general reference to guide the identification and use of relevant documents and frameworks that support the assessment and monitoring activities within the radar.

Type of player	Name of report
Market analysts and consultancies	Gartner Magic Quadrant (for specific tools/platforms)
	Gartner Hype Cycle for Security Operations
	Gartner Market Guide for Security
	Forrester Wave reports (for specific tools/platforms)
	IDC Marketscape (for specific tools/platforms)
International organisations and standards bodies	OECD Digital Security
	International Telecommunication Union (ITU) Global Cybersecurity Index
	WEF Global Cybersecurity Outlook
	ENISA Foresight Cybersecurity Threats for 2030
	ENISA Threat Landscape
Universities and research centres	Oxford Martin School – Impacts of Future Technology (on cybersecurity topics)
	Harvard – Critical and Emerging Technologies Index (on cybersecurity topics)
	Fraunhofer Institute for Secure Information Technology (SIT) research
	MIT Technology Review (on cybersecurity topics)
	JRC Technology Foresight (on cybersecurity topics)
Industry associations and technical alliances	ETSI Technology Radar
	Cloud Security Alliance – Emerging Technologies
	ECSO – Technologies, Innovation, and Industry Working Group reports
Regulatory and legal institutions	Commission reports (on cybersecurity topics)
	National cybersecurity agencies (e.g. Agenzia per la Cybersicurezza Nazionale (ACN) (National Cybersecurity Agency of Italy)) reports
Investment banks and venture funds	PitchBook Cybersecurity Venture Capital Trends
	Cybersecurity Ventures Market Report
	CB Insights Cybersecurity Trends

TP-01-26-007-EN-N

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

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union