R&I Preparation for the Market

A visual guide to the EU Cybersecurity Project landscape

2020

Acknowledgement:

The organisers would like to thank the projects and individual experts that have contributed to the series of webinars on the topic of Market and Technology Readiness Level (MTRL) and the recommendations provided in this document. More details and contact details can be found in section 4.

Cybersecurity and Privacy R&I Projects

Spanish H2020 NCP for the EIC Accelerator

Disclaimer

The work described in this document has been conducted within the project cyberwatching.eu. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under Grant Agreement no.740129. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

Table of Contents

Table of Figures

Terminology

BMC	**Baseboard Management Controller**
CSIRT	Computer Security Incident Response Teams
EC	European Commission
ECHO	European network of Cybersecurity centres and competence Hub for innovation and Operations
EIC	European Innovation Council
EU	European Union
GHOST	Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control
IPR	Intellectual Property Rights
NCP	National Contact Point
NREN	National Research and Education Network
MISP	Malware Information Sharing Platform
MPV	minimum price variation
MRL	Market Readiness Level
MSP	Managed Service Providers
MSSP	Managed Security Service Providers
MTRL	Market and Technology Readiness Level
MVP	Minimum Viable Product

PROTECTIVE	Proactive Risk Management through Improved Cyber Situational Awareness
R&I	Research and Innovation
SME	Small Medium Enterprise
SMESEC	Protecting Small and Medium-sized Enterprises digital technology through an innovative cyber-SECurity framework
SWOT	Strength Weakness Opportunity Threats
TRL	Technology Readiness Level

1 Introduction

The challenges and recommendations towards a secure and trusted Digital Single Market was discussed on the World Café Sessions held during the second (2nd) Cyber Concertation meeting of H2020 projects from unit H1 "Cybersecurity & Privacy" last June 2019[1]. One of the topics being discussed was "How R&I can improve the way they prepare for the market".

The cyberwatching.eu project is addressing this issue in a number of ways. Firstly through the project's European Project Radar which maps and positions over 200 EC-funded projects within the Cybersecurity landscape and secondly through a market and technology readiness level analysis (MTRL) (see cyberwatching.eu D2.3 Methodology for the classification of projects and market readiness)[2] of projects which are used to understand and assess how close the research and innovation (R&I) projects are to the market. And thirdly, the project cybersecurity and privacy marketplace provide a platform for projects to showcase their results to a market audience and rub shoulders with start-ups and SMEs innovating in the area. In this report we'll look in more detail, in particular on the role of the radar and the MTRL analysis is providing a birds-eye view of the current R&I landscape and how this can encourage clustering and the sharing of best practices on market readiness.

With this in mind, cyberwatching.eu held a key webinar in March 2020 which shared some best practices from four different initiatives that are excelling in this area:

- **GHOST**[3] — Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control
- **PROTECTIVE**[4] — Proactive Risk Management through Improved Cyber Situational Awareness
- **SMESEC**[5] — Protecting Small and Medium-sized Enterprises digital technology through an innovative cyber-SECurity framework
- **Spanish H2020 NCP for the EIC Accelerator** — Centro para el Desarrollo Tecnológico Industrial

This report provides an overview of these best practices and gathers recommendations from them.

[1] https://cyberwatching.eu/news-events/events/brussels-second-cw-concertation-meeting-04062019-0
[2] https://cyberwatching.eu/d23-methodology-classification-projectsservices-and-market-readiness
[3] http://cyberwatching.eu/projects/1056/ghost
[4] http://cyberwatching.eu/projects/1036/protective
[5] http://cyberwatching.eu/projects/985/smesec

2 Why and how cyberwatching.eu is supporting projects in assessing their market readiness

Cyberwatching.eu aims to improve the impact of the results of Research and Innovation projects in the European Union and Associated Countries, and to achieve this, the overall cyberwatching.eu methodology is founded on the following 3 macro-activities:

1. Mapping the R&I landscape and the delivery of a European project radar,
2. Clustering and supporting synergies between projects,
3. Supporting projects assess and improve their market readiness

Cyberwatching.eu has mapped and engages with over 200 European projects focusing on cybersecurity and privacy to:

- position themselves within the broader EU landscape,
- demonstrate progress, and market and technology readiness levels,
- showcase their results to the market.

2.1 The European Project Radar

There are 25 calls launched by the European Commission (EC) which were either explicitly supporting projects in the domain of Cybersecurity and privacy or from which projects in this area were supported. Since some of these programmes are now completed, what is the impact that these programmes have had, and more specifically, what is the status of each funded project in respect to its maturity, results and outputs? Are the results of these projects ready to be adopted and used by external stakeholders such as European SMEs and organisations?

Cyberwatching.eu's European Project Radar[6] is trying to answer all of this by using a number of underpinning information sources to visualise the state of these projects as a means to maintain an overview of the larger European Cybersecurity research landscape.

The radar addresses key areas of interests for projects themselves, and for funding agencies:

- What are the focus areas of research and innovation funding in the EU?
- In a nutshell, what does the pipeline in research innovation look like?
- When can we expect results that can be ingested by the target customer segments?
- How well are the projects progressing through their work plan?
- How well are we progressing compared to our competitors?

[6] https://www.cyberwatching.eu/technology-radar

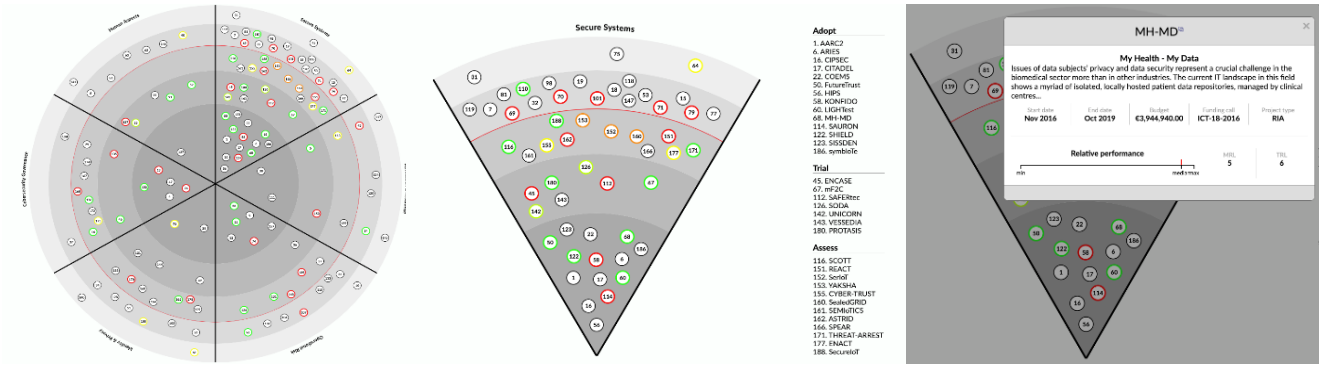

Figure 1 *European Project Radar – Spring 2020 edition*

The radar allows swift yet statistically sound statements on the state of the European cybersecurity and privacy research landscape. It provides a birds-eye view of the complete collection of EU-funded projects in the cybersecurity area. The projects are grouped by research themes, colour-coded to show their position in the project lifecycle and assessed using Market and Technology Readiness Levels methodology.

In June 2020, a new version of the radar will be launched updating on current entries and introducing new projects funded since the last version published in Autumn 2019.

If you want to find out more about each project on the radar, then details, updated information and direct contact with the project is available directly through the radar.

2.2 Market and Technology Readiness Levels

The "Market & Technology Readiness Level" (MTRL) methodology was developed by cyberwatching.eu to evaluate how close projects are to the market. The MTRL is introduced as a complementary methodology to "Technological Readiness Level" (TRL) to assess projects' outcomes.

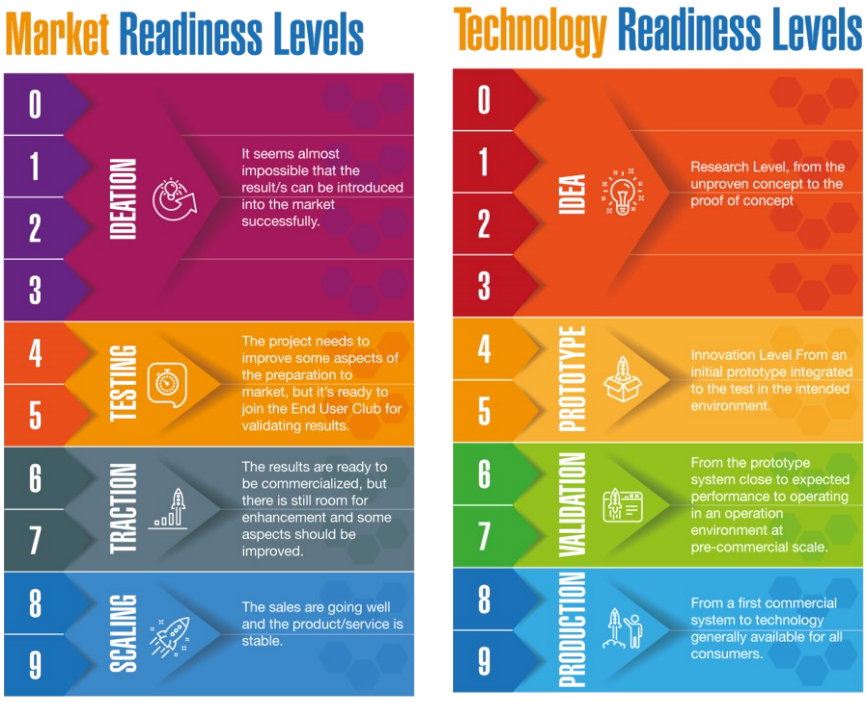

Figure 2 *Market & Technology Readiness Level (MTRL)*

The goals of applying this methodology to the projects, cyberwatching.eu will be able to identify:

- Future collaboration and sharing of experience on common technical priorities;
- Re-use of project results with components, technical ideas, methodologies or best practices identified by a repeatable statistical analysis;
- Identify market positioning and potential exploitation opportunities with other projects.

Based on the analysis and results from applying the methodology described in this document, cyberwatching.eu will hone in on priority areas and actively engage with clustered projects in a series of activities which encourage projects to:

- Attend "Technology Deep Dive" workshops to map existing solutions with priority areas and enable common approaches to similar challenges and facilitate re-use of research results;
- Contribute to white-papers focussing on challenges in Cybersecurity & Privacy, to be also addressed by future Work Programmes;
- Test and validate market readiness of R&I solutions.

This will facilitate the connection between funded projects and future funding actions to find synergies and convergences and to take advantage of previous results to build new products and services on the founding blocks of the identified results.

This allows the user to identify clusters or projects working in the same sub-domain with similar technology readiness or similar market readiness and establish mutually beneficial relationships among projects that can identify common themes and challenges for future activities.

3 From research to market: best practices and recommendations

A great deal of effort of EU-funded projects goes into developing the technological aspects of products and project outputs. However, a corresponding amount of support activity is vital to bring those outputs to the market, providing an organic sustainability plan and an exploitation strategy.

Within the context of sustainability and exploitation, 'Market Readiness' is defined as the process by which a consortium ensures that their project outputs are ready to go to the market.

Research and innovation projects are usually set up to find a solution for a need. Early-stage exploitation planning should be a vital part of a project's activities. To identify the timing for such a decision, a market-based mechanism is relevant.

Market-based mechanisms offer advantages over other regulatory approaches, providing decision-makers with a holistic view of a project's maturity in a simple way - with a single score. It offers decision-makers a faster way to assess, measure and support technology projects.

3.1 GHOST - Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control

Website: www.ghost-iot.eu
Duration: May 2017 - April 2020
Contributor: Javier Augusto Gonzalez, Project Manager, Televés

The **GHOST**[7] project contributed a number of reflections and recommendations on the future exploitation of the project's results during the preparation of the proposal itself. During this stage, two factors are critical:

- First, the composition of the consortium, where we recommended including all the actors of the specific value chain (especially end-users)
- Second, the methodology that needs to be followed during the project, where the GHOST project recommended defining specific activities to test products with potential end-users as soon as possible.

For this second point, many activities should be performed based on the design thinking principles, including real-life trials or pilots (where the systems can be deployed in realistic operational scenarios, unveiling the main issues during day-to-day usage of the products), online questionnaires, focus groups, etc.. The objective of these activities should be to obtain feedback on the acceptance of the products and the potential improvements that the product needs in order to increase the observed acceptance. In this sense, this continuous feedback is the basis of a continuous improvement path from the Minimum Viable Product (or MVP), which should be released (even incomplete) as soon as possible during the project to the final version of the products by the end of the project.

In addition to this general approach and methodology, the focus should be on creating a solid individual or joint business plan through the identification of the final products; the identification of the relevant Intellectual Property Rights for each of these products; the identification of the potential customers; the definition of the user journeys of these customers (including their feelings while using the products, the potential frustration, the touchpoints with the solution, etc.); and through using every tool that can unveil insights into the underlying business models that you are targeting (Lean Model Canvas, etc.).

Even only the exercise of creating this business plan will greatly improve the maturity of your Market Readiness Level as the points addressed will make you take decisions.
For the business plan for the GHOST project, consortium partners decided to follow a joint exploitation model, and we are creating a business plan that includes the following points:

[7] http://cyberwatching.eu/projects/1056/ghost

- Mission and vision
- Short, mid and long-term objectives with a specific market's tactical, strategic KPIs
- Shareholder distribution based on the product and product IPR identification and additional knowledge/value added by some partners (for example, knowledge of the market or the end-users)
- Location and facilities (taking into consideration the average costs, resources availability, maturity of the entrepreneurship ecosystem, geographical placement, international projection)
- Current product and services identification (filtered from the previously identified set of products)
- Future product and services identification
- Market segmentation and analysis
- Value proposition definition
- Team definition (CEO, Sales, Developers, etc.)
- Key financial indicators (annual expenses, annual expenditures, annual revenues, break-even point projection, profit and loss model)

3.2 PROTECTIVE – Proactive Risk Management through Improved Cyber Situational Awareness

Website: https://protective-h2020.eu
Duration: September 2016 - August 2019
Contributor: Marcin Przybyszewski, Exploitation/Dissemination manager, ITTI

The **PROTECTIVE**[8] project contributed observations and **actions implemented to achieve higher market readiness level**. In the PROTECTIVE project, several steps have been taken throughout the project in order to assure a high MTRL/MRL (Market Readiness Level) would be achieved. Already at the pre-project phase, appropriate exploitation tasks were defined, and a draft business plan was created. Also, at the proposal writing stage, future licencing of final system elements were agreed and secured between partners. During the project, the PROTECTIVE consortium used pilots and communication/dissemination activities to both validate and refine plans to maximise the project impact as well as to identify potential for exploitation of the results after the project concludes.

PROTECTIVE concentrated on starting exploitation from the NRENs and progressively expanding to other domains, including a critical infrastructure operator, Managed Security Service Providers (MSSPs), Managed Service Providers (MSPs) – and ultimately, reaching SMEs (clusters of SMEs managed by MSPs). Twenty-five CSIRT-like organisations were contacted for pilot two, with six

[8] https://cyberwatching.eu/projects/1036/protective

committing to the pilot, and another ten engaging with the pilot to varying degrees e.g. through webinars and email conversation. A consortium member MSSP leveraged Threat Intelligence from PROTECTIVE to enrich its services provided to MSPs and SMEs. Four MSPs/MSSPs joined the pilot, having an impact on approximately 350 SMEs.

To increase the potential for technology take-up, PROTECTIVE has been open-sourced with extensive documentation for ease of deployment and to enable further development. To increase impact further, connectors have been prototyped to demonstrate interoperability of PROTECTIVE with MISP communities.

Finally, a key factor was to gain the trust of organizations / CSIRTS outside the PROTECTIVE consortium. To increase trust and reduce the reluctance in sharing data, a new information-sharing compliance module was included in PROTECTIVE.

For future call recommendations, we would suggest that there is a distinction between projects aimed at, for example, market commercialization and projects aimed at kicking-off free/open-source projects. Projects kicking off open-source projects should aim more at building communities around the developed tools and have less focus on market commercialization. On the other hand, projects aiming at market commercialization should have an increased marketing budget as compared to other projects (i.e. increased marketing budget in relation to the budget of technical tasks).

Furthermore, as there are often differences between local markets (size, customer sentiments etc.), this makes it impossible to deliver one solution for the whole EU region. As such, individual exploitation plans – or commercializing single solutions – should be treated equivalently to consortium-wide efforts.

3.3 SMESEC – Protecting Small and Medium-sized Enterprises digital technology through an innovative cyber-SECurity framework

Website: https://smesec.eu
Duration: June 2017 - May 2020
Contributor: Alberto Miranda García, Senior Business Consultant, ATOS

The **SMESEC**[9] project contributed observation as part of the exploitation strategy and business plan approach of the project. The following steps are considered the basis to effectively transfer to the market the project result:

In an exploitation strategy it can be hard for R&I projects to shift mentality to developing new products or technologies that should be ready for the market. Here are some of the topics which are crucial for the exploitation of pre-project considerations that will help you succeed with a solid exploitation plan.

1. **Supply-side.** Keywords: unfair advantage, competitors' analysis
2. **Demand-side.** Keywords: identification of customer needs, market trends
3. **Individual exploitation**. Partners' individual exploitation plans
4. **Joint exploitation.** Intellectual Property Rights (IPR) agreement. Distribution of the intellectual property rights
5. **Exploitation agreement.** Definition of roles, responsibilities and compensation scheme in a future commercial opportunity the partners may go for.

Once the project has concluded, a **business model** is generated to address the sustainability of the project. The business plan summarises the contents and characteristics of the project results, products and services. Below are some guides on how to develop a business model which clearly addresses the following building blocks:

- **Value proposition.** What is the **added value** SMESEC can provide and would a user be **willing to pay for it?**
- **Customer Segment.** Which are the **different target groups** of people or organizations, targeted groups and an estimation of the customers?
- **Distribution channels.** How will we **communicate and contact/reach** our Customer Segments to deliver a Value Proposition?
- **Customer Relationships.** Types of relationships established with the different customer segments.
- **Revenue streams.** How will we **generate incomes** from the different customer segments?
- **Key activities.** Which are the most important actions we must carry out to make this business model work?
- **Key Resources.** Which are the most important **resources needed**?
- **Key Partners.** Main partners or associates to work with

[9] http://cyberwatching.eu/projects/985/smesec

- **Cost Structure.** The Cost Structure describes all costs incurred to operate business activities. What are the main costs attached to our business model?

3.4 CDTI - Centro para el Desarrollo Tecnológico Industrial

Website: http://perspectivacdti.es/
Contributor: Esther Casado, Spanish NCP for the EIC Accelerator, CDTI

Finally, the Spanish National Contact Point for EIC Accelerator from CDTI[10] contributed observations on the commercial exploitation from research and development results to the market.

- Two scales are running in parallel: TRL scale & Market Readiness Level. Make your business move up in the MRL.
- Focus on the market as soon as possible, and start showing the minimum price variation (mpv) to your customer as soon as you can.
- There are many elements to create a Business Plan. They could be organized in three main areas: Business opportunity, Business Model and Sustainability & Financials.
- Four aspects to analyse in a preliminary stage:
    - IPR for exploitation, FTO is mandatory for exploitation
    - Modelling the business to define the strategy
    - Size of the Opportunity, to ensure the scale-up potential
    - Why the client will buy you. The value proposition to align user needs with your strategy.
- There are many tools to analyse the business in different dimensions. The three essentials are Strength Weakness Opportunity Threats (SWOT), Baseboard Management Controller (BMC) or Value Proposition Design.

[10] http://perspectivacdti.es/

4 Conclusion

The Cyberwatching.eu's webinar "From research to market: promising outputs are not enough! "[11] provided some very useful insights into how R&I can improve the way they prepare for the market.

The key advice to improve your project market readiness came from tips and best practices shared from three H2020 projects that are an example of advanced market preparation: PROTECTIVE, GHOST and SMESEC.

These were:

- Learning key factors for market-oriented exploitation,
- Finding out what profiles you need in your project team,
- Discovering the role of Intellectual Property Rights (IPR) management
- Becoming part of our Cyberwatching community.

The key recommendations provided by the speakers are detailed below:

- Keep the focus on creating a solid individual or joint business plan through the identification of the following:
  - final products,
  - relevant Intellectual Property Rights for each of these products,
  - potential customers,
  - user journeys of these customers (including their feelings while using the products, potential frustration, the touchpoints with the solution, etc.).

  Remember to do this through using every tool that can unveil insights into the underlying business models that you are targeting (Lean Model Canvas, etc.).

- Consider the difference between the global and local market for your solution, whether you need the local presence and how to achieve it.
- Acknowledge the importance of starting the exploitation planning and considering the end-user during the implementation and thinking outside the box during the execution stage.
- Presentation of project success stories to showcase the potential ability of the organisation to transfer the project result to the market.

If your project is already in the European Project Radar[12], make sure to update your status and ranking by answering the **MTRL assessment form** sent by the Cyberwatching team.

If you have not yet plugged into this invaluable opportunity, now is the time to participate and register the R&I project in the Cyberwatching Project Hub[13] and answer the MTRL questionnaire to make sure your project is included in the Project Radar Spring edition.

[11] https://cyberwatching.eu/research-market-promising-outputs-are-not-enough
[12] https://cyberwatching.eu/technology-radar
[13] https://cyberwatching.eu/projects

5 Contributing projects

Cyberwatching.eu would like to thank the projects and representatives that have contributed to this document.

- **GHOST**, http://cyberwatching.eu/projects/1056/ghost

  Contributor: Javier Augusto-Gonzalez
  Project Manager, PMP
  TELEVES

- **PROTECTIVE**, http://cyberwatching.eu/projects/1036/protective

  Contributor: Marcin Przybyszewski
  Project Manager
  ITTI

- **SMESEC**, http://cyberwatching.eu/projects/985/smesec

  Contributor: Alberto Miranda
  Business Consultant
  ATOS Spain

- **EIC Accelerator**, http://perspectivacdti.es/

  Contributor: Esther Casado
  Spanish NCP for the EIC Accelerator
  CDTI

- **ECHO**, https://cyberwatching.eu/projects/1043/echo

  Contributor: Matteo Merialdo
  Manager, Security Research and Development (R&D) Projects
  RHEA Group

cyberwatching.eu consortium

Trust-IT Services
Communicating ICT to markets

Oxford e-Research Centre

University of Oxford

ICT Legal Consulting
Balboni Bolognini & Partners

European Digital SME Alliance

CONCEPTIVITY

360 SECURITY

AON

aeiciberseguridad
Agrupación Empresarial Innovadora CIBERSEGURIDAD y Tecnologías Avanzadas

www.cyberwatching.eu

@cyberwatchingeu

/in/cyber-watching/

cyberwatching.eu has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740129.