Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: 1 February 2019
Project duration: 47 months

Cyber Security for Europe

D9.27
Exploitation Strategy Report 3

Document Identification	
Due date	31 December 2022
Submission date	23 December 2022
Revision	1.0

Related WP	WP9	Dissemination Level	PU
Lead Participant	TDL	Lead Author	David Goodman (TDL)
Contributing Beneficiaries	ATOS, JAMK, SINTEF	Related Deliverables	D9.14, D9.19

Abstract

This is the third and final report in a series of three that identifies the exploitable results of CyberSec4Europe relating to assets developed or enhanced during the course of the project. It reflects the methodology first described in the second report for assessing innovation and market sustainability and shows how this was deployed in the evaluation of the assets first by the task team and then by an external independent two-person jury, culminating in presentations given at the Momentum! event in December 2022.

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

Executive Summary

This is the third and final report in a series of three that identifies the exploitable results of CyberSec4Europe relating to the assets developed or enhanced during the course of the project. It reflects the methodology first described in the second report for assessing innovation and market sustainability based on a set of value parameters with associated suggested weightings.

Results from all consortium partners were collected and then evaluated first by the task team with the intention of filtering the number of top key results to 14. A jury of external independent jurors was chosen from the project's associate partners and asked to score the list of 14 assets down to six that would be invited to present their results at the Momentum! event in December 2022 as if they were trying to impress a set of potential investors.

Each of the six asset owners were given 15 minutes each to present to the assembled audience at the event including the jurors who provided their summing up and choice of the most promising two assets which were presented with a trophy to celebrate their achievement. These two assets will be forwarded to the Commission's H2020 Results Platform on behalf of CyberSec4Europe.

Nonetheless, it was and is consistently emphasised that everyone's a winner!

Document information

Contributors

Name	Partner
Aljosa Pasic	ATOS
Christine Jamieson	TDL
David Goodman	TDL
Gencer Erdogan	SINTEF
Jani Paijanen	JAMK
Karin Bernsmed	SINTEF
Per Meland	SINTEF
Shukun Tokas	SINTEF

Reviewers

Name	Partner
Stephan Krenn	AIT
Liina Kamm	CYBER

History

Version	Date	Authors	Comment
0.1	14 December 2022	David Goodman	First draft
0.2	17 December 2022	David Goodman	Second draft
1.0	22 December 2022	David Goodman	Final version
1.0	23 December 2022	Ahad Niknia	Final check, preparation and submission process

Table of Contents

List of Figures

List of Tables

List of Acronyms

D	**DIH**	Digital Innovation Hub
E	**ECCC**	European Cybersecurity Competence Centre
	ECSO	European Cyber Security Organisation
	ENISA	European Union Agency for Cybersecurity
	EU	European Union
	EUCC	European Union Cybersecurity Certification
I	**IDS**	Intrusion Detection System
	ISV	Independent Software Vendor
M	**MISA**	Microsoft Intelligent Security Association
	MISP	Malware Information Sharing Platform
	MSSP	Managed Security Service Provider
N	**NCC**	National Coordination Centre
S	**SIEM**	Security Information and Event Management

List of CyberSec4Europe Partners

A	**ABI**	ABI Lab
	AIT	AIT Austrian Institute of Technology GmbH
	ARCH	Archimede Solutions SARL
	ATOS	Atos
B	**BBVA**	BBVA Group
	BRNO	Masaryk University
C	**C3P**	University of Porto
	CNR	Consiglio Nazionale delle Richerche
	CONCEPT	CONCEPTIVITY
	CTI	Computer Technology Institute and Press “Diophantus”
	CYBER	Cybernetica
D	**DAWEX**	Dawex
	DTU	Technical University of Denmark
E	**ENG**	Engineering Ingegneria Informatica S.p.A
F	**FORTH**	Foundation for Research and Technology Hellas
G	**GEN**	Comune di Genova
	GUF	Johann Wolfgang Goethe-Universität Frankfurt
I	**I-BP**	Informatique Banques Populaires
	ICITA	International Cyber Investigation Training Academy
	ISGS	Intesa Sanpaolo
J	**JAMK**	JAMK University of Applied Sciences
K	**KAU**	Karlstad University
	KUL	KU Leuven
N	**NEC**	NEC Laboratories Europe GmbH
	NTNU	Norwegian University of Science and Technology (NTNU)
O	**OASC**	Open and Agile Smart Cities
P	**POLITO**	Politecnico di Torino
S	**SIE**	Siemens
	SINTEF	SINTEF
T	**TDL**	Trust in Digital Life
	TLEX	Timelex
	TUD	Delft University of Technology
U	**UCD**	University College Dublin & LERO
	UCY	University of Cyprus
	UM	University of Maribor
	UMA	University of Malaga
	UMU	University of Murcia
	UNILU	University of Luxembourg
	UNITN	University of Trento
	UPRC	University of Piraeus Research Center
	UPS-IRIT	Université Toulouse III Paul Sabatier – Institut de Recherche en Informatique de Toulouse
V	**VAF**	VaF
	VTT	VTT Technical Research Centre of Finland

1 Introduction

The new multi-level, multi-stakeholder structure created by the ECCC regulation is sometimes referred as an ecosystem, as it spans three levels (supranational, national and community hubs), people (whether in organisations, communities, hubs etc.), practices, technologies and even different cultural or common values. It might include different roles, tasks and relationships within a value stack or value chain. It is characterised by the reuse of shared resources or scale-up of new solutions, and synergy between different (sub-)communities, for example, for joint maintenance of building blocks or open-source cybersecurity software.

It includes (sub-)communities or stakeholder groups that have something in common. In CyberSec4Europe we consider and acknowledge the co-existence of different cybersecurity communities and the different categorisation of those communities (e.g., research, industry, assurance and certification, national, regional). In our view, activities in an ecosystem are also characterised by trade-offs and consensus, while the joint exploitation can also be understood as "connecting the dots", for example, between the research roadmap of a research community in the domain of cryptology to the exploitation path of a European industrial community in the defence sector.

It is therefore a challenging task to design a joint exploitation strategy "by the community" and "for the community", without having in mind a whole ecosystem, from policy makers and industrial priorities to the research and start-up landscape.

CyberSec4Europe is a pilot project for such a strategy, implementation options and operational execution. While this strategy is clearly to use the power and wisdom of a community at each step, in order to amplify impact and improve research to market transfer, there might be several alternative procedures and implementation choices, from marketplace to innovation competitions. One tactical choice that had its implementation in the final year was the process of filtering and prioritisation of the exploitable results by the community, and posterior selection of the most innovative and market attractive assets by an external jury. The methodology, implementation and the action steps in this process are outlined in the following chapters.

2 Methodology Review

In parallel with the original rendition of the proposed methodology in the second report in this series, a Powerpoint document was circulated to each of the CyberSec4Europe beneficiaries asking them to provide as much information as they can about any exploitable and/or innovative assets developed during the project. They were invited to imagine they were looking for funding for their asset, which they might indeed be, and to consider how they would convince a set of investors.

2.1 Gathering asset information

The questions were:

1. **Asset Overview:**

- What are the needs and challenges, the burning business problems, your asset is addressing?
- Who are the target audience?
- Who owns the asset: is it individually or jointly owned and are there any licence considerations?

Tips:

- *Avoid long stories: a couple of sentences, preferably with keywords*
- *Identify at three levels: (1) sector (2) teams (3) specific name(s)/role(s)*

- *Avoid confusing ownership and licensing!*

2. **Project Dividend:**

- As a result of your participation in the project have there been any noteworthy innovations and / or improvements to the asset?

Tips:

- *Did you start from an existing asset?*
- *Don't be concerned to state that your asset is based on an open source licence?*

3. **Network:**

- Is there a connection with any other tools either from within CyberSec4Europe or beyond?
- Is the asset associated with a particular demonstrator or other use case?

Tips:

- *No need to provide a complete market analysis. You could possibly use a SWOT analysis (cf. the ones in deliverable D4.4[1])*
- *List all inputs and outputs. This is not necessarily business relevant, but it's important to indicate possible dependencies.*

4. **Market:**

- What market segment does the asset fit?
- How would you position your asset in this market?
- Are there potential competitors who you are aware of?

Tips:

- *Again, you don't have to provide a fully-fledged analysis, just a few bullets will do indicating, for example, whether your asset is available standalone or as a service?*

5. **Business Model:**

- The key elements of a business model that have not been addressed already.

Tips:

- *The key words here are 'key elements' – many aspects of a business model will already have been covered by your answers to the previous questions*
- *One option is to use the Business Model Canvas[2] template – but only if you wish to do so. If nothing else, it could be used for guidance.*
- *Be sure not to add any (business) confidential information!*

---

1 https://cybersec4europe.eu/wp-content/uploads/2021/02/D4.4-Research-and-Development-Roadmap-2-v3.0-submitted.pdf

2 https://en.wikipedia.org/wiki/Business_Model_Canvas

3 The execution of the methodology

3.1 Collection of partner input

The intention of the survey was to make it brief and painless to complete but to provide sufficient information for the task team to proceed with the next steps. During the early part of 2022, project partners were sent a Powerpoint template with the survey questions listed in Section 2.1. The responses are highlighted at Annex I.

Given the large number of universities and smaller organisations participating in the project, it was anticipated – and which turned out to be the case – that focussing exploitation on commercial outcomes would not be applicable to all universities, the associations and the micro-SMEs. Most of the assets listed featured in three work packages with a strong degree of collaboration and synergy:

- WP3 – Blueprint Research and Design,
- WP5 – Application Demonstrator Use Cases,
- WP7 – Tools.

3.2 Filtering and merging assets

The WP9/T9.5 team, consisting of representatives from ATOS, JAMK, SINTEF and TDL, were then asked to assess all the partner responses and identify twelve candidates to take forward to the next stage. Given that each organisation had their own 'skin in the game', partners were not allowed to vote for their own asset(s).

Inevitably, despite providing a survey-based template, not all responses were of the same quality or length. In some case, it was necessary to go back to a partner to elicit a clearer picture of what they were offering. However overall, partly through everyone's familiarity with or participation in different aspects of the project there was sufficient information to make objective assessments.

Collating the responses from each of the partners gave considerably more than twelve candidate assets. This was resolved through a team consultation as well as in some cases the merging of two assets which were closely aligned in one of the WP3 or WP5 demonstrator use cases. Ultimately, the list was reduced to fourteen assets. As all the owners of the eventual shortlisted assets were to be expected to present in person in Brussels at Momentum!, one organisation dropped out for the reason that they were not able to travel which left thirteen.

No.	Asset / Solution	Partner Organisation	Type	CO
1	AIRE Incident Reporting Platform	Atos Spain S.A.	IND	ES
2	BowTie++ / CORAS	SINTEF	KI	NO
3	CaPe	Engineering Ingegneria Informatica S.p.A	IND	IT
4	CryptoVault	VTT Technical Research Centre of Finland Ltd	IND	FI
5	EBIDS	Consiglio Nazionale delle Ricerche	KI	IT
6	Elastic TEE Subversion - Resilient TEE	NEC Laboratories Europe GmbH	IND	DE

7	Flagship	JAMK University of Applied Sciences	UNI	FI
8	FlexProd	AIT Austrian Institute of Technology GmbH	KI	AT
9	HoneyGen	University of Cyprus	UNI	CY
	Modssl-hmac			
10	MITIGATE	University of Piraeus Research Center	UNI	GR
	HAMSTERS	University of Toulouse III Paul Sabatier - IRIT	UNI	FR
11	OBSIDIAN	Informatique Banque Populaire	IND	FR
	Sharemind	Cybernetica AS	IND	EE
12	RoCe	University of Trento	UNI	IT
13	SecCerts	Masaryk University	UNI	CZ

Table 1: First shortlist of asset candidates

3.3 Questions with weightings and responses

Before handing over the list to the jury, the thirteen asset owners were asked to complete a self-assessment based on the value proposition parameters first outlined in the second exploitation strategy report, D9.19[3]. The self-assessment questions can be found at Annex II. The responses to the initial survey and the self-assessment were collated together into a single spreadsheet, so that all the information pertaining to each of the thirteen assets could be found in a single document.

4 The jury

4.1 Criteria for choosing the jury

After considerable discussion, it was decided that 'less is more' and that, rather than seek five or six jury members, we would be better served by seeking to identify three. The loose criteria for choosing the jury – or as previously referred to the 'exploitation and innovation board' – were ideally:

- an odd number, so as to facilitate decision making in case of differences,
- a balance in terms of background: given the number of academic institutions, the panel should not simply have an industrial or commercial bias, although these perspectives were considered highly important,
- a balance in terms of geographic provenance i.e., jury members should preferably not come from the same country or institution,
- some previous experience with innovation,
- some familiarity with the project but not directly involved.

The initial preference was to choose participants from CyberSec4Europe's associate partners which would fit the last of the criteria listed above.

4.2 Members of the jury

The three experts chosen were:

- **Aida Omerovic (Norway)** , CEO & Founder (STELLOC), Associate Professor (NTNU),

[3] https://cybersec4europe.eu/wp-content/uploads/2022/02/D9.19-Exploitation-Strategies-Report-4.0_submitted.pdf

https://no.linkedin.com/in/aidaomerovic

- **Stelian Brad (Romania)**, Full Professor in Intelligent Robotics and Innovation Engineering, President Cluj IT Cluster; Co-Chair Focus Group Artificial Intelligence EC JRC / European Digital SME Alliance; Head of the Digital Innovation Hub "DIH4Society" (European DIH); President of ETRIA (The European TRIZ Association for Systematic Innovation) https://www.linkedin.com/in/stelian-brad-phd-eng-phd-econ-0162a862/?originalSubdomain=ro
- **Stefan Bumerl (Austria)**, Owner, CRYPTAS it-Security Gmbh, https://www.linkedin.com/in/stefanbumerl/

Due to a completely unforeseen change of circumstance, Aida asked to be recused from the jury just days before the event in Brussels as she was about to take up a position with one of the partners in CyberSec4Europe which she felt would be uncomfortable. Up until that point, Aida had been fully involved in the workings of the jury.

4.3 Jury's process of assets

At the start of the process, the jury were provided with three documents:

- Guidelines, Shortlist, Score Sheet.xlsx
- Scoring Exemplar.xlsx
- Asset Descriptions.xlsx

The guidelines and scoring suggestions were provided to help the jury evaluate the shortlist but it was made clear that they were welcome to choose whichever criteria they saw fit. A nominal score sheet and scoring exemplar was provided – see Annex III – with the same caveat.

The object of the exercise was to filter the thirteen assets presented down to six whose owners would be invited to present at the event in Brussels during the course of the first day of the conference in Brussels. The jury would be asked to sum up their findings and choose two 'winners', based on the performances on the day.

As with the initial internal filtering process, the jury members were asked to make their own individual assessment and to share them separately with TDL's David Goodman who collated the scores into a single spreadsheet. Again, not surprisingly, there was a disparity in the results but a greater synergy than perhaps anyone had expected. During the course of an online meeting and after a long and in-depth discussion, a consensus was arrived at as to which assets should be taken forward.

5 Momentum!

5.1 Background for the audience

In addition to the printed general event agenda for the event, the attendees were given an additional page listing the assets to be presented and an explanatory text to provide the context for the process:

> *"CyberSec4Europe's legacy beyond the end of the project can be seen in the results of the work carried out by all partners over the past four years.*
>
> *In a series of reports, we highlighted the individual and joint exploitation and innovation plans, involving assets and solutions across the different project domains, ranging from, for example, maritime transport to the Flagship cyber range challenges.*
>
> *As CyberSec4Europe comprises diverse organisations – from software vendors, commercial businesses, universities, research institutes, SMEs, legal and consultancy firms to not-for-*

profit organisations – each type of partner has evolved exploitation strategies in line with their own needs and opportunities. And we celebrate each and every one!

At Momentum! we are showcasing six of the key exploitable assets and solutions over the course of the first day. As difficult as it was to narrow down the results to six, our independent jury members – Stelian Brad from Cluj IT Cluster and Stefan Bumerl of CRYPTAS it-Security GmbH – will identify just two to go forward to the European Commission's Horizon Results Platform."

5.2 The six presentations

The six assets and their owner presenters are listed below together with links to the presentations. To watch and listen to the presenters, these can be found in the video recording of the first day of Momentum![4]

1. **OBSIDIAN Sharemind MPC Extensions**[5]
   Improving the fight against banking fraud ensuring GDPR compliance and banking secrecy
   Liina Kamm, Cybernetica AS
   (Authors: Liina Kamm, Baldur Kubo, Cybernetica; Mederic Collas, Informatique Banque Populaire)
2. **Flagship**[6]
   A realistic cyber security exercise using a feature rich live cyber range
   Jani Päijänen, JAMK
3. **Replica TEE**[7]
   Enabling Seamless Replication of SGX Enclaves in the Cloud
   Alessandro Sforzin, NEC Laboratories Europe GmbH
   (Authors: Claudio Soriente, Ghassan Karame, Wenting Li, Sergey Fedorov, NEC)
4. **CaPe**[8]
   A consent-based personal data suite to manage personal data in compliance with the GDPR
   Vincenzo Savarino, Engineering Ingegneria Informatica S.p.A.
5. **EBIDS**[9] (An ensemble-based intrusion detection system)
   Pushing Intelligence in Threat Sharing Platforms
   Giuseppe Manco, Consiglio Nazionale delle Ricerche (CNR)
6. **SecCerts: datamining security certification documents**[10]
   An analysis tool for certificates of security products
   Petr Švenda, Masaryk University

The speakers were given 15 minutes each, which included time for questions and answers. They were told to imagine that they were presenting to a set of potential investors who already were quite familiar with the description and strengths of their solutions but were looking for that something special that would differentiate them from the others and had a credible opportunity in a competitive marketplace.

4 https://www.youtube.com/watch?v=8Fo7PfX2lNA
5 https://youtu.be/mC0totxhxkk
6 https://youtu.be/GJV0mZRbg-0
7 https://youtu.be/ouG127CaDUU
8 https://youtu.be/LkocGEaO-6E
9 https://youtu.be/johb8bUyrlc
10 https://youtu.be/nyMUchrdCbs

The two jurors were able to question the presenters at the end of each presentation and also took the opportunity to discuss with them during the coffee and lunch breaks.

5.3 The jury summing up

At the beginning of the second day of the summit event, Stelian and Stefan together gave a fulsome description of their approach to the task of adjudication. Here is a more or less transcript of their summing up of the process they undertook and their views on innovation that informed their decisions. Their description is also available online[11].

Stefan: It started a couple of weeks back when David asked for someone external to look at the efforts of the 43 partners and I asked how much time will be necessary for so many results. I was not part of the project, and they were about many areas of expertise that I had no personal core expertise of, so I expected it to be a bit challenging. We had luck – David and his team did a real good job to take the total number of assets and reduced the shortlist to 13 topics that we should look a little deeper into it.

During the first round we really wanted to create a formal process, to create a number of criteria to use to score the assets.

Based on the answers provided in advance we were able to look at criteria such as the needs and challenges, the business model, the network, the market etc, the project dividend. All of this information was gathered and provided to us in advance of the judging. To go ahead, we originally had three evaluators, and to have a common ranking we had an extensive points system based on sustainability, technology market readiness level, policy priorities they address, reusability, affordability, the power of communities and the green aspect.

We narrowed it down to six finalists, and it was really interesting to see in more detail what the projects were really about when presented here – although it didn't make it easier for us!

The goal however was not to stick to simply numbers and points, and we had a lot of discussion about all of the original points we had scored. We tried to look at our role as potential investors.

Stelian: Firstly, I would like to congratulate all the finalists because in our view you did a great job. We have seen the implications of all the teams and from this perspective all are winners. Difficult to compare apples with pears for as you have seen each project was focussed on a different area. We looked at each one's innovation readiness level (which is different from market readiness): every detail of the capability of transferring to be adopted by the market is important. From this perspective I'd like to introduce these projections of innovation for you and I hope you will all understand I make an assessment of your work where you have strengths and where you might have to improve. Maybe from this point of view, you will learn how to reposition yourselves.

About technology readiness it is something that has been introduced, in the pre-selection phase. What was very important to the jury was to differentiate. Both Stefan and I had experience in the market of related products and it is a highly competitive space.

The capacity to differentiate by strategy, by value proposition, by IP (intellectual property) readiness level, from similar technologies, or substitute technologies in the market – we have related experience in these highly competitive markets. The capacity to provide blue ocean space to create radical innovation or disruptive innovation is important. We look where there were gaps in the market that need to be filled with something because, if an ecosystem is not functional because it has a gap, that creates a problem for all of us. This was an important criterion.

[11] https://youtu.be/XfvKR09QaXA?t=1373

Also we had to look at other criteria such as the IP readiness level – in some cases the patents. Patents are OK but they have a value associated with certain business models. Otherwise, they have no value. Here, I have to make a comment about the weakness of the European landscape We are encouraged by the Commission to fund these projects and push them to publish their results because once published they become public good for all of us, not just Europeans, but the world. However, I feel aligned with Professor Bart Preneel's comments yesterday that sometimes in our European innovation landscape is difficult – the businesses which are driven by radical, disruptive technologies we have to take care how we tackle the intellectual property e.g., the example of DARPA.

In terms of market readiness, some of the projects were easier to be introduced, some were needing more work to educate the market for adoption. Sometimes we have to go deeper to understand the behaviours of the market to adopt – and sometimes we have to care for the end users. What will be done with the results further? We need the projects to highlight this and explain what they want to do further. We need to see commitment to move forward rather than just an intellectual exercise to demonstrate professionalism or creativity, and, when seeking capital for finance, we expect to see some more sense of this from the project presenters. Something about the readiness of the company, something about the scalability. We tried to interact with the presenters to find out more information. Also, the capacity to deploy in different locations – that's an important issue. These factors shaped our final decisions.

Some projects are ready now to be in the market, and some need more attention and maybe more encouragement, but they have a huge potential in the cybersecurity landscape. These criteria together shaped the decisions on the winners.

Stefan: We had partners from industry and some from academia and we wondered if this should also shape our decision because of the different backgrounds they originated from. My expectation was there should be a gap between them, but we decided to give two awards which meant we could get round this problem. We decided to give an award to one from each category.

Announcement!

Stefan: The first winner is a clever idea, a new idea – a new idea that makes you think, why isn't that standard out there, because in supply chains, in terms of software sub-components, you need to have a way to address the challenge. You know you have on the one hand commercial supply chains contributing to any product however the reality is that you have a lot of sub-contractors and actually really don't know how many components that are really imbedded in the product which can affect them. That kind of process you need to map these CVD (coordinated vulnerability disclosure) reports on a daily basis and how they are affecting us – if you are not a vendor yourself and you are working with many vendors you cannot understand how faults might be affecting you: it may not be good enough to rely on their reports. SecCerts had that idea and created the mapping - whenever you identify something broken you can see what else needs to be changed. This idea has a lot of potential and I would apply that kind of methodology to the reports coming out of certification, if you are using open source you are forced to mention in the documentation to see what is claimed to be embedded. To have a quick open source library to see what is embedded. So the first winner is SecCerts!

Stelian: I would also like to add something – apart from the name which was interesting, but … they open a new space of consolidating our cyber resilience in Europe. Because if we move a little bit forward to think about innovation, it is not always the most important thing but consolidation of the business environment is also important. We can align these with the forthcoming rights enshrined in the Cyber Resilience Acts and align these with the strong customer rights.

The trophy is awarded!

Stelian: It's my turn to introduce the second winner. Also because the asset is a niche product: that is, it addresses a niche area which is very important and also it's very important the passion you transmit in the public about the product. The courage to demonstrate the uniqueness – something that is difficult to replicate by anyone to consolidate European cybersecurity.

To contribute to the resilience of the cybersecurity of Europe was one way the product fulfils this requirement.

Yesterday we interrogated this winner a lot because we realised that they are capable of creating an automatic system that will strengthen the capacity of firewalls and other devices in order to identify any suspicious behaviours. You need to work more on promotion of this product.

Stefan: We have advice that you should look at promoting this product to vendors within the OT field because you have quite different systems in the OT field your technology could be adaptive enough to cope there.

The second trophy is awarded to EBIDS!

Antonio Skarmeta, the session moderator, thanked the jury, observing how fundamental it is to have external views on the work we do and complimented them on having done a very good job!

Figure 1: Stelian describing the jurors' approach to innovation

Figure 2: Stefan announcing one of the winners

5.4 The winners

Figure 3: Stelian and Stefan with Vashek Matyas, receiving the trophy on behalf of SecCerts

Figure 4: Stelian and Stefan with Giuseppe Manco, with his trophy for EBIDS

6 Recommendations for a market-based approach to the exploitation of project results

The following analysis demonstrates approaches to utilising market knowledge to optimise CyberSec4Europe's (and other projects') exploitation of project results.

The cybersecurity market has several shortcomings, such as a specific type of information asymmetry, a situation where the supply side has more or better information than the demand side, something also known as *'the market for lemons'* [12].

Opportunistic behaviour leads to market failures. There are two major types of opportunistic behaviour: adverse selection and moral hazard. In the first case, supply side stakeholders in cybersecurity are better informed about trustworthiness of their own products, while in the second case they might even take risky actions (e.g., shortening testing or saving costs on assurance).

The first buyers of cybersecurity solutions take a higher risk as it might take them longer to deploy a new solution, there might not be any broad training available, while support and evolutive maintenance might still be at an early stage of maturity. As security and quality assessments, or benchmarking of similar cybersecurity solutions, are difficult to perform for the buyer, there might be incentives for the supply side to inflate the benefits of their product, such as coverage, effectiveness or efficiency. The side effect might be that promising cybersecurity solutions never pass *'the valley of death'* [13] and might disappear from the market. Another distortion is introduced by the strong influence of market analyst reports, many of which are not considering EU cybersecurity solutions since these do not meet the minimum sales required to be included in a market report. Finally, strong preferences for national products or even for proven US or Israeli cybersecurity products might create bias.

A new cybersecurity market model should be based on new incentives for both supply and demand side, and should consider enablers such as independent assessments, labels and certifications.

The transparent assessment of claimed properties of cybersecurity solutions (e.g., coverage, ease of integration or effectiveness) would enable buyers to make optimised purchasing decisions and would give vendors stronger incentives to deliver technology with improved efficacy. “Try before buy” is already used by many vendors, but a further step is needed in relation to assessment. Transparency and independent assessment would also help new innovations from start-ups to faster penetration of the market. It could also help in “test before invest” schemes for cybersecurity investors who are not experts in technology.

This idea obviously brings some important challenges with it. Common assessment standards need to be created and/or reused (e.g., ENISA EUCC, roughly based on existing international schemes such as Common Criteria). Assessment independence and monitoring vendor-linked profit incentives is another issue. The fair distribution of assessment costs between stakeholders, with a role for government as the facilitator, and research institutes that might play a role in low-cost assessments, is another challenge. Finally, monitoring of benefits and market evolution also presents related challenges. We assume that there would be a change of decision-making process on the demand side, and that there would be an increase of trust in the whole ecosystem, but these benefits are difficult to verify. Even more difficult would be the attribution of benefits, such as cybersecurity risk reduction, due to these assessments, transparency and increased knowledge about cybersecurity products and solutions.

We present this market analysis so as to look at several ways to optimise CyberSec4Europe's exploitation of project results.

---

[12] Akerlof, George A. (1970). "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism". *Quarterly Journal of Economics*. The MIT Press. 84 (3): 488–500. doi:10.2307/1879431. JSTOR 1879431.

[13] https://www.investopedia.com/terms/d/death-valley-curve.asp

6.1 Incorporate market issues next to customer needs into the exploitation process

Market attractiveness is not the same as customer need. The less specific a customer need is, the more attractive a market can be, but the mapping of general versus specific pains and gains is not straightforward. In general, the more attractive a solution is for the market, the more customisation might be needed and vice versa.

Stakeholder analysis goes further than only looking at the supply and demand side, or inclusion of other external stakeholders, such as policymakers, certification and standardisation bodies or legal organisations. It needs to consider the current level of maturity, cultural or market adoption differences, the size of organisations, risk-appetite and many other parameters.

Collaboration and cooperation can be analysed from several perspectives, from co-design of a solution (e.g., through a research project) to service co-delivery (e.g., coordinated response from security teams from different Member States). Less visible issues and challenges, such as SME networking, where supply-side SMEs could complement each other, should also be investigated from a wider economic angle.

Besides market readiness and attractiveness, other drivers should be considered in the economic models for cybersecurity ecosystem, including efficiency, avoiding vendor lock-in or the interplay between economics and digital sovereignty. Value network reconfiguration or government intervention through policy might be needed when addressing technology acceptance or user adoption. Growth and evolution of an ecosystem, and the motivation for diverse stakeholders to collaborate and cooperate should also be analysed.

Open-source communities or industrial initiatives (e.g., GAIA-X, ECSO, FIWARE, Digital Innovation Hubs) could have their role in the adoption of CyberSec4Europe results, further development and the sustainability the ecosystem. These exploitation paths adopt various forms, depending on the context, including IP licensing, contracted work, transferring technology, expert and consultancy services, permanent cooperation structures, associations or sub-structures, spin-off and start-up companies supported by ecosystem incubators. We might expect that the final exploitation in a cybersecurity ecosystem configuration would strongly depend on the choice of a governance model and the pool of funds and equipment available *(see figure 5).*

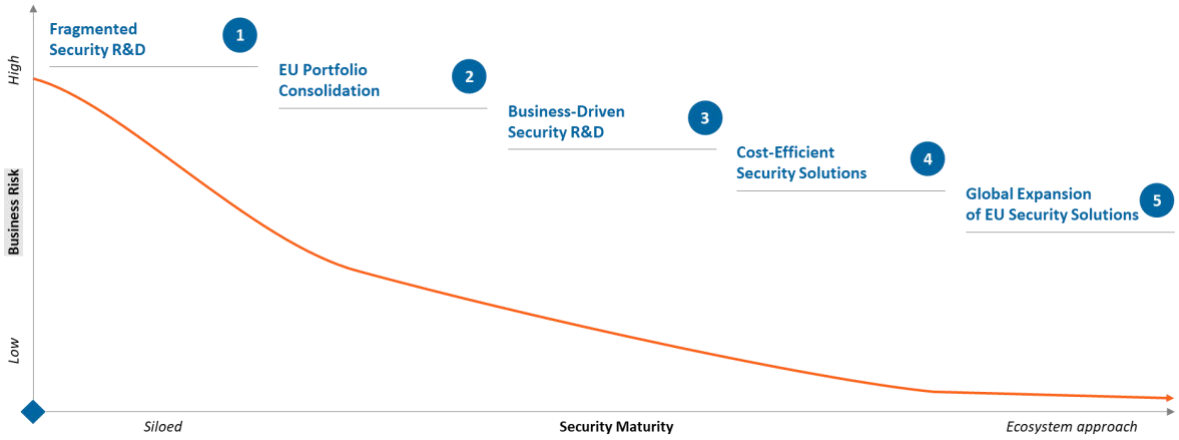

Figure 5: Business risk vs security maturity

From a pan-European perspective, solutions are not only supposed to be reused, or used in a collaborative and cooperative manner, but also evaluated by peers from the same target audience, as it was done at Momentum! in December 2022. Failure to synchronise activities across Member States, pertinent to the national coordination centre tier of this ecosystem (NCC) would cause excess effort put into reinventing the wheel, too much overhead activity, additional challenges of benchmarking, interoperability, matching and reconfiguration, with the possibility of missing compatible value propositions and others.

6.2 Allocate resources to those results that make the most impact with a similar budget

Balancing the risk and reward for new innovations is not easy. There are many incremental innovations, especially in EU projects and it is difficult to evaluate and prioritise new projects or actions. However, it would be fair to redistribute resources to create the best value, in terms of economic, societal and policy impact for money that has been invested in research.

When it comes to technology maturation or market maturation paths, some strategies from pre-commercial procurement might be used *(see figure 6)*. Here the process is divided into phases when a potential customer is ready to buy one of the results based on a research project prototype. While several alternative prototypes compete during the conceptual phase, a customer decides on which solutions are to be selected for further investment, until one prototype is built for integration into an operational environment. A dossier describing project results or a whole portfolio of results could be prepared describing as many details as possible related to the specific use case or business opportunity, including draft financial conditions, list of concerned parties and any other information that the demand side customer considers important to realise the opportunity. In case the chosen solution could be easily replicable, arrangements could include some sort of partnership or discount, as well as pre-investment agreements.

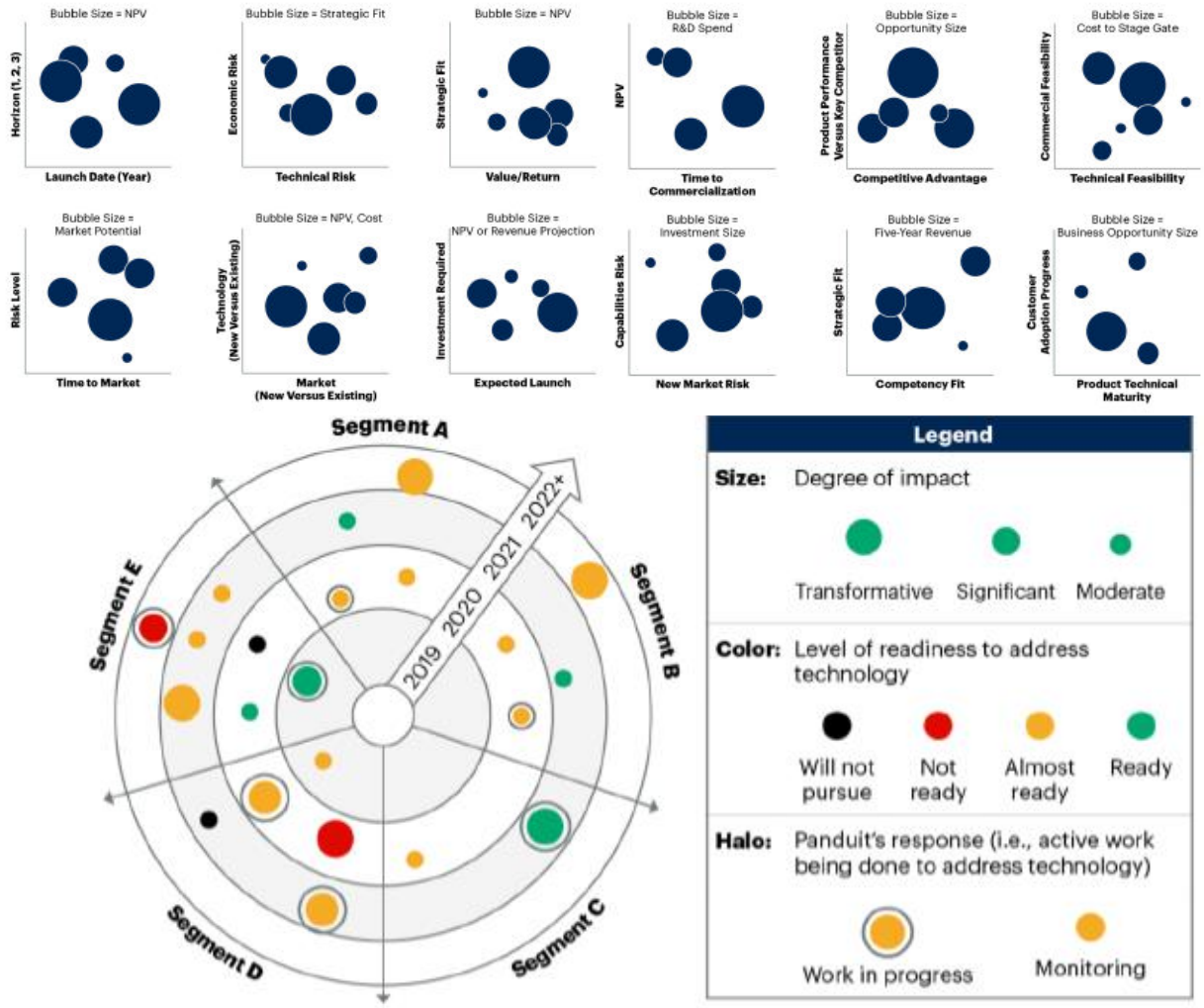

Figure 6: Visualisations of different exploitable results is an important help in decision making about the further investment, (Based on a few examples from Gartner report)

6.3 Use common building blocks and grow portfolio around them

The building blocks are needed to make a (set of) EU cybersecurity reference architectures that would describe an ecosystem's cybersecurity capabilities and assets. A portfolio should also describe integration with existing platforms and other enablers. We can find an example in deliverable D3.1[14] that outlines the goals and scope of the reference framework behind a proof-of-concept demonstrator. It discusses the architecture, functionalities and assets used for the cooperation with threat intelligence services and the deployment of adaptive honeypots. The MISP threat intelligence platform is just one example of a common EU building block around which many additional assets can be built. The Microsoft Intelligent Security Association (MISA)[15] is an example of an ecosystem entered in a single vendor with many independent software vendors (ISV) and managed security service providers (MSSP) that have integrated their solutions with Microsoft's security technology. While it is unlikely that the EU could have one single security information and event management (SIEM) or intrusion detection system (IDS) solution as a building block, there are open-source initiatives, such as COSSAS[16], that harvest and grow cybersecurity assets from EU projects or other efforts. Another example of an EU initiative that started with generic enablers and building blocks is FIWARE[17].

6.4 Link to cybersecurity ecosystem governance

There are several challenges when it comes to the ecosystem approach to exploitation. One is the tyranny of the majority, whether this is a research (sub-)community, or some other group around a specific interest. Similar holds for the challenge of the organised minority, that could manage to promote specific solutions or topics because of the lack of interest of others. Finally, we should not forget rational ignorance from opportunity seekers – those that do not have a specific cybersecurity background, but promote topics and solutions for specific reasons. Polycentric governance, like the one described in CyberSec4Europe's work package on governance (WP2), could deal with these challenges through incentives management (e.g., incentives to participate in a jury for selection of the most innovative project results), or more efficient information dissemination. Individuals should be rewarded (either in transferable tokens or in a reputation score which is not transferable) not only by their tangible contributions to the ecosystem (e.g., development of an asset), but also by their participation in particular processes, such as exploitation (e.g., filtering and selection of the most innovative assets, organisation of events). This will be an important step towards a spontaneous decentralised collaborative ecosystem that could possibly use distributed ledger technologies in the future to support this incentive structure.

7 Conclusion: 'Everyone's a winner'

Although the culmination of the latter phase of the project's exploitation activity was the nomination of two winners based on the evaluation of two external independent reviewers, it was consistently asserted that everyone, every organisation that has worked so industriously over the last four years in CyberSec4Europe and generated such high quality results, all of them are winners and will be listed in posterity on the project website.

Having said that the two winning entries, SecCerts and EBIDS, will be put forward to the H2020 Results Platform on behalf of CyberSec4Europe.

---

14 https://cybersec4europe.eu/wp-content/uploads/2020/06/D3.1-Handbook-v2.0-submitted-1.pdf
15 https://www.microsoft.com/en-us/security/business/intelligent-security-association
16 https://cossas-project.org/
17 https://www.fiware.org/

In addition, TDL is intending to track the evolution of the assets generated by the project over the next two-three years.

Annex A: Partner assets

1. Associations

OASC	No response
TDL	New and enhanced areas of research and collaboration

2. Banking

ABI Lab	No asset
BBVA	No response (collaboration with ISPS)
i-BP	OBSIDIAN (Open Banking Sensitive Data Sharing Network For Europe)
ISPS	Incident reporting platform

3. Government

GEN	Collaboration with ENG

4. Industry

ATOS	SPEIDI (Service Provider eIdentity Infrastructure) TIE (Threat Intelligence Integrator) DANS (Data Anonymisation Service) AIRE (Atos Incident Reporting Engine) FE2MED (Functional Encryption To Medical Data)
DAWEX	eIDAS – FranceConnect
ENG	RATING (Risk Assessment Tool for Integrated Governance) TO4SEE (Assessment Tools for Social Engineering Exposure) CaPe (Consent-based Personal Data Suite)
NEC	Blockchain Platform Elastic TEE (Trusted Execution Environment) Subversion-resilient TEE
SIE	Workflow Compliance Assurance Workflow Compliance Accountability
VTT	CryptoVault EEVEHAC (End-to-End Visualizably Encrypted and Human Authenticated Channel)

5. Research Institutes

AIT	FlexProd
CNR	EBIDS (Ensemble Based Intrusion Detection System) UASD (Unauthorized App Store Discovery) GENERAL_D (GDPR-based Enforcement of Personal Data) SYSVER
FORTH	Dissemination, publications, expertise, future projects, etc
SINTEF	BowTie++ & CORAS PKI demonstrator

6. Legal firms

TLEX	Development of Timelex Cybersecurity Helpdesk Expansion of legal work in cybersecurity-related innovation actions Provision of legal assistance to clients

7. Micro-SMEs

CONCEPT	No assets
VAF	No assets

8. SMEs

ARCH	No asset
CYBER	Sharemind PLEAK (Privacy Leakage Analysis Tools) Secure maritime communication prototype Certification assistant
ICITA	No asset

9. Universities (with exploitable assets)

BRNO	Cyber Sandbox Creator SCRUTINY SecCerts
CTI	PP-SSI Management
JAMK	Flagship
NTNU	Guidelines for monitoring and enhancement of societal security awareness
UCD	Adaptive Authentication
UCY	EvilText HoneyGen Modssi-hmac
UM	GDPR guidelines
UMA	HADES JUDAS (JSON Users and Device Analysis Tool) PMEC (Privacy Manager for IoT data based on Edge Computing Technologies)
UMU	dp-ABC or ppIdM pp-CTI
UNILU	Privacy-by-design for highly-sensitive data (genomic data)
UNITN	RoCe (Risk of Compromise Estimation) Educational Framework
UPRC	MITIGATE (Evidence-driven Maritime Supply Chain Risk Assessment)
UPS-IRIT	HAMSTERS (Human – centered Assessment and Modelling to Support Task Engineering for Resilient Systems) HAMSTERS Extended

10. Universities (without exploitable assets)

C3P	Improvements to assets
DTU	Internal developments
GUF	Educational courses Research proposals
KAU	Internal and collaborative development
KUL	Scientific dissemination, teaching and future research
POLITO	No response
TUD	Improvements to university courses

Annex B: Value proposition questions

A. Project Dividend

- Completely conceived and developed within CyberSec4Europe
- Major improvement on an existing asset
- Minor improvements on an existing asset
- Major addition to existing open source components: for example, new modules, replacement of libraries etc
- Minor improvements on existing open source components: for example, customisation, integration, etc
- Other (please comment)

B. Market traction

- No contacts with end users
- We are the end user
- We work on a pilot with an end user organisation in the consortium
- An end user organisation outside the consortium is consulted for post-project collaboration
- An end user organisation outside the consortium is working with us and adopting asset
- Other (please comment)

C. Exploitation plan

- Technology transfer from academy to industry
- Enhancement of an existing product,
- Contribution to open source community
- Spin-off/start-up
- Maturing an existing technology
- Commercialisation of the new products/services
- Input and support to policy
- Generation of the new knowledge
- Research collaboration and networking
- Further internal research

D. Existing competition and alternatives

- No competitors that we are aware of
- Some research prototypes exist
- Emerging market with few commercial offerings
- Well established market segment with similar offerings

E. Technology (and market) readiness levels

- TRL1
- TRL2
- TRL3
- TRL4
- TRL5
- TRL6
- TRL7
- TRL8
- TRL9

F. Novelty or innovation levels

- Several research papers describing beyond technological state of the art have been published
- Acknowledged as highly innovative by a third party (e.g., Innovation Radar)

- Considered highly innovative technology by the owners of asset
- Considered as innovative in non-technological areas (for example, in terms of model, service provision etc)
- Other (please comment)

G. Affordability

- Open source
- As a service
- Proprietary fixed fee licence
- Under discussion/review
- Not applicable

H. Sustainability

- Clear plans for development and/or maintenance beyond the end of the project
- Availability of information about future investment
- Not applicable
- Other (please comment)

I. Policy priority

- Alignment with EU policies is important
- Not applicable

J. Green credentials

- The asset benefits climate
- The asset relies on a disproportionate use of electric power
- The asset contributes to other types of credentials; for example, EU cybersecurity certification or other policy objectives.
- Not applicable

K. Power of community

- Builds on the idea of the strength of the positive impact of networking
- What might be called the “community exploitation” of a shared but separate endeavour, such as threat intelligence sharing.
- A perceived increase in value as an active member of a consortium where externalities (for example, a certification scheme) play a role.
- Not applicable
- Other (please comment)

Annex C: Scoring exemplar

		Suggested scoring		Asset / Solution
		Sub-limits	Totals	Widget
A	Project dividend		15	
	Completely conceived and developed within CyberSec4Europe	*15*		
	Major improvement over an existing asset	*10*		10
	Minor improvements over an existing asset	*5*		
	Major addition to an existing open source components *(for example, new modules, replacement of libraries etc)*	*10*		
	Minor improvements over an existing open source *(for example, customisation, integration, etc)*	*5*		
	Other	*15*		
B	Market traction		15	
	No contacts with end users	*5*		
	We are the end user	*10*		
	We work on a pilot with an end user organisation in the consortium	*10*		
	An end user organisation outside the consortium is consulted for post-project collaboration	*10*		10
	An end user organisation outside the consortium is working with us and adopting asset	*15*		
	Other	*15*		
C	Exploitation plan		15	
	Technology transfer from academy to industry	*15*		
	Enhancement of an existing product,	*5*		
	Contribution to open source community	*10*		
	Spin-off/start-up	*10*		
	Maturing an existing technology	*5*		3

	Commercialisation of the new products/services	*10*			
	Input and support to policy	*5*			
	Generation of the new knowledge	*5*			
	Research collaboration and networking	*5*			
	Further internal research	*5*			
D	Existing competition and alternatives		10		
	(From 1 to 10, where 1 is market segment already saturated and 10 is no competition)				
	No competitors that we are aware of	*10*			
	Some research prototypes exist	*5*			
	Emerging market with few commercial offerings	*10*			5
	Well established market segment with similar offerings	*5*			
E	Technology and market readiness levels		10		
	(From 1 to 10)				6
F	Novelty or innovation levels		10		
	Several research papers describing beyond technological state of the art have been published	*10*			
	Acknowledged as highly innovative by a third party (e.g., Innovation Radar)	*10*			
	Considered highly innovative technology by the owners of asset	*10*			
	Considered as innovative in non-technological areas (for example, in terms of model, service provision etc)	*10*			7
	Other	*10*			
G	Affordability		10		
	Open source	*10*			10
	As a service	*5*			
	Proprietary fixed fee licence	*3*			
	Under discussion/review	*3*			
	Not applicable	*5*			

H	Sustainability		10	
	(For the evolution or maintenance of code, beyond the initial go-to-market outlay)			
	Clear plans for development and/or maintenance beyond the end of the project	*10*		
	Availability of information about future investment	*10*		
	Not applicable	*5*		3
	Other	*10*		
I	Policy priority		5	
	Alignment with EU policies is important	*5*		
	Not applicable			0
J	Green credentials		5	
	The asset benefits climate	*5*		
	The asset relies on a disproportionate use of electric power	*0*		
	The asset contributes to other types of credentials; for example, EU cybersecurity certification or other policy objectives.	*5*		
	Not applicable	*0*		0
K	Power of community		10	
	Builds on the idea of the strength of the positive impact of networking	*10*		5
	What might be called the “community exploitation” of a shared but separate endeavour, such as threat intelligence sharing.	*10*		
	A perceived increase in value as an active member of a consortium where externalities (for example, a certification scheme) play a role.	*10*		
	Not applicable	*0*		
	Other	*10*		
	Total:		**100**	**59**