



# SPARTA

## D10.5 Sustainable Exploitation Documents

<b>Project number</b>	830892
<b>Project acronym</b>	SPARTA
<b>Project title</b>	Strategic programs for advanced research and technology in Europe
<b>Start date of the project</b>	1 <sup>st</sup> February, 2019
<b>Duration</b>	41 months
<b>Programme</b>	H2020-SU-ICT-2018-2020

<b>Deliverable type</b>	Report
<b>Deliverable reference number</b>	SU-ICT-03-830892 / D10.5 / V1.0
<b>Work package contributing to the deliverable</b>	WP10
<b>Due date</b>	June 2022 – M41
<b>Actual submission date</b>	12 <sup>th</sup> July, 2022

<b>Responsible organisation</b>	SMILE
<b>Editor</b>	Kadri Bussov
<b>Dissemination level</b>	PU
<b>Revision</b>	V1.0

<b>Abstract</b>	The Exploitation Roadmap is designed to help in streamlining exploitation activities for SPARTA partners based on the TRL-s of the developed technology. Different levels of TRL require different considerations in regarding exploitation and IPR activities. The D10.5 creates a practical toolbox in considering exploitation activities within SPARTA.
<b>Keywords</b>	Exploitation, open-source software, licensing, technology readiness, TRL, commercial readiness, CRI



**Editor**

Kadri Bussov (SMILE)

**Contributors** (ordered according to beneficiary numbers)

Henrik Plate (SAP)

Kadri Bussov, Julie Hallinger, Tun Hirt, Bertrand Lathoud (SMILE)

**Reviewers** (ordered according to beneficiary numbers)

Daniel Meyer (UBO)

Artsiom Yautsiukhin (CNR)

**Disclaimer**

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

## Executive Summary

This deliverable is aimed at presenting Sustainable Exploitation Tools developed under SPARTA WP10. SPARTA WP10 was tasked in leading the Exploitation track within the project and to oversee exploitation activities such as licensing of results, granting licenses to third parties and development of spin-off start-ups. The main challenge in achieving the stated goals have been in bridging the gap between academia and entrepreneurship within the SPARTA project. The D10.5 provides methodological tools in the form of Exploitation Roadmap and legal licensing support to provide help in managing the transfer of results from SPARTA research work packages to potential commercial undertakings. The second part of the D10.5 focuses on the practical activities on commercial exploitation already conducted during the 41 months of the project. Practical activities are analyzed and recommendations and lessons learned are provided for any future continuation of exploitation activities.

The Exploitation Roadmap presented in this D10.5 is built on the principles of TRL system developed by NASA. The Exploitation Roadmap uses TRL as a technical indicator that triggers commercial and intellectual property activities. The Exploitation Roadmap creates a practical tool to connect intellectual property to ownership and ownership to exploitation. The Exploitation Hackathons and Startup Mentorships conducted under WP10 have provided information on the practical technology transfer methods from a project to external teams. The Exploitation Hackathons provided the teams with open-source results from the SPARTA project and industry mentors. The teams were then tasked to develop business models within 48-hours and competed for an opportunity to participate in a follow-up Startup Mentorship supervised by SPARTA partner. The ability to conduct two consecutive Hackathons and Mentorships allowed for a thorough lessons learned analysis and recommendations that are provided in Chapter 4.

# Table of Content

<b>Chapter 1</b>	<b>Introduction .....</b>	<b>1</b>
<b>Chapter 2</b>	<b>Exploitation Roadmap .....</b>	<b>2</b>
2.1	The Definition of Exploitation .....	2
2.2	Technology Readiness Level (TRL) in cybersecurity innovation .....	4
2.2.1	High-readiness of technology and low-innovation context.....	5
2.2.2	Low-readiness of technology and high-innovation potential context.....	6
2.2.3	High-readiness of technology and high-innovation potential context.....	7
2.3	Commercial and non-commercial Exploitation .....	8
2.3.1	TRL in commercial exploitation .....	8
2.3.2	TRL in non-commercial exploitation.....	9
2.4	RAMP as a tool for non-commercial exploitation .....	9
<b>Chapter 3</b>	<b>Legal Tools for Exploitation .....</b>	<b>11</b>
3.1	Choosing open-source license .....	11
3.2	Exploitation and data protection .....	12
<b>Chapter 4</b>	<b>Support to Exploitation Activities .....</b>	<b>15</b>
4.1	Summary of the Exploitation Workshop .....	15
4.2	Exploitation Hackathons .....	17
4.2.1	Exploitation Hackathon, January 2022.....	17
4.2.2	Cross-Pilot Exploitation Hackathon, May 2022 .....	19
4.2.3	Lessons Learned .....	23
4.2.4	Proposed Framework Approach for Business Development Hackathon for open-source... .....	25
4.3	SPARTA Start-up Mentorship .....	26
4.3.1	Summary of the Startup Mentorship I .....	26
4.3.2	Preparation of the Startup Mentorship II .....	26
<b>Chapter 5</b>	<b>Exploitation activities related to Open-source Supply Chains (SAP).....</b>	<b>28</b>
5.1	Open-source Programs in the Industry .....	28
5.1.1	Google.....	29
5.1.2	GitLab.....	29
5.1.3	Zalando .....	30
5.1.4	Yahoo.....	30
5.1.5	FINOS Reference FOSS Policy for Financial Services Institutions .....	30
5.1.6	Summary.....	31
5.2	Regulatory Initiatives, Open Standards and Certification Schemes .....	31
5.2.1	EU Cybersecurity Certification Scheme for Cloud Services (EUCS) .....	32
5.2.2	White House Executive Order from May 12, 2021 .....	32
5.2.3	OWASP Software Component Verification Standard .....	32
5.2.4	Supply Chain Levels for Software Artifacts (SLSA).....	33
5.2.5	Know, Prevent, Fix: A framework for shifting the discussion around vulnerabilities in open source .....	33
5.3	The different results of SPARTA.....	34
5.3.1	BuildWatch (UBO) .....	34
5.3.2	Backstabber's Knife Collection (UBO, SAP).....	34
5.3.3	Interactive Attack Tree (SAP) .....	35
5.3.4	Eclipse Steady (SAP) .....	35
5.3.5	Project KB (SAP) .....	36
5.3.6	VulnEx (UKON) .....	36



**Chapter 6 Conclusion ..... 37**

**Chapter 7 List of Abbreviations..... 38**

**Chapter 8 Bibliography ..... 39**

**Chapter 9 Annexes ..... 42**

9.1 Annex 1: Exploitation Roadmap: Technology Readiness Level (TRL), Commercial Readiness Index (CRI) and Intellectual Property Rights (IPR) Correspondence Table ..... 42

9.2 Annex 2: TRL Assessment Questionnaire ..... 45

9.3 Annex 3: IPR and Market Maturity Assessment Roadmap ..... 48

9.4 Annex 4: CRI and Business Model Assessment Roadmap..... 49

9.5 Annex 5: Exploitation support documentation in RAMP ..... 51

## List of Figures

Figure 1: Different assessment tools available on the RAMP platform. ....	10
Figure 2: The scale of intellectual property measures in relation to their protectiveness.....	12
Figure 3: Protectiveness comparison table for permissive and copyleft open-source license. ....	12
Figure 4: Questions of the registration form and the repartition of the answers .....	16
Figure 5: Mapping of security policies to project categories. ....	30
Figure 6: SLSA Supply Chain Threats (Copyright 2021 The Linux Foundation). ....	33
Figure 7: Eclipse Steady in TODO Group's OSPO landscape.....	36
Figure 8: Step by step on how to use the Exploitation Roadmap in Annexes 1 - 4. ....	42

## List of Tables

Table 1: Exploitation Hackathon I teams, solutions and used open-source tools.....	18
Table 2: Open-Source tools from SPARTA used in the Exploitation Hackathon I.....	19
Table 3: Participating teams, their solutions and used open-source tools. ....	20
Table 4: Open-Source tools from SPARTA used in the Exploitation Hackathon II.....	21
Table 5: Open-Source tools from CONCORDIA used in the Exploitation Hackathon II .....	22
Table 6: Open-Source tools from ECHO used in the Exploitation Hackathon II.....	22
Table 7: Proposed Schedule for Exploitation Hackathon activities .....	26

## Chapter 1 Introduction

Exploiting results of research activities has become one of the corner-stones in innovation driven economy. However, developing a practical approach in exploitation activities and tools is a complicated task. There is an inherent gap between research activities and commercial activities. One that is also set in the core mission of either activity. Commercial and exploitation activities require a vastly different mindset in approaching technical results than research activities do. Therefore, the tasks under WP10 and D10.5. took a more experimental and practical approach in understanding and developing tools and activities that would grant practical and usable ways to exploit research activities from the SPARTA research WPs. Special consideration was given to finding ways to exploit open-source results.

The deliverable D10.5. has reviewed several approaches to develop exploitation tools. Chapters 2 and 3 explore methodological approach to understanding exploitation. Chapter 2 will mainly look at innovation context and its relationship to the use of technology readiness levels (TRL). The Chapter will describe the legal tools for open-source licensing. Chapter 2 furthermore introduces a TRL-based Exploitation Roadmap for understanding the relationship of TRL to the commercial readiness and intellectual property requirements for the technology. This relationship is based on the understanding that certain activities such as publishing a peer-reviewed article on a technical solution will prevent future trademarking of such a solution as the information has been made public before trademark has been applied for. This, in turn, will hinder potential exploitation activities for the solution. The Exploitation Roadmap that is more detail presented in Annex 1 with TRL and CRI assessment questions in Annexes 2 – 4, explains how TRL, commercial readiness and intellectual property interact and depend on each other.

Chapters 4 and 5 will provide a practical approach with examples to plan exploitation activities of open-source research results. Practical approach was also preferred as one of the mandatory KPI-s under WP10 was also the creation of 3 start-ups that would use the technical results of the SPARTA project. As establishing a start-up is a multi-layered decision with implications on individual's standards of living and well-being it became apparent that it was not feasible to expect any SPARTA participant to decide to establish a start-up because it was set so by the KPI-s of the project. For that reason, an approach was developed that would incentivize external teams to adopt and use the SPARTA results in developing business ideas for start-up creation in controlled environment. This approach is described more detail in Chapter 4 "Support to Exploitation Activities".

Chapter 5 provides an overview about common elements of open-source policies and programs, based on publicly available information, as well as related standards and government initiatives. In this context, it summarizes and positions some of the works performed in SPARTA, and highlights selected dissemination and exploitation activities. The wide-spread interest of both industry and academia in SPARTA results demonstrates their impact on and significant contribution to the security of today's open-source supply chains.

## Chapter 2 Exploitation Roadmap

### 2.1 The Definition of Exploitation

In order to understand how to approach exploitation activities or what to consider as an exploitation activity, it is first important to understand what do we talk about when we say “exploitation”. In order to understand what do we talk about, when we say “exploitation” within SPARTA we first need to define it through the SPARTA project, its activities and anticipated results. The Grant Agreement of SPARTA does not give as a defined exploitation as such but merely dictates activities through reached KPI-s.

One of the goals of the SPARTA project is to leverage Europe’s strengths and opportunities across multiple disciplines and locations and improving Europe’s strategic autonomy through developing novel technologies in the field of cybersecurity. The main tool in achieving these goals within SPARTA are the four key programs that were launched under WPs 4 to 7. These programs are T-shark in WP4 which is a full-spectrum cybersecurity awareness research program, CAPE in WP5 is continuous assessment in polymorphous environments research program, HAIL-T in WP6 is high-assurance intelligent infrastructure toolkit program, and SAFAIR in WP7 is secure and reliable AI systems for citizens program. By design these four programs should yield a multitude of novel technologies that promise different types of useful outlets external to SPARTA project. Exploitation of project results is also foreseen by the H2020 Program. As part of the H2020 Open Access guidelines, SPARTA is subject to exploitation activities regarding the specific project results achieved.<sup>1</sup>

In order to approach the topic of exploitation, exploitation within the SPARTA Project was defined as follows:

*In the context of the Sparta project, exploitation can be understood as the commercial and non-commercial utilization of project results, including software, databases, and processes by public entities, industrial actors, cybersecurity practitioners, research organizations and academic institutions, and within special consideration to the sustainability and legal security of project results.*

The definition of exploitation within SPARTA establishes three main constituting elements of exploitation and two specific requirements exploitation should follow within SPARTA. Following this definition, exploitation can be characterized by answering these three questions about its constituting elements:

1. What activities are considered exploitation activities?
2. What are the results that can be exploited?
3. Who can exploit these results?

The definition gives rather open-ended answers to these questions, keeping the list open for unexpected and unforeseen results. The two specific requirements that the definition poses are unique in a sense that not every exploitation roadmap is required to follow these. They are not sine qua non to exploitation activities but rather reflect the values of the SPARTA project. These specific requirements are:

1. Sustainability
2. Legal security of project results.

---

<sup>1</sup> *Dissemination & Exploitation of Results*, European Commission Funding and Tender opportunities, accessed online 10.08.2021, [https://ec.europa.eu/research/participants/docs/h2020-funding-guide/grants/grant-management/dissemination-of-results\\_en.htm](https://ec.europa.eu/research/participants/docs/h2020-funding-guide/grants/grant-management/dissemination-of-results_en.htm)



These unique requirements are the result of EU H2020 Open Access Guidelines and are in line with EU values of sustainable exploitation and protection of intellectual property.

Human Brain Project (HBP) which is one of the largest and longest running EU funded research programs and one of three Future and Emerging Technologies Flagship programs<sup>2</sup> has approached the question of exploitation activities through establishing the three pillars of exploitation and the close link between them.<sup>3</sup> These three pillars are:

1. Protection of results through intellectual property
2. Ownership of results as a basis for protection and exploitation.
3. Exploitation of results materialized by technology transfer to user's market

The three elements and two unique requirements established with the definition of the exploitation within the SPARTA project correlate perfectly with the three pillars established by the Human Brain Project illustrating the cohesion of approach within the EU.

The first two pillars established by the HBP correlate with the two specific requirements posed by the definition of exploitation within the SPARTA. The sustainability and legal security of project results correlate with the pillars of intellectual property and ownership from the HBP. The third pillar of exploitation incorporates the three elements of exploitation from the SPARTA exploitation definition.

The HBP establishes three main pillars of exploitation strategy. As mentioned above, these pillars are protection, exploitation activities itself and ownership.<sup>4</sup> The protection pillar focuses mainly on the intellectual property requirements and possibilities of the project results. The SPARTA project results are software, databases, methodologies, processes, articles and documentation. The intellectual property requirements are restricted based on the format of the result. Articles and documentation fall under copyright law and are granted to the authors automatically on the moment of the creation of the work as per Berne Convention. Software, databases and processes warrant a more thorough approach based on the desired exploitation plan to choose a suitable intellectual property regime. Methodologies as such are difficult to protect by any intellectual property regime unless methodology is established in an article or a documentation and therefore are protected by the copyright, which, however, does not provide a protection from reuse by others but merely grants protection to the authors' moral rights.<sup>5</sup> Useful methodologies are best protected as trade secrets through non-disclosure agreements (NDA) and contractual clauses.

From an intellectual property perspective, the desired exploitation plan for the result directs the selection of the intellectual property regime most suitable for the result. This places a significant burden on the partner of SPARTA to plan for the exploitation at the very early stages of the technology development. In some aspects, there is an inherent conflict between the scientific research and commercial exploitation. Scientific research, however, is often done in the earliest stages of Technology Readiness Level (TRL) which are not in any way suitable for commercial exploitation and require further maturation before commercial exploitation can begin. However, the potential exploitation activities can be considered at very early stages of the TRL.

In the following chapters we will explore in more detail how TRL is a useful tool in establishing a comprehensive exploitation roadmap for managing innovation from the research and development stage all through establishing the best exploitation strategy – commercial or non-commercial. Under

---

<sup>2</sup> *Overview*, Human Brain Project, accessed online 22.11.2021, <https://www.humanbrainproject.eu/en/about/overview/>

<sup>3</sup> *Exploitation Plan Course*, Human Brain Project, accessed online 22.11.2021, <https://www.humanbrainproject.eu/en/col-laborate/exploitation-plan-course/>

<sup>4</sup> *Exploitation Plan Course*, Human Brain Project, accessed online 10.08.2021, <https://www.humanbrainproject.eu/en/col-laborate/exploitation-plan-course/>

<sup>5</sup> *Copyright*, WIPO, accessed online 10.08.2021, <https://www.wipo.int/copyright/en/>

WP10 we have developed a comprehensive Exploitation Roadmap tool that consists of several elements in the exploitation approach – TRL, Commercial Readiness Indicator (CRI), TRL assessment questions, CRI assessment questions, and IP tools.

## 2.2 *Technology Readiness Level (TRL) in cybersecurity innovation*

The Exploitation Roadmap<sup>6</sup> is designed to guide emerging SPARTA technology through its technological and commercial maturity. The main tool used in the creation of the Exploitation Roadmap is the Technology Readiness Level or TRL. In order to adjust already existing TRLs to meet SPARTA needs, we looked into already existing TRLs and their use cases. The three sources for compiling TRL scale for SPARTA project were NASA TRL, Human Brain Project (HBP) TRL and articles published regarding corresponding TRLs for cybersecurity purposes. As of our knowledge, there is no agreed industry-wide TRL for cybersecurity, rather a loose understanding of the TRL derived from the general knowledge of the TRL scale requirements and TRLs used are rather tailored to fit a specific project. In the following paragraphs we will look more closely how different TRL levels can be adopted into SPARTA needs and why TRL should be looked at in terms of exploitation of SPARTA results. Furthermore, we will also explore how TRL levels in conjunction with environmental readiness can be used to predict and measure market adoption of new technologies.

The SPARTA Exploitation Roadmap has been inspired and shares elements with the comprehensive methodology worked out within the HBP. There are clearly significant differences between SPARTA and HBP, nonetheless, the theoretical and practical methodology synthesized by the Innovation and Technology Node of the HBP warrants a closer look. The theoretical principles should be analyzed in the context of the SPARTA and SPARTA should aim to adopt and learn from the best practices that have been developed. Furthermore, the EU Horizon 2020 work program general Annex G for period 2014-2015 establishes TRL levels for technologies that are being developed under H2020 projects. All TRL levels used are based on the NASA 9-step TRL levels that were developed to measure technology readiness for space flight.<sup>7</sup> The use of TRLs in estimating flight readiness for space flight technology stems from the restrictive Earth environment and the need for standardized assessments for novel technologies before deployment to space.<sup>8</sup> Since the introduction of the TRL levels in 1989 other industries and agencies have used NASA TRL as a basis in developing technology readiness assessment levels for novel technologies. Going a step further, Australia has adopted commercial readiness index (RCI) to accompany TRL in order to help in the assessment of market ready technologies and their deployment.<sup>9</sup>

For this purpose, the decision was made to build the Exploitation Roadmap on Technology Readiness Levels. The Exploitation Roadmap is not designed to assess the effectiveness of the technologies as a cybersecurity technology. All these considerations should be part of overall Exploitation Roadmap cycle and be conducted in parallel. The goal of the Exploitation Roadmap is to indicate the readiness of the technology that is being developed for exploitation and to help in understanding when during the technology development cycle intellectual property protection should be implemented, when market research should be considered and so on. The effectiveness, novelty, and applicability of the technology itself should become apparent during the implementation process of the Exploitation Roadmap.

TRL levels are used in many industries to assess the readiness of new technologies and to direct, manage, and anticipate innovation. In the specific field of cybersecurity two aspects need to be considered to understand the potential applicability of a new technology – technological innovation and

---

<sup>6</sup> See Annexes 1 – 5.

<sup>7</sup> Straub, J., 2021, April. Evaluating the Use of Technology Readiness Levels (TRLs) for Cybersecurity Systems. In *2021 IEEE International Systems Conference (SysCon)* (pp. 1-6). IEEE.

<sup>8</sup> Héder, M., 2017. From NASA to EU: the evolution of the TRL scale in Public Sector Innovation. *The Innovation Journal*, 22(2), pp.1-23.

<sup>9</sup> *Ibid.*, 15.

contextual innovation.<sup>10</sup> Technological innovation can be easily indicated by the use of TRL and which aims to assess the readiness level of the technology itself. The contextual innovation indicates, however, the readiness of the innovation environment itself.<sup>11</sup> The innovation environment is the environment in which the technology will be deployed. According to the article by D. Kapletia, N. Wainwright, and M. Felici, there are essentially three distinctive combinations of the technological and contextual innovation.<sup>12</sup>

### **2.2.1 High-readiness of technology and low-innovation context.**

This characterizes a situation where technology has been extensively developed but for various reasons the deployment context is unable to benefit from it.<sup>13</sup> In the context of Annex 1, it would reference a situation where technology is taken from TRL 1 to TRL 9 and where technological capability has been demonstrated but the ability to conduct a commercial deployment is hindered as the environment for the deployment is not capable or willing to adopt or implement the technology.

The environmental hold-up could stem from several reasons. It could stem from the lack of supporting infrastructure which is common in the field of space technology. An example of this could be the development of autonomous rovers for mining space resources on Moon and on asteroids. In this case, the TRL of the rover's capability can reach to 8 or even to 9, but the maturity of the environment is still low and therefore, the technology would not be deployed in the target environment. Similar situation was present in the case of the touch screen which was developed in 1965 and went through several improvements on the technology and reached a high level of TRL before finally being picked up by Apple in 2005.<sup>14</sup> In cybersecurity the situation tends to be the opposite. Cybersecurity technologies tend to play catch-up to technologies enabling cyber intrusions as it is the sophistication of cyber intrusions that dictate the development of cybersecurity technologies.<sup>15</sup>

Another hold-up in the environmental adaptability could stem from the redundancy of the technology. In this case a new technology can reach a high TRL but is not adopted by the environment because there is no actual need for it as market needs are met by other technologies. A good example of an innovative product that despite of its ground-breaking technology was not adopted by the environment was Google Glass. Google Glass was a highly priced product that allowed the wearer to access internet services using the Google Glass as well as receiving useful information on your field of view as you conducted wide-range of other activities.<sup>16</sup> The promise of Google Glass was that the customer could access relevant online information without the use of a phone or a computer.<sup>17</sup> Apple Watch is a product with a similar promise and a similar premise – an apparently everyday wearable item that doubles as a device to be connected to online activities. Apple Watch was launched in 2015 with a fitness-oriented focus.<sup>18</sup> On the surface, these two items service a similar gap in the market, yet one item was adopted while another one was rejected. The readiness of the consumer

---

<sup>10</sup> Kapletia, D., Felici, M. and Wainwright, N., 2014, May. An integrated framework for innovation management in cyber security and privacy. In *Cyber Security and Privacy Forum* (pp. 135-147). Springer, Cham.

<sup>11</sup> Kapletia, D., Felici, M. and Wainwright, N., 2014, May. An integrated framework for innovation management in cyber security and privacy. In *Cyber Security and Privacy Forum* (pp. 135-147). Springer, Cham., 136.

<sup>12</sup> Kapletia, D., Felici, M. and Wainwright, N., (2014), *supra nota*, 7, 136.

<sup>13</sup> *Ibid.*

<sup>14</sup> A *Brief History of Touchscreen Technology*, Accessed online on 25.11.2021, <https://www.zytronic.co.uk/insights/article/history-of-touchscreen-technology/>

<sup>15</sup> *Explainer: As cybercrime evolves, how can companies keep up with their cybersecurity?* World Economic Forum, Accessed online on 24.01.2022. <https://www.weforum.org/agenda/2021/11/cyber-security-evolving-cyber-crime-attacks/>

<sup>16</sup> *How and Why Google Glass Failed?*, Accessed online on 29.11.2021, <https://www.investopedia.com/articles/investing/052115/how-why-google-glass-failed.asp>

<sup>17</sup> *Ibid.*

<sup>18</sup> A *Timeline: A brief History of Apple Watch*, Accessed online on 29.11.2021, <https://www.verizon.com/articles/brief-history-of-apple-watch/>

to adopt a vanity item as an extension of their smart device in a form of glass was low, while readiness to adopt a similarly functioning item in the form of a watch was high.

To speculate the reasons for this apparent disparity of environmental adoption context could lead us to consider the invasiveness of the vanity item. Watch on a wrist is less conspicuous and can be worn despite of environmental changes. Glasses, however, are more invasive, extremely visible and environmental changes have huge implications on their wearability and therefore, to their functional usefulness as would the wearers own healthiness of the eyesight. The examples of Google Glass and Apple Watch may seem distant to a cybersecurity market, yet, it indicates the human behavior as a critical element in adoption in new technologies. Human element as a facilitator or an inhibitor of adoption of new solutions is well documented in the cybersecurity sector.<sup>19</sup> In order to launch a successful product, the developer needs to evaluate the potential of the market to adopt the new innovation and product from early on in the development process and to try to take into account how different aspects of the target consumer might influence the adoption process.

The main tools within the Exploitation Roadmap to help in measuring the market situation in regards to the technology readiness is the TRL assessment questionnaire in Annex 2, and to understand the environmental innovation context the tool to use is the assessment questionnaire for Commercial Readiness Index (CRI) in Annex 4.

### **2.2.2 Low-readiness of technology and high-innovation potential context.**

This refers to a situation where the innovation environment is ready for a technology which is under-developed. From a commercial exploitation perspective, a low TRL combined with high-innovation potential context should result in in-house R&D activities, proprietary intellectual property, early-stage investments, and rapid growth-based market roll-out in order to ensure considerable market size before a competitor. In many aspects this can be a sweet-spot for fast growth and seizing a trailblazer position and creating a new market. Some examples of this type of exploitation roadmap would be Space X and their re-usable rocket, Airbnb hosting or Uber rideshare, and more recently – developing vaccines for Covid-19.

High potential innovation context dictates more secretive R&D process. A developer that has identified an urgent need on the market and has the sufficient competencies to address it, is more likely to make significant financial investments in solving the problem they foresee. This leads the developer into making a business decision to launch the product on the market with a prize that could retroactively cover the R&D investments they made during the R&D phase. This, however, can also result in a release of a technology that is lacking in maturity in order to secure a market position and gain customers.

There are many cybersecurity companies within the EU with in-house R&D teams and strongly guarded proprietary software products in their portfolio. The proprietary software development approach, however, in the cybersecurity fields, creates a closed loop in where portability of cybersecurity products from one platform or a cloud-service to another is incompatible and the developer is required to develop a new solution for the platform/cloud. This creates a situation, where the overall TRL on these services and products remain low as the proprietary method restricts the large-scale cross-platform adoption of the technology and every new offering requires developing the technology from the start to be compatible with the new requirements.

---

<sup>19</sup> Boletsis, C., Halvorsrud, R., Pickering, J.B., Phillips, S.C. and Surridge, M., 2021, February. Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment. In *VISI-GRAPP (3: IVAPP)*(pp. 266-274).

The proprietary approach creates a situation in where companies opting for proprietary approach lock themselves into perpetual low TRL high innovation context scenario that allows them to financially benefit from the market need for their developed projects. However, this also increases a risk for the business model if/when a competing open-sourced solution is pushed to the market that would allow for community involvement and resulting in a higher TRL for the technology in a shorter period of development time that stems from a higher volume of human resources on the project through community engagement.

### **2.2.3 High-readiness of technology and high-innovation potential context.**

High-readiness of technology and high-innovation context is most commonly faced TRL to market environment. In these market conditions a certain technology has been developed and perfected over longer period of time and the maturity of the market has proven itself by adopting similar technology/products or earlier iterations of the same technology. Personal computers, smart phones, electric cars, smart household items and many other everyday consumer electronics fall into this category as well as several cybersecurity solutions.

There are several cybersecurity products that are within the high TRL and high innovation potential context that should warrant a closer look. Most notably, many cybersecurity products tend to rely on open-source communities in developing the technology.<sup>20</sup> This approach is specifically favored within the cybersecurity domain as it allows for maneuverability of the technology to meet changing market conditions. Cybersecurity presents a unique challenge as the field is in a constant state of flux that stems from the rapid change of the ICT technologies, capabilities and environment.

Open-source approach is, therefore, one of the most suitable approaches within the cybersecurity sector to provide high TRL cybersecurity services in a high potential innovation context. The benefits of open-source approach become especially evident when compared to the risks of proprietary software approach described in earlier section. This is not to state that open-source approach is without challenges.

Based on the study commissioned by the European Commission regarding the impact of open-source software and hardware on technological independence, competitiveness and innovation within the EU, the stated challenges were regards to human resources as (1) community engagement, and (2) steep learning curve of contributors.<sup>21</sup> As was mentioned above when we addressed the low TRL and high innovation potential context, the risk in proprietary solutions emerges when a more agile open source solution is released and the agility of the solution stems from the larger community engagement that acts as a bigger pool of human resources focused on the development. This all, however, is dependent on the developers' ability to build and maintain a contributing community. The EC commissioned study indicates, however, that long-term community engagement is presenting a challenge and many developers opt to provide employment contracts to their most active contributors to maintain their interest and involvement.<sup>22</sup> The strength of open-source development, however, is in the high level of intercommunication and interdependencies between different development projects.<sup>23</sup> This results in the developments to influence each other, learn from best practices and to allow a greater level of compatibility which, as we saw, is an element that inhibits some proprietary software to reach high TRL even in high potential innovation context.

---

<sup>20</sup> Blind, K., Böhm, M., Grzegorzewska, P., Katz, A., Muto, S., Pätsch, S. and Schubert, T., 2021. The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy., 57.

<sup>21</sup> *Ibid.*, 72.

<sup>22</sup> Blind, Böhm, Grzegorzewska, Katz, Muto, Pätsch, Schubert (2021), *supra nota*, 19.

<sup>23</sup> *Ibid.*, 82.



## 2.3 Commercial and non-commercial Exploitation

Exploitation Roadmap is designed to guide different exploitation activities for technologies and principles developed within SPARTA. As we saw from defining “exploitation”, it can be both commercial and non-commercial. The goal of the Exploitation Roadmap is to provide a tool to help to understand the different activities and the interoperability of intellectual property considerations with technological development cycles and commercial and non-commercial exploitation planning.

Commercial and non-commercial exploitation are based on a fundamentally different approach to utilizing assets or in the case of SPARTA, the project results and assets. Commercial exploitation is built on the premise that the result of an intellectual work is covered by intellectual property and can be leveraged by means that results in a maximum financial gain to the holder of the intellectual property. Non-commercial exploitation indicates to a situation in where the result of an intellectual work is protected by intellectual property in a manner that would allow for the result to be leveraged for other benefits than financial gain. These benefits can be in place to advance public interests, a community, or a cause to name a few. The defining character of non-commercial exploitation is that generating financial gain through business activities is not the goal of the exploitation activities. This does not exclude the situation in where generating financial gain from the exploitation activities is a side result.

The TRL assessments can be useful for both commercial and non-commercial exploitation. The CRI assessment describes a clear pathway for commercial exploitation and is part of business model development. The TRL in non-commercial exploitation, however, can provide a significant added value in applying for different European science and development funding for academic and R&D purposes.

### 2.3.1 TRL in commercial exploitation

TRL in commercial exploitation is most beneficial when the R&D activities are conducted within a research institution and there is a clear intent of transferring the results into a commercial spin-off or to other types of commercial activities. In such a situation, the TRL assessments provide a useful tool in managing the R&D process and identifying the most suitable time for technology transfer or inviting a commercial partner into a project. When using the provided TRL assessment questions and the Exploitation Roadmap provided in the Annex 1 and Annex 2, then the consideration for technology transfer should be done during TRL 5 or TRL 6 which are located at the end of pilot phase on the CRI scale. Commercial partner should be involved before the technology reaches CRI phase 2 which is the commercial trial. This is typically when the technology has reached TRL 7 and TRL 8.<sup>24</sup> When a commercial partner is included in the later stages of the technology development, the assessment considerations in CRI phase 1 should be made when the commercial partner is being involved or during the involvement negotiations, especially any IP considerations that may arise.

SPARTA is a research and innovation project with high emphasis on developing sustainable and open-sourced new technologies in the field of cybersecurity within the EU. Furthermore, the pillars of the SPARTA project are built on four independent and far-reaching research projects with the aim of furthering Europe’s strategic autonomy. Each of the four research projects within SPARTA are a consortium of multiple partners from private and public sector. This makes SPARTA project a prime candidate for using TRL-based technology transfer from SPARTA research projects into commercial exploitation through partnering with commercial partners or to endorse the creations of spin-offs. This specific goal is also emphasized in the Grant Agreement objective 7 and the established KPI-s #7.1, #7.2 and #7.3. The KPI-s #7.1 and #7.3 being especially biased toward commercial exploitation as establishing SPARTA goals to be measured through how many results are being licensed out and how many results are transformed into newly established start-ups.

---

<sup>24</sup> Héder (2017), *supra nota*, 9, 16.

The benefits of TRL levels in a commercial entity to manage their in-house R&D is questionable and is dependent on the structure of the company. It is, however, more likely that a functioning for-profit entity that is developing new technologies has already developed a functioning system for managing R&D. This system may be built on the principles of TRL but the premise is not universal and therefore, will not be addressed within the scope of this Deliverable.

### **2.3.2 TRL in non-commercial exploitation**

Large portion of SPARTA partners are public institutions and universities. Which means that there is a high probability that SPARTA results developed under different research programs will be utilized in non-commercial exploitation activities. The exploitation definition of SPARTA does not describe or state which activities are considered non-commercial exploitation, it merely states that non-commercial exploitation falls within the scope of what we consider an exploitation within the SPARTA project.

An example of a non-commercial activity that has resulted from the SPARTA project is the development and launch of a spin-off project within the Baltic Region called EACDTA. EACDTA is built on the principle of “last mile” development to help in the developments of EU-funded cybersecurity project results with TRL 8 to reach market maturity and streamline the exploitation activities straight to European public security practitioners.<sup>25</sup> EACDTA aims to make use of the different developments conducted under EU-funded projects in the cybersecurity field and to provide the gap in the practical exploitation stream for these results which might not have exploitation interests by the developer themselves. With this example we see clear connection between TRL and non-commercial exploitation as the purpose of the EACDTA Project is to cater technology needs of EU public sector.

Another example of using TRL levels in a non-commercial exploitation is applying for a specific EU funding designed to increase the TRL levels of a technology. These funding schemes are open for both scientific institutes and for SME-s.<sup>26</sup> The tool developed under SPARTA that can provide technical support in non-commercial exploitation for creating consortiums, managing assets and assessing TRL levels is RAMP.

## **2.4 RAMP as a tool for non-commercial exploitation**

RAMP (Research Asset Management Platform) is an online platform and tool that has been developed under the SPARTA project. Its main aim is to simplify meta-data management related to research assets and their future exploitation. In the case of SPARTA, the platform should maximize the benefits of exploitation activities inside SPARTA and externally. Due to its agile architecture, the tool is designed to be able to provide asset management throughout the entire lifecycle of an asset. In this way, RAMP provides an asset management platform designed specifically to simplify data management and the platform thus finds its place in the overall sustainable exploitation planning.

The platform provides a common place for accessing and identifying assets that can be shared within whole RAMP instances, communities or only within organization that use RAMP. The tool’s versatility allows the users to not only manage their assets but also to manage results of their assets and assess the maturity of their developed technology. Furthermore, mandatory actions such as the creation of data management plans (DMP’s), which are mandatory in any EU project, can also be linked to the assets. Exploitation also requires actions such as privacy or security assessments, which can also be linked to the assets. Here again, due to the versatility of the platform, various forms or assessments, as they are needed, can be created with the help of the platform.

---

<sup>25</sup> EACTDA Project was presented during a workshop held on 25th of November, 2021 on the topic of „SPARTA Partnership Program for Baltic Sea Region Stakeholders“.

<sup>26</sup> *Funding for SMEs and mid-caps*, EU Funding Playbook, Accessed online on 14.12.2021, <https://eufundingplaybook.fi/small/>

As a future goal and planned developments, RAMP will be opened up to users outside of SPARTA and would allow for them to search and view already existing assets to form new consortiums for future projects and developments. Examples of tools available on RAMP are brought in the Annex 5.

In the Annex 5 screenshots different forms for asset management are provided. All these forms are currently available online for all SPARTA partners to use in their asset management. These forms include the creation of an asset, assessment form for pre-existing resources (APER) conjunction to the asset, the previously mentioned DMP form and form to identify produced results (IDPR) regarding the asset. In addition, the RAMP, furthermore, allows to assess the security, privacy, intellectual property and impact and sustainability of the asset. The different opportunities of RAMP are visualized in the Figure 1.

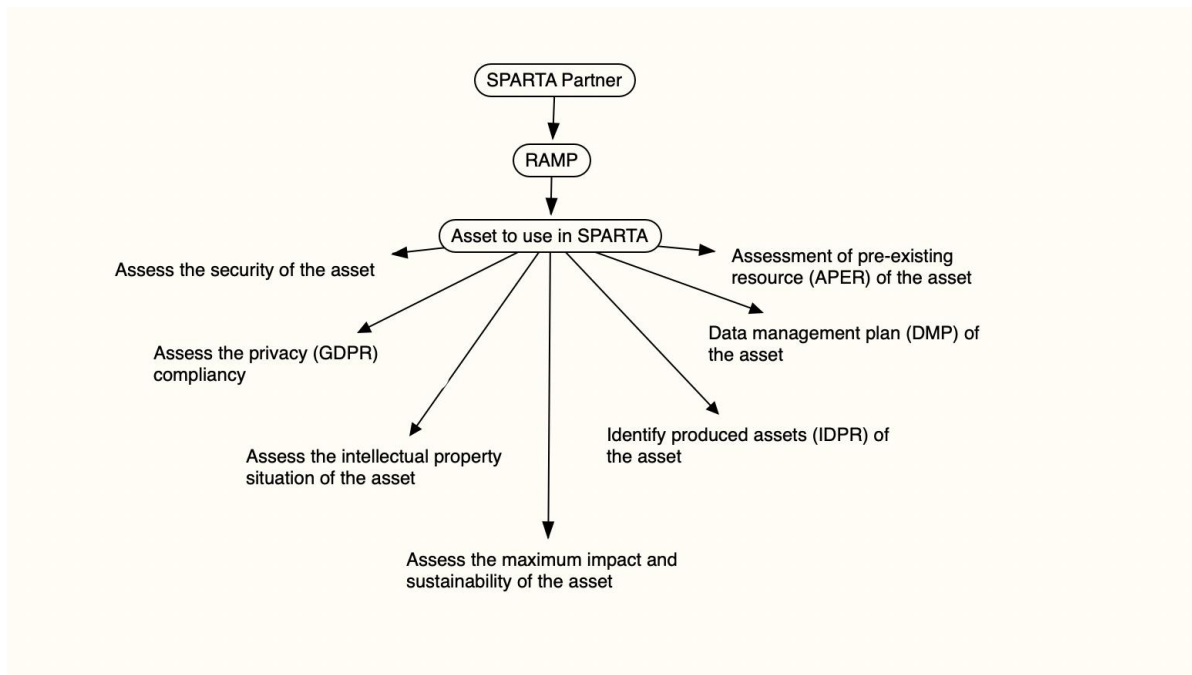


Figure 1: Different assessment tools available on the RAMP platform.



## Chapter 3 Legal Tools for Exploitation

Intellectual Property<sup>27</sup> is a branch of property law that protects intangible assets. An intangible asset is an asset that is not physical in nature. Goodwill, brand recognition and Intellectual Property, such as patents, trademarks, and copyrights, are all intangible assets.<sup>28</sup> The most suitable intellectual property regime used in SPARTA is open-source licensing. As was described in the previous chapter, intellectual property is a vital element in the exploitation process, creating legal grounds for ownership claims on SPARTA results. Proof of ownership is an integral part in the exploitation process. It is only appropriate to spend some time into creating insight into the practical side of the intellectual property question within the SPARTA project.

### 3.1 Choosing open-source license

The relevant question for any SPARTA member to ask, is which open-source license to use. There are many considerations that goes into choosing a suitable open-source license. The topic of choosing an open-source license was also covered and included in the Exploitation Workshop.

There are several questions that need to be answered by the developer that will dictate, which open-source licenses are available to their software. The questions to consider are:

1. Is the software you are building based on already available open-source software?
2. What is the open-source license of the software you are basing your development on?
3. What is permitted and not permitted by this open-source license?

These three questions are the most relevant ones to ask. It is these questions that will determine whether the developer infringe on someone else's intellectual property right or not. If the development is entirely original or is based on free and public software with no legal restrictions of any kind, then the questions the developer needs to ask are as follows:

1. Do you want 3<sup>rd</sup> parties to be able to commercially profit from your work?
2. Do you want to build commercial product based on your work?
3. Do you want your work to be available for public use without the ability of 3<sup>rd</sup> parties to commercially benefit from it?

Based on these questions, the developer should understand what are their limitations and options. If the current development is built on an already existing open-source software, then the restrictions and options stem from the license the software is based on and the developer is legally bonded to the conditions of the open-source license.

The open-source licenses fall on the scale of least protective to most protective. The within the scale should be done based on the answer to the previous questions. If the developer wants to keep the right to commercialize on the technology they have developed, yet would also like to benefit from community engagement, the more protective licenses should be considered. If the situation is reversed and the developer wishes to release the technology to a wider use without many restrictions, more permissive license should be considered. It is, however, important to note that the scale and information provided in this chapter does not replace a thorough study into different open-source licenses. The purpose of this chapter is merely point out relevant aspects that influence the eventual decision of which open-source license to use. The license scale in Figure 2 is a general visual guide

---

<sup>27</sup> According to the World Intellectual Property Organization (WIPO), Intellectual property ("IP") refers to legal protection of creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce.

<sup>28</sup> Investopia, *What is an intangible asset?*, Accessed online 04.04.2012, <https://www.investopedia.com/terms/i/intangibleasset.asp>

to see how intellectual property is protected as you move from technology being published on a public domain without any license towards in-house development that is being kept proprietary by trade secret.

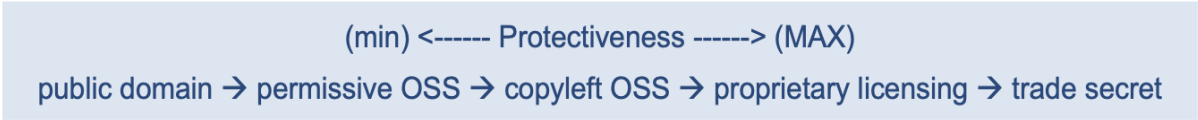


Figure 2: The scale of intellectual property measures in relation to their protectiveness.<sup>29</sup>

Additional requirement in open-source license use is the requirement set in the open-source license for any further development based on the published technology needs to use the same license as the technology used as a basis. This is called a copyleft license and it grants more protection to the original developer. Failing to consider the existing license when basing a new development on top of open-source technology with copyleft license is considered an infringement of intellectual property. From a commercial exploitation perspective, these differences are relevant as they will have significant implications on the commercial exploitation path available.

If a developer is interested in using a large community to improve the product without granting the developers the opportunity to use the technology in building a competitive product, they should consider copyleft open-source licenses. If a team of developers want to build a commercial exploitation on top of open-source technology, they need to make sure that the license is permissive that would allow this type of activities. Figure 3 gives a general overview of the differences of copyleft and permissive open-source licenses.

COPYLEFT	PERMISSIVE
<b>MORE PROTECTIVE</b>	<b>LESS PROTECTIVE</b>
The copyleft clause states that any additional code or derivated code is required to use the same copyleft license	The reseipient can modify and redistribute the resulting derivated work under different license term – including closed source proprietary terms
Guarantees the use of source code in exploitation activities for the original License holder	Allows anyone to exploit the source code for their purposes
Moral rights to every contributor remains with the source code	Moral rights to every contributor remains with the source code

Figure 3: Protectiveness comparison table for permissive and copyleft open-source license.<sup>30</sup>

### 3.2 Exploitation and data protection

<sup>29</sup> Blind, K. and Böhm, M., 2019. The Relationship Between Open Source Software and Standard Setting, Thumm, N.(Ed.) EUR 29867 EN, JRC (Joint Research Centre) Science for Policy Report, Publications Office of the European Union, Luxembourg, 2019.

<sup>30</sup> For detailed information about different open-source licenses available, we recommend to visit the website for Open Source Initiative. Available at: <https://opensource.org>

Since the entering into force of the General Data Protection Regulation in EU 2016/679, and its applicability since May 24, 2018, data protection should be dealt with as an inherent criterion of success for new business projects, especially those that deal with data.

Governance is a key aspect for a successful data collection and usage. Governance is required to ensure the quality of data, but as well for complying with legal requirements in terms of providing (i.e. transferring) the relevant ingested data to the appropriate teams that are in charge of specific projects. The main governance tasks are data authentication, access control and audibility, so as regulatory requirements of managing the data lake.

Data sharing means the disclosure of data collected for one purpose to another person or organization to use for another permitted purpose. In order to be able to share data, data has to be on a server of the data sharing organization. Before sharing data, compliance with applying regulations should be ensured. It should be ensured, that the organization is a lawful rights holder for the data that will be shared. European law has at the moment no specific legal framework regarding data sharing.

In case, personal data is involved, the GDPR regulation applies. It is here recommended to use data sharing agreements which are an important requirement for accountability compliance. Furthermore, specific security safeguards are required by the GDPR as well as specific obligations when data is shared to international organizations outside the European Union.

Non-personal data can in principle be shared freely, with some specific regulations applying in certain cases. This ad-hoc regulation framework is complex and fragmented. There is some general and horizontal legislation and there are sector-specific rules. The general and horizontal legislation, for example the GDPR, can have an impact on the sharing of non-personal data. Sector-specific regulations mainly apply to the financial, industrial and critical infrastructure sectors.

Anti-trust law is regulated on a European level. It is important to comply with the main provisions of the Treaty on the Functioning of the European Union (“TFEU”), articles 101 and 102, that protect the open-market economy, and ensure the proper functioning of the internal market. This legislation is important to data sharing practices when data sharing agreements are established, for example.

Data sharing agreements should, in any case, be arranged with parties with whom data is shared. A data sharing agreement is a contract containing the roles of the parties, the purpose of the data sharing, for example. If personal data is involved, the GDPR sets some specific rules for data sharing agreements. The data sharing agreement should, furthermore, provide rules on control, ownership, and usage rights. It can cover the ownership of data, patents, trademarks, copyrights, and database rights.

Data sharing agreements are subject to the freedom of contract principle. However, the more detailed they are, the more they ensure legal safety for the data sharing organization. They should be envisioned as a contractual framework. They should, furthermore, at a minimum, set out provisions relating to the content or nature of the data, commercial and business provisions (like pricing), and liability and jurisdiction terms.

Regarding Intellectual Property law, the Database Directive<sup>31</sup> creates the *sui generis* right and further copyright protection for databases. Compliance has to be ensured with this directive before ingesting or processing contents of a database. The Regulation on the free flow of non-personal data in the EU applicable as of 28 May 2019, aims at removing obstacles to the free movement of non-personal

---

<sup>31</sup> Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (Database Directive), <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31996L0009&from=LT>.

data across the Member States and IT systems in Europe.<sup>32</sup> This legislation is important to data-sharing as it removes certain barriers to the free flow of non-personal data in the internal market of the European Union.

An important legislation is the Open Data Directive<sup>33</sup> which will replace the Directive 2003/98/EC as of 17 July 2012. The Open Data or PSI (“Public Sector Information”) Directive focuses on the economic aspects of the re-use of information rather than on access to information by citizens. It encourages the Member States to make as much information available for re-use as possible. It addresses material held by public sector bodies in the Member States, at national, regional and local levels, such as ministries, state agencies and municipalities, as well as organizations funded mostly by or under the control of public authorities (e.g. meteorological institutes).<sup>34</sup>

The Directive covers written texts, databases, audio files and film fragments; it does not apply to the educational, scientific and broadcasting sectors.

The PSI framework has a strong focus on the availability of APIs of high-value datasets. The Directive aims to boost the socio-economic potential of public-sector information and makes this information more easily available for companies by increasing the supply of dynamic data and datasets with a particularly high economic impact, while at the same time promoting competition and transparency in the information market.<sup>35</sup>

In conclusion, when sharing data, personal or non-personal, it is important to comply with the different applying data sharing and IP legislation frameworks. First, an analysis of the data itself has to be set out to verify the application of the GDPR. Secondly, a proper overview of the licenses affected to the datasets that will be *ingested* has to be carried out. In a third step, license agreements have to be created for the third parties and industrial partners with whom the data will be shared.

---

<sup>32</sup> Regulation 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Free Flow Regulation), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN>.

<sup>33</sup> Directive 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1024&from=EN>.

<sup>34</sup> EC, European legislation on open data and the re-use of public sector information, <https://ec.europa.eu/digital-single-market/en/european-legislation-reuse-public-sector-information> .

<sup>35</sup> Support Centre for data sharing, *B2 – Analytical report on EU law applicable to sharing of non-personal data*, 24 January 2020, [https://eudatasharing.eu/sites/default/files/2020-02/EN\\_AR%20on%20EU%20law%20applicable%20to%20sharing%20of%20non-personal%20data.pdf](https://eudatasharing.eu/sites/default/files/2020-02/EN_AR%20on%20EU%20law%20applicable%20to%20sharing%20of%20non-personal%20data.pdf).

## Chapter 4 Support to Exploitation Activities

### 4.1 Summary of the Exploitation Workshop

The purpose of the Exploitation Workshop organized by SMILE was to map and understand the readiness of the SPARTA partners to conduct exploitation activities of the results by themselves. The KPI-s under WP10 require the establishment of 3 start-ups based on the technical results of the SPARTA project. Therefore, it was paramount to understand whether or not there is a willingness to establish start-ups by the SPARTA partners themselves and if so, and they have not done so, is there a lack of understanding on how to approach establishment of the start-up. The secondary purpose of this workshop was to determine partners' level of situational awareness regarding exploitation activities and understand the extent of their knowledge in this matter, and especially potential issues that would have risen regarding Intellectual Property and exploitation of their results. Through a simple workshop, we aimed at compensating the infrequent provision of information regarding current or planned partners' exploitation activities, namely by giving them the opportunity to get their questions answered.

SMILE organized an online Exploitation Workshop on November 9<sup>th</sup> 2021 to all the SPARTA partners. The Workshop was based on the same topics addressed in the Deliverable 10.5. and was designed to provide an overview of different exploitation tools used in SPARTA based on the different types of results produced in SPARTA.

The workshop lasted for 90 minutes. Some topics at the core of exploitation activities that were addressed above in this chapter were developed as follows:

1. Definition of Exploitation
2. The Pillars of Exploitation
3. Intellectual Property
4. Ownership
5. Exploitation

In order to determine the elements on which participants needed guidance regarding their exploitation activities, an online registration form with questions was sent to SPARTA partners. In registration form, 10 individuals signed up from SMILE, Luxembourg Institute of Science and Technology, Tecnalía, TECHNIKON Forschungs- und Planungsgesellschaft mbH, Polish Platform for Homeland Security, Enel Global Services, Vicomtech, Technical University of Munich, TECNALIA and Leonardo. Participants of the workshop were divided between several WP6, WP7, WP13, WP9, WP4 and WP10 from SPARTA. The registration form also gave the participants the opportunity to pose specific questions about exploitation to be answered during the workshop.

The questions of this registration form as well as the repartition of the answers are presented hereafter:

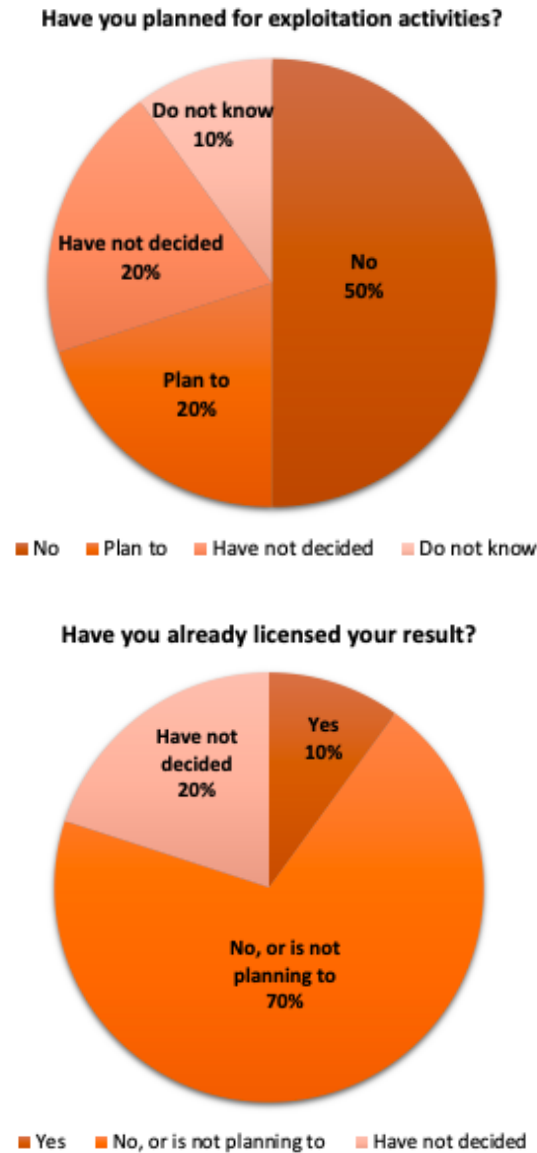


Figure 4: Questions of the registration form and the repartition of the answers

Answers to the registration form revealed that most partners did not conduct or plan exploitation activities for their result yet, and only few of them have already licensed their result. Regarding the nature of planned or conducted exploitation activities, most partners do not know or have not decided whether or not they would like their result to have a commercial outlet or an outlet for public interests. Very few specific questions about the addressed topic were raised.

In conclusion, the workshop had a double purpose: introduce exploitation tools to SPARTA partners, and learn about the status of their exploitation activities. We have been able to collect useful information about participants' current or planned exploitation of activities. Despite the fact that not many questions were asked, participants could get an overview of what exploitation activities in the context of SPARTA is comprised of and how they can be conducted. The results of the Exploitation Workshop led to the development of Exploitation Hackathon as a tool to incentivize external teams in developing exploitation activities based on the SPARTA results.



## 4.2 Exploitation Hackathons

One of the resulting KPI-s of SPARTA project is the creation of 3 start-ups. The specific definition of what constitutes as a start-up as a KPI of SPARTA project is not specified. However, based on the variation of different open-source tools developed under the project, the use of the developed tools as a premise of a commercial plan was taken as a starting point of the exploitation activities for SPARTA. The deliverable D10.6 explores business canvas approach to SPARTA results. The Exploitation Hackathons aimed to develop a more agile and open approach for initiating startup creation. Based on the feedback from the SPARTA partners from the Exploitation Workshop it became necessary to incentivize external teams to develop exploitation activities and business models based on SPARTA results. For that purpose, two Exploitation Hackathons were conducted. The first Hackathon took place before the end of M36. The extension of the project, however, presented us an opportunity to conduct a second and improved Hackathon based on the lessons learned from the first Hackathon.

### 4.2.1 Exploitation Hackathon, January 2022

The first Exploitation Hackathon by the name of SPARTA Cybersecurity Hackathon took place remotely on the weekend of 28 – 30 of January.<sup>36</sup> The purpose of the Hackathon was to develop business ideas based on the open-source cybersecurity tools developed under the SPARTA research work packages 4 to 7. The teams were tasked to present a working prototype by the end of the event.

The Hackathon was built up to support team formation and idea creation. The format of the Hackathon was 48-hour continuous work with expert mentors available during the entire period. As a result, we had 129 registered participants, 22 participating participants and 8 teams were formed. Out from these 8 teams, 2 quit the Hackathon before the end. Due to the online format of the event participants were located in various places in European continent.

During the Hackathon 6 open-source tools from the SPARTA were made available for the teams to work with. The tools were published on the website of the event and an online platform Eventornado was made available for the teams and individuals to post their initial ideas and attract team members. During the pre-event period 9 ideas were posted using the Eventornado platform.<sup>37</sup>

In the following tables the teams, their solutions and available open-source tools are provided.

Team Name	Solution	Used OSS
FuzzyBird 1 <sup>st</sup> Place	Mobile security tool for securing sensitive personal data within the devices. Extension for alerting suspicious online activities such as fake webpages, phishing etc.	SMILE/MISP
CoOrder8 2 <sup>nd</sup> Place	User App for reporting cyber incidents to CERT-s for average person.	SMILE/MISP
TustHub 3 <sup>rd</sup> Place	Policy as a code for IoT devices.	SMILE/MISP
SecuredPI	Real-time alert for sensor malfunction.	SMILE/MISP
Polaris	Fake news alert extension for web browsers.	SMILE/MISP

<sup>36</sup> SPARTA Cybersecurity Hackathon, Available at <https://garage48.org/events/sparta-cybersecurity-hackathon>

<sup>37</sup> SPARTA Cybersecurity Hackathon Pitched Ideas, Available at <https://eventornado.com/event/spartacybersec#ideas>

Team Name	Solution	Used OSS
AutoSec	Securing data streams from sensors to decision making systems of autonomous vehicles.	SMILE/MISP

Table 1: Exploitation Hackathon I teams, solutions and used open-source tools

Name of the Tool	SPARTA Partner/WP	Description	License
NEMEA (Network Measurements Analysis)	CESNET	NEMEA system is a <b>stream-wise, flow-based</b> , and <b>modular</b> detection system for network traffic analysis. It consists of many independent modules which are interconnected via communication interfaces and each of the modules has its own task. Communication between modules is done by message passing where the messages contain flow records, alerts, some statistics or preprocessed data.	Permissive License with some restrictions
VulnEx	UKON/WP5	The web client of the VA tool, served by the server component Db-connector: The database connector module for the db-importer and server Db-importer: creates the database used for the VA tool Server: the server of the VA tool, serving the static content and REST API	Apache License 2.2. Commercial use permitted
TSOpen	WP5	TSOpen is a flow-, path- and context-sensitive tool to detect logic bombs in Android applications.	GNU Lesser General Public License v2.1.
Eclipse Steady	SAP/WP5	Detective control that supports application developers in the detection, assessment and mitigation of open-source code with known vulnerabilities. The tool analyzes Java and Python applications in order to: <ul style="list-style-type: none"> <li>• detect whether they depend on open-source components with known vulnerabilities,</li> <li>• collect evidence regarding the execution of vulnerable code in a given application context (through the combination of static and dynamic analysis techniques), and</li> <li>• support developers in the mitigation of such dependencies.</li> </ul>	Multiple Licenses
BuildWatch	UBO/WP5	Detects and filters suspicious activities that happen during project builds e.g. network activity or file system access.	GNU Affero Public License v3.0.
MISP	SMILE	MISP is an open-source software solution for collecting, storing, distributing and sharing cyber security indicators and threats about cyber security incidents analysis and malware analysis. MISP is	GNU Affero Public License v3.0.



Name of the Tool	SPARTA Partner/WP	Description	License
		<p>designed by and for incident analysts, security and ICT professionals or malware reversers to support their day-to-day operations to share structured information efficiently.</p> <p>The objective of MISIP is to foster the sharing of structured information within the security community and abroad. MISIP provides functionalities to support the exchange of information but also the consumption of said information by Network Intrusion Detection Systems (NIDS), LIDS and also log analysis tools, SIEMs.</p>	

Table 2: Open-Source tools from SPARTA used in the Exploitation Hackathon I

#### 4.2.2 Cross-Pilot Exploitation Hackathon, May 2022

The second Exploitation Hackathon with the name of Cybersecurity Hackathon #MayYourSourceBeOpen took place in person in Luxembourg during the weekend of 20 – 22 of May. The #MayYourSourceBeOpen Hackathon aimed to build business development ideas on the open-source cybersecurity tools developed under three of cybersecurity pilot program SPARTA, ECHO and Concordia. As the event took place in person. Participants were mainly students from University of Luxembourg and University of Lorraine.

In the following tables the teams, their solutions and available open-source tools are provided.

Team Name	Solution	Open-Source Tools used
1 <sup>st</sup> Price Mimics Protect	Protecting building control and automation protocols from cyberthreats	CESNET/NEMEA (SPARTA) CETIC/VASCINE (SPARTA) DDoS Clearing House (Concordia)
2 <sup>nd</sup> Price ShareME	Real-time data sharing in a secure way (focus on health care industry)	IMT / Multi-Client Clusion (SPARTA)
3 <sup>rd</sup> Place URC <sup>2</sup>	Common content for security training and a unified language for Cyber Ranges	KYPO Cyber Range (Concordia) Cyber Sandbox Creator, Cryton, Virtual Host Images (Concordia)
Identity Guardian	Phishing protection when using self-sovereign (digital) identity authentication.	CESNET/EXPLAIN (SPARTA)
5Giligence	A tool for assessing security in 5G hardware and to detect the lack of compliance to the existing standards NAIMEI.	CESNET/NEMEA (SPARTA)
SECOM PRO	Security tests of the financial markets for testing the IT infrastructure.	DDoS Clearing House (Concordia) KYPO Cyber Range (Concordia) Cyber Sandbox Creator, Virtual Host Images (Concordia)

Team Name	Solution	Open-Source Tools used
DDoS PRO	Cloud based solution to prevent DDoS attacks on edge devices	CETIC/VASCINE (SPARTA) DDoS Clearing House (Concordia)

Table 3: Participating teams, their solutions and used open-source tools.

Name of the Tool	SPARTA Partner/WP	Description	License
NEMEA/DDoS Backscatter Module	CESNET/WP4	The objectives of the tool are to utilize the backbone network hosting several / 16 prefixes as an observation point for the backscatter traffic. In such a case it is not possible to use raw packet capture as a source of data but to use flow collected from the edges of the backbone to collect all back-scatter traffic flowing through the backbone. Machine learning methods will be employed to train heuristics which will classify back-scatter and no-back-scatter traffic.	Permissive License with some restrictions
Sharing of Machine Learning Modules (EXPLAIN)	CESNET/WP4	Numerous malware families rely on domain generation algorithms (DGAs) to establish a connection to their command and control (C2) server. Counteracting DGAs, several machine learning classifiers have been proposed enabling the identification of the DGA that generated a specific domain name and thus triggering targeted remediation measures. However, the proposed state-of-the-art classifiers are based on deep learning models. The black box nature of these makes it difficult to evaluate their reasoning.	Apache 2.0
BuildWatch	UBO/WP5	Detects and filters suspicious activities that happen during project builds e.g. network activity or file system access.	GNU Affero Public License v3.0.
Backstabber's Knife Collection	SAP/UBO/WP5	Backstabber's Knife Collection, developed by the University of Bonn and SAP, is an open-source dataset of malicious open-source packages used in real-world attacks. This dataset is an invaluable resource supporting the development of preventive and detective safeguards.	Accessible per request
Eclipse Steady	SAP/WP5	Eclipse Steady is a detective control that supports application developers in the detection, assessment and mitigation of open-source code with known vulnerabilities. Ideally, it is periodically triggered by automated CI/CD pipeline jobs throughout the whole software development lifecycle. The features provided by Steady support developers to meet several of SCVS's	Apache License 2.0

Name of the Tool	SPARTA Partner/WP	Description	License
		certification requirements in the categories V3 (Build Environment) and V5 (Component Analysis)	
Project KP (Element of Eclipse Steady)	SAP/WP5	Project KB, developed by SAP, is an open-source dataset with code-level information about open-source vulnerabilities. The datasets fuels Eclipse Steady, which needs the detailed, code-level vulnerability information in order to perform its various code analyses <i>SAP/Project-kb</i> .	Apache License 2.0
VulnEX (Element of Eclipse Steady)	UKON/WP5	VulnEx reads and aggregates information read from Eclipse Steady in order to support OSPOs and other organizational stakeholders in the organization-wide analysis of open-source consumption and open-source vulnerabilities.	Apache License 2.0
TSOpen	WP5	TSOpen is a flow-, path- and context-sensitive tool to detect logic bombs in Android applications.	GNU Lesser General Public License v2.1
CRACK	CINI/WP6	CRACK supports the design, validation, deployment and testing of scenarios for a Cyber Range. Scenarios are encoded using a domain specific language, called SDL, which extends the OASIS standard TOSCA. CRACK also supports the automatic verification of a scenario against its training objectives. After a successful verification, the scenario is automatically deployed in the Cyber Range and automatically tested to check the correspondence between the behaviour of the deployed system and its specification.	AGPL v3
Multi-Client Clusion	IMT/WP6	Extension of the functionality of the Clusion SSE open-source library to the multi-client setting. Data owners can outsource an encrypted dataset to a service provider. Data clients submit queries on the outsourced data, using search tokens provided by the data owner.	GPL v3
Vaccine	CETIC/WP5	Vaccine is an open-source security orchestration, automation and response tool that provides adaptive security for distributed systems. The tool relies on continuous monitoring of Cloud and Edge systems to define, evaluate and apply automated countermeasures such as firewalls, intrusion detection systems, honeypots or quarantining.	

Table 4: Open-Source tools from SPARTA used in the Exploitation Hackathon II

Name of the Tool	Owner	Description	License
KYPO Cyber Range	Mazaryk University	Cyber Range is a virtual environment for training and educating students, professionals, and others on different scenarios regarding cybersecurity. It is based on modern approaches such as containers, infrastructure as code, microservices, and open-source software.	No info about specific License
Cyber Sandbox Creator, Cryton, Virtual Host Images	Mazaryk University	Cyber Sandbox Creator: A versatile tool for creating lightweight virtual labs – isolated environments for cybersecurity training, experimentation, or testing based on user input; Cryton: An attack automation tool that allows executing the same attack scenarios over and over again. It also compares these executions among themselves; Virtual Host Images: Custom images with handpicked preinstalled tools and configuration options enable seamless use for Cyber Sandbox Creator and KYPO Cyber Range Platform.	No info about specific License
DDoS Clearing House	Anti-DDoS-Coalite	The DDoS Clearing House (DDoSCH) is a system that enables organisations to continually and automatically share measurements of the DDoS attacks they handle in the form of “DDoS fingerprints”. The Clearing House thus widens these organisations' view on the DDoS attack landscape and enables them to proactively prepare their networks for a particular DDoS attack before it might actually hit them, which reduces the probability of system outages and increases the availability of services for customers and users. The DDoS Clearing House is an additional layer of security that complements DDoS mitigation services, which organisations need to have in place to handle actual DDoS traffic.	

Table 5: Open-Source tools from CONCORDIA used in the Exploitation Hackathon II

Name of the Tool	Owner	Description	License
Malware Analysis and Intelligence Tool (MAIT)	BU	An automated and behaviour-based malware analysis toolkit that identifies potential malicious executables files (.exe, .dll) and collect Cyber Threat Intelligence for the file by using online resources. By utilising a BU-CERT instance of open-source state-of-the-art malware static and dynamic analysers (such as cuckoo sandbox) and with the use of open-source malware databases, this tool aims to provide a malware signature along with an intelligence report collected from public sources.	No info available

Table 6: Open-Source tools from ECHO used in the Exploitation Hackathon II

### **4.2.3 Lessons Learned**

#### **4.2.3.1 Lesson 1: The availability of open-source owners as Mentors creates bias**

During the first Exploitation Hackathon in January, the owners and developers of MISP open-source tool were available to all teams and participants during the entire event. Which, in turn, led to a clear bias to use MISP tool instead of other available open-source tools.

During the second Exploitation Hackathon in May, none of the owners or developers of the open-source tools were participating the Hackathon as mentors. The result was visible through more diverse adoption of the available open-source tools by the teams. Even though, there were still some tools that were more popular, the trends did not show any indication of preferential selection of any certain open-source tool by the teams.

#### **4.2.3.2 Lesson 2: General Mentors vs Team Mentors**

General Mentors approach was used during the Exploitation Hackathon I. General Mentor approach means that each mentor is available to mentor and coach each participating team. The positive aspect of General Mentor approach is that the event can cover more expertise with smaller number of expert mentors.

The negative aspect of General Mentor approach seemed to have been three-fold. First negative aspect was the limited focus from a mentor to a team. As all mentors helped all teams, they did not have the opportunity to delve into specific challenges of any specific team. That led to shallower engagement from a single mentor to a team. The second negative aspect in General Mentor approach was over-use of some mentors and under-use of others. As mentioned in a previous Lessons Learned the presence of developers of MISP tool resulted in most teams using MISP as the open-source tool for their solution. This also led to the over-use of the mentors of MISP owners. The final aspect in General Mentor approach seemed to have been the multiplicity of opinions on the same issue for a team and resulting confusion in the team of the best approach to take.

Team Mentor approach was used during the Exploitation Hackathon II. Team Mentor approach means that each team is assigned specific mentor(s) who will work exclusively with their assigned team during the whole period of the Hackathon. The negatives and positives of a Team Mentor approach seemed to be more evenly distributed and did not create a clear bias throughout the event.

As a positive effect, having specific Team Mentors for the duration of the event led for the Mentors to have more time and engaged involvement with specific teams. This allowed for the teams to exploit the knowledge and expertise of the mentors to the full as the team had the full attention of the mentor. From a negative perspective Team Mentor approach limited the distribution of expertise among the pool of mentors. This, however, did not seem to have a deep negative affect on the team progress. The risk of Team Mentor approach stems from mismatch of a mentor and a team.

Compared to the General Mentor approach, the Team Mentor approach is recommended. Focused engagement from experienced industry professional seems to have been more effective than shallow engagement from a vast variety of industry professionals. The General Mentor approach is not recommended for any future Hackathon event.

#### **4.2.3.3 Lesson 3: Prize Matters**

Exploitation Hackathon I and II posed prizes for the winning teams. The proposition of a prize was meant to incentivize participation and collaboration during the event.

Exploitation Hackathon I had 3 prizes for the teams. The 1<sup>st</sup> place team was to receive a cash prize of 5000€ from SMILE, the 2<sup>nd</sup> place was to receive a 3000€ cash prize. Unplanned 3<sup>rd</sup> place and a mentorship prize was posed during the jury deliberation period and proposed by the representative

of CONCORDIA Project. The Mentorship prize for the teams was an *ad hoc* addition to the winning teams based on their proposed solutions.

Exploitation Hackathon II tied cash prize with the Mentorship milestones. The Exploitation Hackathon II posed similar prizes for 1<sup>st</sup> and 2<sup>nd</sup> place. The prize for the winner and runner-up was a Mentorship with SMILE up to 12 months with up to 5000€ available for milestone-based expenses. Exploitation Hackathon II removed the promise of available cash as a prize and tied the monetary prize with the Mentorship milestones for the teams. More detailed description of the Mentorship program will be provided in the following Chapter 4.3.

The Prize change from cash to sponsored mentorship stems from the purpose and the aim of the Exploitation Hackathon. The purpose of the Exploitation Hackathon is to incentivize startup creation not competition for winning cash. As only one team from Exploitation Hackathon I is committed to continuing the development of their solution the potential financial and time loss for the organization managing the Mentorship is high. On the other hand, connecting Mentorship with the financial support for milestone-based progress and expenses should have more positive impact on filtering out teams willing to develop their solutions into functioning startups. Milestone-based expense support Mentorship prize is recommended.

#### **4.2.3.4 Lesson 4: Focus on Business model creation rather than technical prototype**

The expected end result for the teams in the Exploitation Hackathon I was a working prototype of their solution. As the format of 48-hours is limited it resulted in not sufficient time to develop new technical solutions. This restriction resulted with the teams focusing mainly in further developing the open-source solution and less focusing on market validation or business models for their solutions. Such a restriction and expectation on working prototype might have also been the reason why MISIP tool was so widely used.

During the Exploitation Hackathon II the focus was on business model development and the requirement for technical prototyping was restricted to the understanding of the feasibility and technical restrictions of the open-source tool. Furthermore, the Mentorship program as a means to further develop the technical solution after the Hackathon was communicated to the teams. Therefore, the teams were expected to understand what were the further technical steps they would need to take during a longer period of the Mentorship rather than to focus on this during the 48-hour period.

Focus on business model development with technical feasibility study for a 48-hour Exploitation Hackathon is recommended.

#### **4.2.3.5 Lesson 5: Pre-event communication with participants is key**

The communication with participants during the Exploitation Hackathon I took place electronically using the Eventornado platform. The participants could pose their ideas, get feedback from the mentors and OSS owners and recruit team members. With the approach of the event the communication was directed to Discord where dedicated communication channels were opened for teams and mentors. No dedicated pre-event was organized.

The Exploitation Hackathon II a Discovery Session with participants was organized via Zoom. The purpose of the Discovery Session was two-fold. The first aim was to introduce and explain the open-source tools used in the event. The open-source tools were organized in a unified manner giving participants the description of the tool, example use-cases and directing them to the repositories for further inquiry. As this was communicated before the Discovery Session many participants had already familiarized themselves with the open-source tools. The second aim of the Discovery Session was to engage registering participants before the event and thus make them more likely to participate.



Pre-event in a form of Discovery Session is recommended. However, for any future event a participation of the tool owners in the Discovery Session should be considered to better explain the tools and their use cases. Dissemination of the Discovery Session open-source tool slides is recommended as it gives visual and simple reminder for participants in preparation and during the event.

#### **4.2.4 Proposed Framework Approach for Business Development Hackathon for open-source**

In conclusion of the two Exploitation Hackathons a framework approach for conducting open-source business development hackathons is proposed. The proposed framework is based on the recommendations and lessons learned from the two conducted Exploitation Hackathons.

##### **4.2.4.1 Pre-event Discovery Session with owners of open-source tools**

In a week leading to the event a Discovery Session with participants where open-source tool owners are introducing the tools and their use cases should be conducted. The open-source tools should be organized in a similar manner and focus should be on the use cases.

Discovery Session has two benefits for the upcoming event. Firstly, it consolidates the commitment of the participants. Secondly, it helps the participants in understanding the tools and to devise ideas to pitch during the event.

From the experience with the Exploitation Hackathon I, the recommendation would be to limit the owners of the open-source tools during the Discovery Session as to remove the bias from the actual event.

##### **4.2.4.2 Focus on Team Mentors**

Each team should have minimum of 2 dedicated mentors for the period of the Hackathon. These mentors should be professionals in the industry with a background in business development, cyber-security, use of open-source in commercial product development, product owners, startup founders, marketers and so on. The available mentors should be able to help the teams with understanding of startup creation.

For this purpose, a lot of pre-work needs to be done in the preparation of the Hackathon to make sure that relevant expertise is covered. As the Exploitation Hackathon aims in startup creation, the focus should remain on recruiting mentors with industry and commercial experience.

Another aspect to pay attention to is the commitment and availability of the mentors to engage with the teams on all days of the event. It is recommended to have continuous mentors present during the event as they can engage in the teams progress throughout the entire event.

##### **4.2.4.3 Proposed schedule of the event**

The proposed schedule and activities for the event are given in the following table. In using the table for organizing an Exploitation Hackathon, the Lessons Learned and recommendations from Lessons Learned should be taken into account when adjusting the framework for specific goals.

<b>Time</b>	<b>Activity</b>	<b>Who is involved</b>
Week leading into the event	Pre-Event Discovery Session	Registered participants, future team leads, owners & developers of open-source tools
Day 1	Opening of the event	Participants, sponsors, mentors
	Mentoring Sessions	Teams, dedicated mentors

Time	Activity	Who is involved
	Teamwork	Teams
Day 2	Workshops on relevant topics. Examples: business canvas, pitching, open-source licensing etc.	Participants, dedicated lecturers
	Teamwork	Teams
	Mentoring Session	Teams, dedicated mentors
	Teamwork	Teams
Day 3	Teamwork	
	Preparation for the Finals	Teams, pitch coach
	Finals & Closing of the event	Teams, mentors, jury, audience
After the event	Mentorship begins	Winning teams, coaches and mentors for the Mentorship program

Table 7: Proposed Schedule for Exploitation Hackathon activities

### 4.3 SPARTA Start-up Mentorship

#### 4.3.1 Summary of the Startup Mentorship I

The Startup Mentorship I followed the Exploitation Hackathon I. Two teams, CoOrder8 and TrustHub, were rewarded with an opportunity to have a 2-month Mentorship with SPARTA partners SMILE and Vicomtech. The Startup Mentorship I was conducted using informal approach. The goals of the Mentorship were discussed and set loosely to benefit the technical development of the teams. The CoOrder8 set up a dedicated communication channel with SMILE for technical mentorship. The technical discussion between the developers of MISP and CoOrder8 is ongoing and the team has continued to develop the solution. As there were no specific milestones or final goal set at the beginning of the Mentorship the current status of the Mentorship has moved towards continuous collaboration between MISP team and CoOrder8 based on questions that arise.

The mentorship conducted with Vicomtech faced similar challenges due to the informal approach. The specific challenges were posed and discussed. First attempts in solving the challenges were made and feedback provided to the team. After which, contact to the team was lost.

In summary, the team CoOrder8 is continuing their development of the user application to submit relevant data for CERTS about cyber incidences. There has been interest in their solution from military and defense sector as a tool to be used by their employees to inform about such events. The tool uses MISP data sharing software as a baseline architecture for sorting of submitted data. However, as no formal requirement for the mentorship was set it is also difficult to assess the success of the mentorship.

#### 4.3.2 Preparation of the Startup Mentorship II

Learning from the mistakes of the Mentorship I in preparation for the Mentorship II the approach was tailored after an example of NASA Commercial Orbital Transportation Service (COTS) program.<sup>38</sup> The concepts in the COTS project that made COTS a success were a) limited government

<sup>38</sup> Lindenmoyer, Alan, and Dennis Stone. "Status of NASA's commercial cargo and crew transportation initiative." *Acta Astronautica* 66, no. 5-6 (2010): 788-791.



investment, b) “Buy a Ticket, not a Vehicle” approach, c) performance-based fixed-price milestones and c) no procurement contracts.<sup>39</sup>

For the Startup Mentorship II some concepts from NASA COTS program will be implemented as well as more formal approach will be taken. The Mentorship II will be conducted and finished after the end of SPARTA Project. The principles for the Startup Mentorship II are the following:

1. Performance-based limited funding for legitimate expenses
2. Conditional contract between the team and SMILE for the execution of the agreed Roadmap with specific end-goal
3. Proof of Concept pilot for technical solution with industry partner as a mandatory condition for the continuation of the Mentorship. Failure to conduct one during the 12-month mentorship program results in the expulsion from the Mentorship.
4. Graduation of the team into an accelerator program.

The Startup Mentorship II will have a duration of 12 months and the Startup Mentorship started after the Exploitation Hackathon II which took place in May, 2002. Therefore, the results of the Startup Mentorship II will extend the timeframe of the SPARTA project.

---

<sup>39</sup> NASA, *Commercial Orbital Transportation Services. A New Era in Spaceflight*, 2014, p 10-14

# Chapter 5 Exploitation activities related to Open-source Supply Chains (SAP)

This chapter introduces industry best-practices regarding the contribution and consumption of open-source, with a particular focus on security. Thereafter, it provides a brief overview about different regulatory initiatives and open standards related to software supply chain security, which further underlines the need for software and service providers to formulate and implement policies regarding open-source consumption as part of their open-source programs. Finally, this background is used to position the exploitation and dissemination of related work conducted specifically in SPARTA's CAPE program.

## 5.1 Open-source Programs in the Industry

The increased dependency of commercial software development organizations on open-source, as well as the possibilities to support business models and strategies, require industrial players to address open-source more systematically and holistically than before, when consumption and contributions were ad-hoc, opportunistic and did not follow central guidance.

This requirement is commonly reflected by so-called open-source programs. At high-level, the objective of an open-source program is to define, govern and support all interactions of an organization with the open-source community in order to meet the organization's strategic goals.

For what concerns software and service providers, it typically covers the consumption of and contribution to open-source projects throughout the software development lifecycle, esp. in regards to mitigating legal risks. Furthermore, it commonly addresses training needs, and defines and implements communication strategies.

Such an open-source program is often devised, implemented, and monitored by Open-Source Program Offices (OSPO). The structure, organizational setup and staffing of OSPOs change from one company to another, depending on various factors like industry or company size.

Nevertheless, the remainder of this section aims at distilling common elements of such open-source programs, esp. regarding the secure consumption of open-source software, a topic which is addressed by several partners participating in SPARTA's CAPE program.

To this end, we rely on publicly accessible information about open-source programs. Particularly important sources of information are the material published by the TODO Group<sup>40</sup> and the OSPO Alliance<sup>41</sup>, both of which are open groups supporting organizations in the creation of an OSPO.

This public material has been reviewed to compile a list of topics typically covered by open-source programs, as well as a list of instruments (approaches or controls) commonly used within each of those areas.

---

<sup>40</sup> *Talk Openly, Develop Openly*, TODO Group, Accessed online 07.12.2021, <https://todogroup.org>

<sup>41</sup> *OSPO Zone*, OSPO Zone, Accessed online 07.12.2021, <https://ospo.zone>

### 5.1.1 Google

Google publishes detailed internal documentation regarding open-source processes online<sup>42</sup>, with just little internal or confidential information scrubbed, e.g. email addresses. The documentation is structured into three parts: (1) Creating open-source, (2) using open-source and (3) growing open-source, the latter of which covers community-building activities.

(1) Creation of open-source covers the release of code written by Google employees, e.g. patches to existing external projects or the creation of a new standalone project. The default license for new projects is the Apache License v2. Except for low-risk projects, the release process includes a staging environment, where code will be scanned for license and 3rd party code issues before being pushed to GitHub<sup>43</sup>, which is Google's default source code repository<sup>44</sup>.

(2) Use of open-source provides guidance regarding the handling of various license types, e.g. restricted or permissive licenses, and includes a list of licenses forbidden at Google, e.g. AGPL or the European Union Public License (EUPL). Google has a strict policy to only use one version of a given open-source project across its product range (the One Version Rule<sup>45</sup>), in order to avoid version conflicts in complex dependency trees. The use of binary artifacts downloaded from package repositories is forbidden, thus, the source code of every component must be mirrored at Google. Every component has an owner with defined responsibilities, e.g. vulnerability monitoring and patching.

(3) Growing of open-source mentions activities to build and maintain Google's connections with the open-source community, e.g. student programs (Summer of Code, Code-in), nomination-based bonus payments to Google-external open-source contributors, monthly events with multiple sessions around open-source, dedicated blogs and social media channels and OSPO ambassadors.

### 5.1.2 GitLab

The GitLab team handbook<sup>46</sup> describes how the company is run, covering many enterprise functions from sales to finance, from human resources to marketing. Open-source is covered in the engineering section<sup>47</sup>. With regard to using open-source, it mostly focuses on license issues, with the exception of recommendations regarding project forks. It does not mention any security requirements or policies regarding the consumption of upstream open-source projects.

With regard to releasing new open-source projects, the handbook refers to the general guidelines<sup>48</sup>, which also cover company related projects. In this context, the categorization of projects decides about the applicability of security policies<sup>49</sup>, e.g. the use of SAST or dependency scanners (cf. Figure 5).

---

<sup>42</sup> Docs, Google Open Source, Accessed online at: <https://opensource.google/docs>

<sup>43</sup> *Ibid.*

<sup>44</sup> *Ibid.*

<sup>45</sup> *Ibid.*

<sup>46</sup> Handbook, GitLab, Accessed online at: <https://about.gitlab.com/handbook/>

<sup>47</sup> We believe in Open Source, GitLab, Accessed online at <https://about.gitlab.com/handbook/engineering/open-source/>

<sup>48</sup> *Ibid.*

<sup>49</sup> *Ibid.*

Categories	Policies
red-data, product, library	SAST, Dependency Scanning and Secret Detection must be enabled
use_pat, website + external	Dependency Scanning and Secret Detection must be enabled
website + external + yellow/orange/red_data	DAST must be enabled. Overall SSL grade must be 'A' or 'A+'
keep_private	Project visibility must be private
library   use_pat   website   api/service   green/yellow/red-data   3rdparty	Default branch must be protected (Allowed to merge: Maintainers, Allowed to push: Maintainers)

Figure 5: Mapping of security policies to project categories.

### 5.1.3 Zalando

Zalando's open-source documentation<sup>50</sup> is structured into three sections (1) *Using*, (2) *Releasing* and (3) *Promoting* open-source. The use of open-source focuses on license compliance, thereby allowing and forbidding certain licenses, as well as on contributor license agreements in regard to contributions to existing external open-source projects. Security requirements or policies are not mentioned.

The release of open-source follows a defined process starting with management sign-off, and finishing with the review of the repository before its release on GitHub. Zalando uses the MIT license when releasing open-source projects. Security is only mentioned in the repository's preparation phase, where developers are asked to avoid the use of vulnerable dependencies, and the leakage of credentials or other confidential data.

### 5.1.4 Yahoo

The Yahoo open-source developer guide<sup>51</sup> is structured into using open source, publishing a new open-source project, contributing to open-source projects, launching mobile apps, promoting projects and accepting contributions. Guidelines regarding the use of open-source only cover license compliance. The publication of new projects mentions a 3-step process. In general, Yahoo prefers permissive licenses, and the scrubbing of repositories mentions as two security requirements to remove any credentials or other secrets as well as to "perform any paranoid-required code review for vulnerabilities in static code or dependencies"<sup>52</sup>.

### 5.1.5 FINOS Reference FOSS Policy for Financial Services Institutions

The Fintech Open-Source Foundation (FINOS) provides a template for a comprehensive free and open-source software policy for financial services institutions<sup>53</sup>. This template proposes provisions regarding three different areas: (1) FOSS Use Policy, (2) FOSS Modification Policy and (3) FOSS Contribution and Publication Policy.

<sup>50</sup> Documentation. Zalando's Open Source Documentation, Zalando, Accessed online at: <https://open-source.zalando.com/docs>

<sup>51</sup> Yahoo Open Source Developer Guide, Yahoo, Accessed online at: <https://yahoo.github.io/oss-guide/>

<sup>52</sup> <https://yahoo.github.io/oss-guide/docs/publishing/prepare.html#scrub-your-repository>

<sup>53</sup> <https://github.com/finos/reference-foss-policy/blob/master/src/FINOS-reference-FOSS-policy.adoc>

Regarding the consumption of open-source, the (1) FOSS Use Policy prescribes the use of a dedicated request system with which project teams can request the use of open-source components. This review process includes a security review with tools, and possibly 3<sup>rd</sup>-party audits, and the obligation to check for known vulnerabilities using the NVD and to fix outstanding critical vulnerabilities identified through scanning. It furthermore includes a risk analysis to identify legal, financial security and other risks, demands the separate maintenance of the open-source code and more security controls throughout the use of the open-source component.

The (2) FOSS Modification Policy makes provisions regarding modifications of open-source components, e.g., the need to request approval for such, the tracking of code changes or compliance with its license terms. Finally, the (3) FOSS Contribution and Publication Policy states requirements regarding open-source contributions, both small ones to existing open-source projects, as well as the creation of new projects.

### 5.1.6 Summary

In conclusion, the review of five high-level and publicly available open-source policies showed that the differences are significant in the level of detail: FINOS' reference policy for financial institutions as well as Google's internal documentation provide a number of detailed provisions and recommendations on how to consume and contribute open-source. In particular, they describe concrete, readily applicable safeguards on how to securely consume open-source.

In more detail, their recommended safeguards related to secure open-source consumption comprise:

- An internal system and processes for submitting, discussing, and resolving open-source use and contribution requests, linked to a review board that investigates various risks related to open-source use (e.g. license, security, strategy, reputation).
- The local storage and maintenance of source code of consumed open-source projects, which results in the necessity to build those projects locally.
- The identification or appointment of owners of consumed open-source components, with defined responsibilities concerning the component's in-house use.
- Defined activities related to the disclosure of vulnerabilities in used open-source, e.g. the implementation of safeguards or the notification of downstream users.

Unfortunately, the publicly available material of other companies focused much more on just two aspects: Acceptable licenses that can be used for internal consumption, and the contribution of open-source. With regards to security, the provisions mostly focus on the scrubbing of codebases before releasing them as open-source, in order to prevent the leakage of sensitive information like authentication credentials. Only Zalando explicitly mentions to also look for project dependencies with known vulnerabilities before releasing a given project under open-source license terms.

## 5.2 Regulatory Initiatives, Open Standards and Certification Schemes

Security threats stemming from software supply chains are also recognized by government bodies. Although, within the scope of this deliverable, national schemes, such as SecNumCloud in France or the C5 methodology from BSI in Germany, are not considered.

For instance, both the White House Executive Order on Improving the Nation's Cybersecurity<sup>54</sup>, issued in May 2021, and the candidate European Union Cybersecurity Certification Scheme for Cloud Services (EUCS)<sup>55</sup>, published by the ENISA in Dec 2020, mention open-source security explicitly.

---

<sup>54</sup> *Executive Order on Improving the Nation's Cybersecurity*, White House, Accessed online: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

<sup>55</sup> ENISA, 2020, EUCS – Cloud Service Scheme. A candidate cybersecurity certification scheme for cloud services, *European Union Agency for Cybersecurity*.

The ENISA has further published a dedicated report on the threat landscape for supply chain attacks in July 2021<sup>56</sup>, acknowledging the increase in number and sophistication of supply chain attacks.

### **5.2.1 EU Cybersecurity Certification Scheme for Cloud Services (EUCS)**

The candidate scheme for EUCS requires, as part of DEV-02 (Development Supply Chain Security), that cloud service providers maintain a list of dependencies used throughout service development (DEV-02.1), document and implement policies related to the use of third-party and open-source (DEV-02.2), make software bill of materials available to customers (DEV-02.3) and perform risk assessment for every procured and development-related product (DEV-02.4).

Which requirements have to be met by a given cloud service provider depends on the targeted assessment level. The (1) basic assurance level, which relates to services for non-critical data and systems, only requires service providers to meet DEV-02.1. The (2) substantial assurance level, which addresses services for business-critical data and systems, requires providers to meet DEV-02.1 to DEV-02.3. Finally, the (3) high assurance level is intended for mission-critical systems and data *“to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources”*. It requires providers to meet all four requirements.

Requirement DEV-02.2, in particular, is inspired by the OWASP Software Component Verification Standard (cf. next Section), thus, the policies should cover aspects such as component age, components that are end-of-life or end-of-service or exclusion criteria for components with known vulnerabilities.

### **5.2.2 White House Executive Order from May 12, 2021**

The executive order demands, as part of Section 4, Enhancing Software Supply Chain Security, the creation of guidelines that *“include criteria that can be used to evaluate software security, include criteria to evaluate the security practices of the developers and suppliers themselves, and identify innovative tools or methods to demonstrate conformance with secure practices”*. Further guidance shall include standards, procedures and criteria regarding, e.g., development and build environments, the use of automated tools to detect known and potential vulnerabilities, or code integrity and provenance, with a particular mentioning of open-source software. Such guidance will need to be followed by all government agencies when procuring software.

### **5.2.3 OWASP Software Component Verification Standard**

In June 2020, the Open Web Application Security Project (OWASP) published version 1.0 of the Software Component Verification Standard (SCVS), which provides a set of activities, controls and best-practices to reduce software supply chain risks<sup>57</sup>.

These activities and controls are organized in the following six categories: Inventory (10 controls), Software Bill of Materials (18), Build Environment (21), Package Management (19), Component Analysis (12) as well as Pedigree and Provenance (7).

The SCVS also introduces three certification levels for low-assurance requirements, moderately sensitive software and high-assurance requirements. For each of the categories mentioned above, the different certification levels require an increasing set of safeguards to meet the respective level.

---

<sup>56</sup> ENISA, 2021, ENISA Threat Landscape for Supply Chain Attacks, *European Union Agency for Cybersecurity*.

<sup>57</sup> SCVS. *Software Component Verification Standard. Version 1.0.*, OWASP Standard, Accessed online at: <https://owasp-scvs.gitbook.io/scvs>



Finally, the SCVS recommends that all organizations consuming open-source should have a corresponding open-source policy, and suggest a couple of topics to be covered by such policy, e.g. component age and update strategies or acceptable version ranges.

### 5.2.4 Supply Chain Levels for Software Artifacts (SLSA)

The Open-Source Security Foundation (OpenSSF) provides tools, services, training, infrastructure and resources to achieve their vision of an open-source ecosystem, where security is handled proactively and by default.

In June 2021, the OpenSSF proposed an end-to-end framework<sup>58</sup> for ensuring the integrity of software artifacts throughout the software supply chain. The framework is called Supply chain Levels for Software Artifacts (SLSA)<sup>59</sup>, and primarily addresses supply chain attacks as seen in Figure 6. It is inspired by an internal framework used at Google for more than eight years, and which is mandatory for all of Google's production workloads.

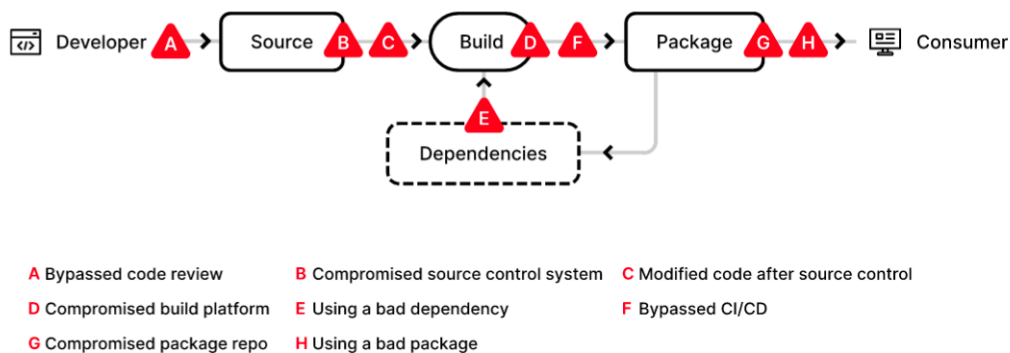


Figure 6: SLSA Supply Chain Threats (Copyright 2021 The Linux Foundation).

SLSA consists of four security levels, whereby each level imposes certain requirements on a software development project. The levels are incremental and the requirements are grouped into four categories related to source code (4 requirements), the build process (8), provenance information (5) as well as common security properties (3).

At the time of writing, SLSA is a collection of best-practices, but the final goal is to make it automatically enforceable, both in regards to the creation of auditable metadata for specific packages and build platforms, consumed by policy engines to give "SLSA certification", as well as by open-source consumers.

### 5.2.5 Know, Prevent, Fix: A framework for shifting the discussion around vulnerabilities in open source

In February 2021, Google proposed a framework called "Know, Prevent, Fix"<sup>60</sup> to improve the developers' handling of vulnerabilities in upstream open-source software components.

The first objective of the framework relates to the identification of vulnerabilities in open-source, which requires the availability of a precise and standardized schema for vulnerability metadata.

<sup>58</sup> *Improving artifact integrity across the supply chain*, SLSA, Accessed online at: <https://slsa.dev/>

<sup>59</sup> *Introducing SLSA, an End-to-End Framework for Supply Chain Integrity*, Google Security Blog, Accessed online at: <https://security.googleblog.com/2021/06/introducing-slsa-end-to-end-framework.html>

<sup>60</sup> *Know, Prevent, Fix: A framework for shifting the discussion around vulnerabilities in open source*, Google Security Blog, Accessed online at: <https://security.googleblog.com/2021/02/know-prevent-fix-framework-for-shifting.html>

The second objective aims at preventing for new vulnerabilities to enter a development project. This goal can be supported by security ratings, e.g. OpenSSF's security scorecards<sup>61</sup>.

The third and last objective relates to fixing and removing vulnerabilities, e.g. by updating to non-vulnerable versions (if available and possible), or by contributing fixes to the affected open-source project.

## 5.3 The different results of SPARTA

As was identified in the Exploitation definition, the SPARTA results are software, databases and processes. This section introduces and positions several of the works conducted in SPARTA's CAPE program with respect to open-source programs, regulatory instruments and open standards outlined in previous sections of Chapter 4. Some of those contributions take the form of datasets ("Backstabber's Knife Collection" and "Project KB"), while others are tools. They all have in common to secure the consumption of software components produced by open-source projects.

### 5.3.1 BuildWatch (UBO)

BuildWatch<sup>62</sup>, developed by the University of Bonn, is based on the well-known malware sandbox Cuckoo<sup>63</sup>. It detects and filters suspicious activities that happen during project builds, e.g. network activity or file system access. As such, it can be considered a detective control, used by open-source consumers to spot whether open-source components (or component updates) show malicious behaviour. The features provided by BuildWatch relate to SCVS's certification requirements in category V3<sup>64</sup> (Build Environment).

Inspired by BuildWatch, GitLab, one of the leading Git hosters, implemented the very same approach for dockerized build systems<sup>65</sup>. Approach and tool were also presented to Greenbone, a German SME offering the OpenVAS vulnerability scanner.

### 5.3.2 Backstabber's Knife Collection (UBO, SAP)

Backstabber's Knife Collection<sup>66</sup>, developed by the University of Bonn and SAP, is an open-source dataset of malicious open-source packages used in real-world attacks. This dataset is an invaluable resource supporting the development of preventive and detective safeguards.

It attracted the interest of commercial players such as Sonatype or IQT Labs, both of which actively contribute to the dataset. As of November 19, 2021, a total of 42 individuals were granted access to the repository, both from commercial organizations like GitLab, Fastly, Spotify, Palo Alto Networks and others, as well as from universities from all around the world.

---

<sup>61</sup> *OSSF/Scorecard*, Github Repository, Accessed online on 07.12.2021, <https://github.com/ossf/scorecard>

<sup>62</sup> Ohm, M., Sykosch, A. and Meier, M., 2020, August. Towards detection of software supply chain attacks by forensic artifacts. In *Proceedings of the 15th international conference on availability, reliability and security* (pp. 1-6).

<sup>63</sup> *What is Cuckoo*, Cuckoo, Available online at: <https://cuckoosandbox.org/>

<sup>64</sup> *V3 Build Environment*, OWASP Standard, Available online at: <https://owasp-scvs.gitbook.io/scvs/v3-build-environment>

<sup>65</sup> *Meet Package Hunter: A tool for detecting malicious code in your dependencies*, Gitlab, Accessed online at: <https://about.gitlab.com/blog/2021/07/23/announcing-package-hunter/>

<sup>66</sup> *Backscatter Night Collection*, Accessed online at: <https://dasfreak.github.io/Backstabbers-Knife-Collection/>





The dataset has been used as part of the security analysis of GitHub Copilot<sup>67</sup>, to check whether Copilot's ML models suggest the use of typo-squatted and malicious Python components. Moreover, the University of Bonn received a request from the Israeli start-up Illustria to use the dataset for their offering.

### 5.3.3 Interactive Attack Tree (SAP)

The interactive attack tree for open-source supply chain attacks, developed by SAP, aims at providing a comprehensive taxonomy for possible attack vectors on open-source based software development projects. It takes the form of an attack tree, whereby each leaf node represents an attack vector, and comes with references to corresponding real-world incidents and appropriate safeguards. As such, the taxonomy somewhat overlaps with the taxonomy proposed by ENISA in their document "Threat Landscape for Supply Chain Attacks"<sup>68</sup>. However, their taxonomy is much less fine-grained regarding possible attack vectors, and instead covers also the victim's perspective and possible impact.

The attack tree will be published on a dedicated website to support various use-cases, e.g. to raise awareness among developers, to guide penetration tests of development infrastructures or to serve threat modelling activities.

Both the Backstabber's Knife Collection as well as the interactive attack tree have been presented at several public events, e.g. Webinars organized by SAP or the German SAP User Group (DSAG). We also received an invitation to present those works to several work groups of the Open-Source Security Foundation (OpenSSF), including the work group "Supply Chain Integrity", which produced the SLSA framework (cf. Section 5.2.4).

### 5.3.4 Eclipse Steady (SAP)

Eclipse Steady, initially developed by SAP and now part of the Eclipse Software Foundation, is also a detective control that supports application developers in the detection, assessment and mitigation of open-source code with known vulnerabilities. Ideally, it is periodically triggered by automated CI/CD pipeline jobs throughout the whole software development lifecycle. The features provided by Steady support developers to meet several of SCVS's certification requirements in the categories V3<sup>69</sup> (Build Environment) and V5<sup>70</sup> (Component Analysis) (3.20, 5.4, 5.5, 5.7, 5.10).

As part of SPARTA, its first official Eclipse release has been created following ESF's release process (v3.2.0, released in June 2021). Several improvements developed in the context of SPARTA are meant to lower the barrier for using and contributing to Eclipse Steady, e.g. by improving the usability and footprint of its Docker Compose application.

In November 2021, the first release of OSPO Alliance's open-source governance handbook<sup>71</sup> highlights Eclipse Steady to detect and manage known open-source vulnerabilities. The same month, it is listed among the SCA tools in TODO Group's OSPO landscape<sup>72</sup> (see Figure 7).

---

<sup>67</sup> Chen, M., Tworek, J., Jun, H., Yuan, Q., Pinto, H.P.D.O., Kaplan, J., Edwards, H., Burda, Y., Joseph, N., Brockman, G. and Ray, A., 2021. Evaluating large language models trained on code. *arXiv preprint arXiv:2107.03374*.

<sup>68</sup> ENISA, *supra nota*, 43

<sup>69</sup> OWASP Standard, *supra nota*, 57

<sup>70</sup> V5 Component Analysis, OWASP Standard, Accessed online at: <https://owasp-scv.s.gitbook.io/scvs/v5-component-analysis>

<sup>71</sup> OW2 & The Good Governance Initiative participants, 2021, *Open-Source Good Governance Handbook*. V.1.0.

<sup>72</sup> OSPO Landscape, OSPO, Accessed online at: <https://landscape.todogroup.org/>

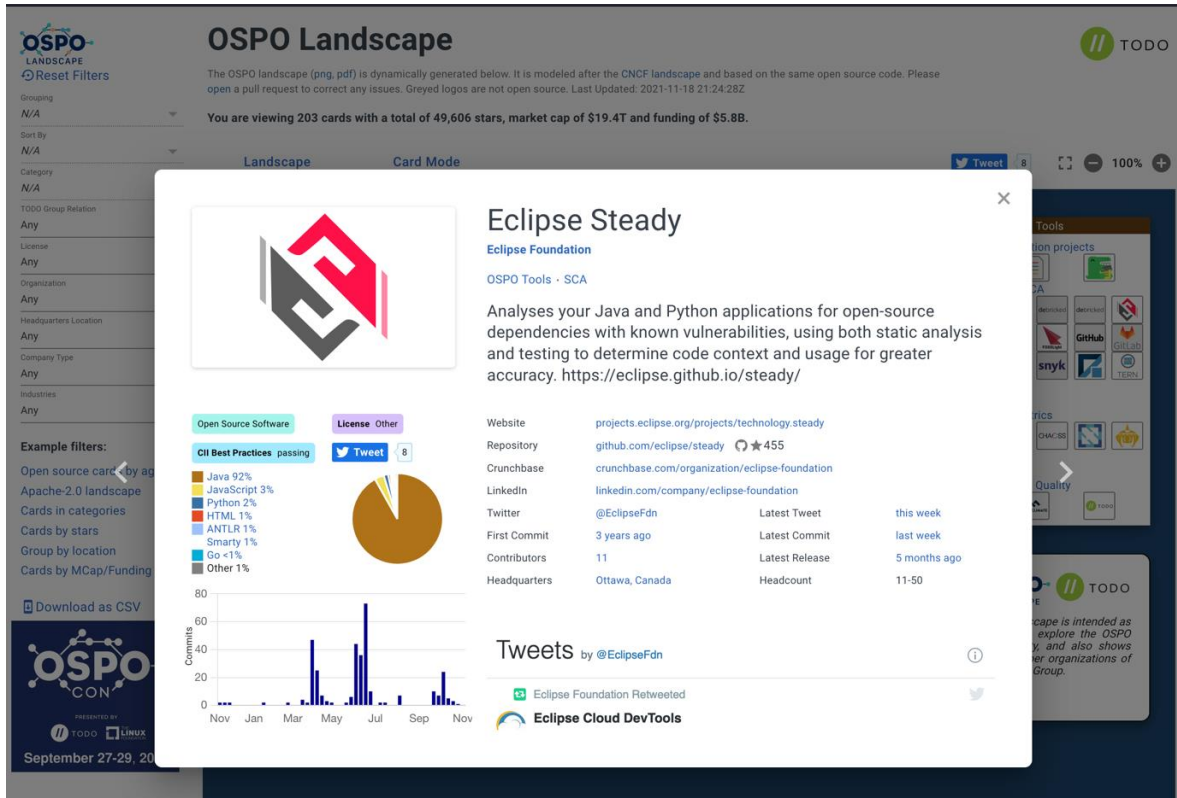


Figure 7: Eclipse Steady in TODO Group's OSPO landscape

### 5.3.5 Project KB (SAP)

Project KB<sup>73</sup>, developed by SAP, is an open-source dataset with code-level information about open-source vulnerabilities. The datasets fuels Eclipse Steady, which needs the detailed, code-level vulnerability information in order to perform its various code analyses. Note that work on this dataset and related tooling is continued as part of the EU research project AssureMOSS (grant agreement 952647).

Both Eclipse Steady and Project KB have been presented at several public events, e.g. during the EclipseCon 2019 and 2020, Eclipse SAM IoT 2020 or as part of a 2 hours lecture at the University of Salerno.

### 5.3.6 VulnEx (UKON)

VulnEx, developed by the University of Konstanz, reads and aggregates information read from Eclipse Steady in order to support OSPOs and other organizational stakeholders in the organization-wide analysis of open-source consumption and open-source vulnerabilities. As reported in the scientific paper accepted at VizSec 2021<sup>74</sup>, industry experts in open-source vulnerability management provided initial requirements and positively evaluated the tool.

<sup>73</sup> SAP/Project-kb, Accessed online at: <https://github.com/sap/project-kb>

<sup>74</sup> F. L. Dennig, E. Cakmak, H. Plate and D. A. Keim, "VulnEx: Exploring Open-Source Software Vulnerabilities in Large Development Organizations to Understand Risk Exposure", 2021 IEEE Symposium on Visualization for Cyber Security (VizSec), 2021

## Chapter 6 Conclusion

The preparation of Deliverable 10.5 has brought out several aspects on what to reflect on and to consider in any future exploitation activities. The Exploitation Roadmap creates a comprehensive set of tools to strategically plan exploitation activities, especially when transferring technology from a research institution into a commercial exploitation. It is paramount that Exploitation Roadmap with accompanying indicators are created and set in place at the beginning of the project to facilitate faster streamlining of technological innovation into private sphere.

The Exploitation Hackathons and following Startup Mentorships have provided a unique understanding on practical opportunities and activities to incentivize transfer of results from a project or a research institution to an external team. Chapter 4 provides several lessons learned and recommendations to consider when planning on conducting Exploitation Hackathon events. Unfortunately, there was not sufficient time to conclude the second Startup Mentorship and have more detailed information on lessons learned for the Mentorship program. The first iteration of the Mentorship program indicated several challenges that should be addressed in the second iteration. These were taken into consideration in planning the approach for a 12 months long Startup Mentorship. However, as the second iteration begins in June 2022, the results will not be reviewable within the scope of SPARTA project. Therefore, the activities based on the Startup Mentorship will be reached within 2023 after the end of SPARTA project.

## Chapter 7 List of Abbreviations

Abbreviation	Translation
API	Application Programming Interface
CRI	Commercial Readiness Index
DSAG	German SAP User Group
EC	European Commission
ENISA	The European Union Agency for Cybersecurity
EUCS	European Union Cybersecurity Certification for Cloud Services
EUPL	European Union Public License
FINOS	Fintech Open-Source Foundation
FOSS	Free and Open-Source Software
GDPR	The General Data Protection Regulation
HBP	Human Brain Project
ICT	Information Communication Technology
IPR	Intellectual Property Regulation
KPI	Key Performance Indicator
NASA	The National Aeronautics and Space Administrator
NDA	Non-Disclosure Agreement
OpenSSF	Open-Source Security Foundation
OSPO	Open-Source Program Offices
OWASP	Open Web Application Security Project
R&D	Research and Development
SAST	Static Application Security Testing
SCA	Strong Customer Authentication
SCVS	Software Component Verification Standard
SLSA	Supply Chain Levels for Software Artifacts
SME	Small and Medium Enterprise
TFEU	The Treaty of the Functioning of the European Union
TRL	Technology Readiness Level
UBO	University of Bonn
UKON	University of Konstanz

## Chapter 8 Bibliography

### European Union Sources

1. ENISA, 2020, EUCS – Cloud Service Scheme. A candidate cybersecurity certification scheme for cloud services, *European Union Agency for Cybersecurity*.
2. ENISA, 2021, ENISA Threat Landscape for Supply Chain Attacks, *European Union Agency for Cybersecurity*.
3. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (Database Directive).
4. Regulation 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Free Flow Regulation).
5. Directive 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information.

### Articles

1. Boletsis, C., Halvorsrud, R., Pickering, J.B., Phillips, S.C. and SurrIDGE, M., 2021, February. Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment. In *VISIGRAPP (3: IVAPP)*(pp. 266-274).
2. Straub, J., 2021, April. Evaluating the Use of Technology Readiness Levels (TRLs) for Cybersecurity Systems. In *2021 IEEE International Systems Conference (SysCon)* (pp. 1-6). IEEE.
3. Héder, M., 2017. From NASA to EU: the evolution of the TRL scale in Public Sector Innovation. *The Innovation Journal*, 22(2), pp.1-23.
4. Kapletia, D., Felici, M. and Wainwright, N., 2014, May. An integrated framework for innovation management in cyber security and privacy. In *Cyber Security and Privacy Forum* (pp. 135-147). Springer, Cham.
5. Kapletia, D., Felici, M. and Wainwright, N., 2014, May. An integrated framework for innovation management in cyber security and privacy. In *Cyber Security and Privacy Forum* (pp. 135-147). Springer, Cham., 136.
6. Blind, K., Böhm, M., Grzegorzewska, P., Katz, A., Muto, S., Pätsch, S. and Schubert, T., 2021. The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy., 57.
7. Blind, K. and Böhm, M., 2019. The Relationship Between Open Source Software and Standard Setting, Thumm, N.(Ed.) EUR 29867 EN, JRC (Joint Research Centre) Science for Policy Report, Publications Office of the European Union, Luxembourg, 2019.
8. Support Centre for data sharing, *B2 – Analytical report on EU law applicable to sharing of non-personal data*, 24 January 2020.
9. Ohm, M., Sykosch, A. and Meier, M., 2020, August. Towards detection of software supply chain attacks by forensic artifacts. In *Proceedings of the 15th international conference on availability, reliability and security* (pp. 1-6).
10. Chen, M., Tworek, J., Jun, H., Yuan, Q., Pinto, H.P.D.O., Kaplan, J., Edwards, H., Burda, Y., Joseph, N., Brockman, G. and Ray, A., 2021. Evaluating large language models trained on code. *arXiv preprint arXiv:2107.03374*.
11. OW2 & The Good Governance Initiative participants, 2021, *Open-Source Good Governance Handbook. V.1.0*.



## Online Sources

12. *Dissemination & Exploitation of Results*, European Commission Funding and Tender opportunities, accessed online 10.08.2021, [https://ec.europa.eu/research/participants/docs/h2020-funding-guide/grants/grant-management/dissemination-of-results\\_en.htm](https://ec.europa.eu/research/participants/docs/h2020-funding-guide/grants/grant-management/dissemination-of-results_en.htm)
13. *Overview*, Human Brain Project, accessed online 22.11.2021, <https://www.humanbrainproject.eu/en/about/overview/>
14. *Exploitation Plan Course*, Human Brain Project, accessed online 22.11.2021, <https://www.humanbrainproject.eu/en/collaborate/exploitation-plan-course/>
15. *Exploitation Plan Course*, Human Brain Project, accessed online 10.08.2021, <https://www.humanbrainproject.eu/en/collaborate/exploitation-plan-course/>
16. *Copyright*, WIPO, accessed online 10.08.2021, <https://www.wipo.int/copyright/en/>
17. *A Brief History of Touchscreen Technology*, Accessed online on 25.11.2021, <https://www.zytronic.co.uk/insights/article/history-of-touchscreen-technology/>
18. *How and Why Google Glass Failed?*, Accessed online on 29.11.2021, <https://www.investopedia.com/articles/investing/052115/how-why-google-glass-failed.asp>
19. *A Timeline: A brief History of Apple Watch*, Accessed online on 29.11.2021, <https://www.verizon.com/articles/brief-history-of-apple-watch/>
20. Investopia, *What is an intangible asset?*, Accessed online 04.04.2012,
21. <https://www.investopedia.com/terms/i/intangibleasset.asp>
22. *Talk Openly, Develop Openly*, TODO Group, Accessed online 07.12.2021, <https://todo-group.org>
23. *OSPO Zone*, OSPO Zone, Accessed online 07.12.2021, <https://ospo.zone>
24. *Docs*, Google Open Source, Accessed online at: <https://opensource.google/docs>
25. *Handbook*, GitLab, Accessed online at: <https://about.gitlab.com/handbook/>
26. *We believe in Open Source*, GitLab, Accessed online at <https://about.gitlab.com/handbook/engineering/open-source/>
27. *Documentation. Zelando's Open Source Documentation*, Zelando, Accessed online at: <https://opensource.zalando.com/docs>
28. *Yahoo Open Source Developer Guide*, Yahoo, Accessed online at: <https://yahoo.github.io/oss-guide/>
29. <https://yahoo.github.io/oss-guide/docs/publishing/prepare.html#scrub-your-repository>
30. <https://github.com/finos/reference-foss-policy/blob/master/src/FINOS-reference-FOSS-policy.adoc>
31. *Executive Order on Improving the Nation's Cybersecurity*, White House, Accessed online: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>
32. *SCVS. Software Component Verification Standard. Version 1.0.*, OWASP Standard, Accessed online at: <https://owasp-scvs.gitbook.io/scvs>
33. *Improving artifact integrity across the supply chain*, SLSA, Accessed online at: <https://slsa.dev/>
34. *Introducing SLSA, an End-to-End Framework for Supply Chain Integrity*, Google Security Blog, Accessed online at: <https://security.googleblog.com/2021/06/introducing-slsa-end-to-end-framework.html>
35. *Know, Prevent, Fix: A framework for shifting the discussion around vulnerabilities in open source*, Google Security Blog, Accessed online at. <https://security.googleblog.com/2021/02/know-prevent-fix-framework-for-shifting.html>
36. *OSSF/Scorecard*, Github Repository, Accessed online on 07.12.2021, <https://github.com/ossf/scorecard>
37. *What is Cuckoo*, Cuckoo, Available online at: <https://cuckoosandbox.org/>
38. *V3 Build Environment*, OWASP Standard, Available online at: <https://owasp-scvs.gitbook.io/scvs/v3-build-environment>
39. *Meet Package Hunter: A tool for detecting malicious code in your dependencies*, Gitlab, Accessed online at: <https://about.gitlab.com/blog/2021/07/23/announcing-package-hunter/>
40. *Backscatter Night Collection*, Accessed online at: <https://dasfreak.github.io/Backstabbers-Knife-Collection/>



41. *V5 Component Analysis*, OWASP Standard, Accessed online at: <https://owasp-scvs.github.io/scvs/v5-component-analysis>
42. *OSPO Landscape*, OSPO, Accessed online at: <https://landscape.todogroup.org/>
43. *SAP/Project-kb*, Accessed online at: <https://github.com/sap/project-kb>
44. *Appendix A: Guidelines for the Definition on the software technology readiness level*, European Space Agency, Accessed online on 02.12.2021, [https://artes.esa.int/sites/default/files/TRL\\_Handbook.pdf](https://artes.esa.int/sites/default/files/TRL_Handbook.pdf)
45. *Funding for SMEs and mid-caps*, EU Funding Playbook, Accessed online on 14.12.2021, <https://eufundingplaybook.fi/small/>.
46. *Explainer: As cybercrime evolves, how can companies keep up with their cybersecurity?* World Economic Forum, Accessed online on 24.01.2022. <https://www.weforum.org/agenda/2021/11/cyber-security-evolving-cyber-crime-attacks/>

## Chapter 9 Annexes

### 9.1 Annex 1: Exploitation Roadmap: Technology Readiness Level (TRL), Commercial Readiness Index (CRI) and Intellectual Property Rights (IPR) Correspondence Table

This table aims at providing partners with understanding of the technology readiness level of their developed technology and the ensuing implications in terms of commercial readiness. It has an informative value and serves as a guide through the different stages of technology and commercial readiness of the result, helping in knowing what has to be considered before hypothetical commercial exploitation.

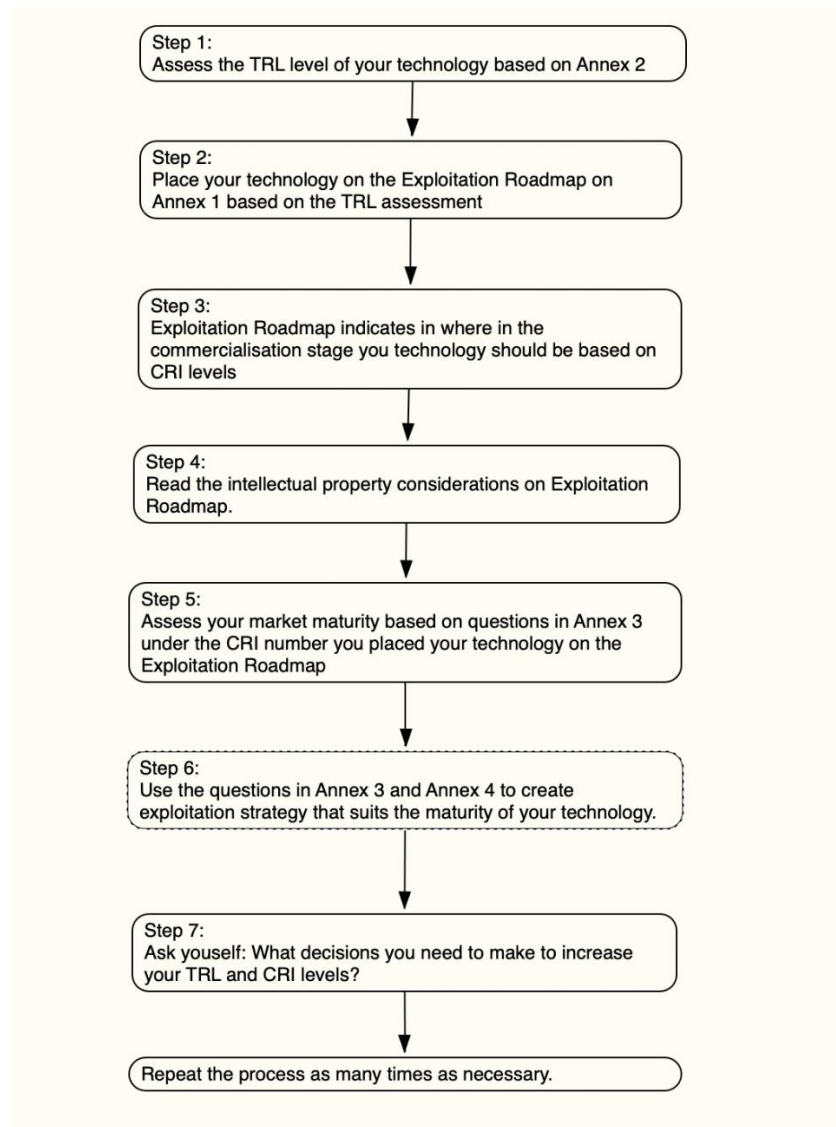


Figure 8: Step by step on how to use the Exploitation Roadmap in Annexes 1 - 4.



Commer- cialization Phases	TRL	Corresponding Cyber Descrip- tion	Commer- cial Read- iness Indi- cator	CRI De- scrip- tion	Copyright	Open Source	Proprietary	Trade Secret	Patent
R&D	TRL 1	Cyber Capability Research			Copyright is authors right and is automatic and belongs to the creator of software, databases and technical drawings.* Applicable if results are published in peer-reviewed articles. In the context of SPARTA this applies to research to the point of building theoretical concept. Applicable of first part of R&D.		Most commonly used IPR regime in commercial ICT R&D. License needs to be agreed before use of software. During R&D period, NDA-s should be used by employees and partners. Software can be registered at a notary in order to establish its legal status as proprietary or contractual clauses can be used.	R&D activities should be conducted inhouse without external peer-review on the underlying technology. This requires a high R&D capability and inhouse investments. In order to keep the result a secret, NDA-s should be in place with employees and with all business partners that one collaborates during the R&D phase.	Exclusive right granted to a product or a process. Patent is not applicable to use on software, databases and technical drawings. There is likely little use for patents in SPARTA. However, patent should be applied for during the R&D period, latest when proof-of-concept designs are finalized at NASA TRL 5 or TRL 6. It would be advised to refrain from publishing articles on design and underlying technology until the patent application is submitted.
	TRL 2	Cyber Capability Concept							
	TRL 3	Cyber Capability Proof-of-Concept							
	TRL 4	Cyber Capability Demonstration							
	TRL 5	Cyber Capability Conceptual Design							
	TRL 6	Cyber Capability Preliminary Design							
Demon- stration	TRL 7	Cyber Capability Detailed Design	CRI 1	Pilot Scale - hypothetical commercial proposition	Even if Copyright is automatic, it does not grant economic right on its own without additional legal protection. The owner has the right to sue an unauthorized use but once the information is public, it allows for others to add elements which can result in a new original work or addition. The	Publishing the source code as an open source using one of several OS licenses available	Same as R&D phase	Demonstration and investment phase similarly requires strict NDA-s and run a	Protected by patent application or granted patent



Commercialization Phases	TRL	Corresponding Cyber Description	Commercial Readiness Indicator	CRI Description	Copyright	Open Source	Proprietary	Trade Secret	Patent
	TRL 8	Cyber Capability Unit & Integration Tested			best way to further protect works during the rest of the R&D, Demo and Deployment period is to protect the original work with either adding legal license or protecting the work as trade secret. This, however, restricts the publishing of research results in research articles.			risk of exposing the result to a partner/investor who has no interest in keeping with the NDA and rather steals the secret and pays the fine as the fine could likely be less than the potential profit of the result.	
	TRL 9	Cyber Capability Beta Tested	CRI 2	Commercial trial					
Deployment	TRL 10	Cyber Capability Successfully Deployed	CRI 3	Commercial scale up	The Deployment period of the software depends on the OS community and their adoption of the software. Based on the license, the application and deployment use-cases differ.		Public use of SW only after terms and conditions are accepted. Developer has a warranty requirement each party is liable to.	Product on an open market runs a risk of reverse-engineering. Without additional IPR protection there is no protection if reverse engineering is successfully done and product launched to the market by a competitor	Protected by patent application or granted patent
			CRI 4	Multiple commercial applications					
			CRI 5	Market competition driving widespread deployment					
	TRL 11	Cyber Capability in Successful Secure Persistent Use	RCI 6	Commercially competitive - "Bankable" Grade Asset Class					

## 9.2 Annex 2: TRL Assessment Questionnaire

IP Disclaimer: The TRL levels and questionnaires presented is a synthesis of two published TRL level assessment guides and an article *Evaluating the Use of Technology Readiness Levels (TRLs) for Cybersecurity Systems* by Jeremy Staub<sup>75</sup>. The TRL assessment sourced are: TRL assessment questions is a European Space Agencies' Guideline for the definition of the software technology readiness level; Human Brain Project published HBP Technology Readiness Assessment guide.

The purpose of this questionnaire is to guide partners in assessing the TRL level of their results. By determining, for each TRL level, whether or each proposed affirmation reflects the current status of the developed technology, the partner will be able to determine the actual TRL level of his result. The TRL level is a self-assessment tool in where the elements in the respective levels should be present to grant a given TRL assessment level as reached.

### TRL 1: Cyber Capability Research

1. Basic technology and scientific knowledge underpinning software applications are known.<sup>76</sup>
2. Technology principles and high-level objectives are defined.
3. Supporting information include published research or other references that identify the principles.
4. There is an expression of a problem and a concept of the solution.<sup>77</sup>
5. Feasibility to be implemented in software with available computing facilities are demonstrated.<sup>78</sup>

### TRL 2: Cyber Capability Concept

1. Individual algorithms or functions are prototyped.
2. Documentations on algorithm implementation and results.
3. Practical applications are being identified. At least part of a problem has been identified.
4. Single algorithms are being tested for feasibility and characterization.
5. Feasibility to build critical functions in a system architecture is demonstrated.

### TRL 3: Cyber Capability Proof-of-Concept

1. Analytical studies and small-scale studies to validate the analytical predictions of separate components of the software have been performed.<sup>79</sup>
  2. Architectural design and critical functions are identified without integrating components into a complete system.
  3. Some use cases are being identified. Solutions to several problems are being identified.
  4. A subset of the overall functionality is implemented and tested to allow the demonstration of performance in a simulated laboratory environment.
  5. Feasibility to build an operational system taking into account performance and usability aspects are being demonstrated.
- Feasibility to build an operational system taking into account performance and usability aspects demonstrated

<sup>75</sup> Staub (2021), *supra nota*, 8.

<sup>76</sup> Human Brain Project, *supra nota*, 5.

<sup>77</sup> Appendix A: Guidelines for the Definition on the software technology readiness level, European Space Agency, Accessed online on 02.12.2021, [https://artes.esa.int/sites/default/files/TRL\\_Handbook.pdf](https://artes.esa.int/sites/default/files/TRL_Handbook.pdf)

<sup>78</sup> All further questions are derived from these sources. For the purpose of reducing footnote clutter, the individual footnotes from this point forward will not be added.

<sup>79</sup> Human Brain Project, *supra nota*, 5.

**TRL 4: Cyber Capability Demonstrated**

1. Requirements for solutions to a range of problems specified.
2. Initial architecture documentation available.
3. All use cases are identified and implemented.
4. Verification and Validation (V&V) process is partially completed, or completed for only a subset of the functionality or problem domain. V&V in a representative simulated laboratory environment.
5. Verification and Validation (V&V) process is partially completed, or completed for only a subset of the functionality or problem domain. V&V in a representative simulated laboratory environment.

**TRL 5: Cyber Capability Conceptual Design**

1. Full documentation according to the applicable software standards, which include testing reports and application examples.
  2. Validated against the requirements of the complete domain of applicability. Relevant quality assurance aspects are taken into account.
  3. V&V in laboratory environment, which also include V&V using real data.
  4. Laboratory scale testing has been conducted. Analysis of the differences between laboratory and eventual operating system, and analysis on what the experimental results mean for the eventual operating system/environment have been documented.
  5. All required and relevant data formats are specified.
  6. Feasibility to fix all reported problems within available resources are demonstrated. User support organisation systems are in place.
- Full documentation according to the applicable SW standards, incl testing reports and application examples

**TRL 6: Cyber Capability Preliminary Design**

1. Integrated systems or high-fidelity prototype implementations of the software are tested in a relevant environment under sufficient stress. Operation of the software is being demonstrated on a full-scale realistic problem.
2. The operating environment for the testing represents the actual operating environment.
3. Initial system documentation, user documentation, and final architecture documentation are available.
4. All possible use cases and error handlings are identified and implemented. User friendliness has been validated.
5. V&V process is complete for the intended scope. Configuration control and quality assurance processes are fully deployed.
6. Feasibility to be applied in an operation project has been demonstrated.
7. Ready to be used in an operational/production context. User support is capable of handling operational/production context.

**TRL 7: Cyber Capability Detailed Design**

1. Validation of a prototype software with all key functionality available in a relevant real-world environment.
2. Well integrated with operational software systems demonstrating operational feasibility.
3. Software is mostly cleaned from bugs.
4. Data formats or application programming interfaces no longer change.
5. Supporting information include results from the full-scale testing and analysis of the differences between the test and real-live environment.
6. Final design is virtually complete.
7. Engineering support and maintenance organization in place, including helpdesk.



**TRL 8: Cyber Capability Unit & Integration Tested**

1. The entire software system has been proven to work in its final form under stress and expected conditions. End-to-end system has been created with all of its components.
2. All functionalities are successfully demonstrated in simulated operational scenarios.
3. End-to-end systems are tested and integrated in real world environment with a number of real end-users.
4. User acceptance and performance is tested and debugged.
5. Software has been fully integrated with all operational software systems.
6. All user documentation, training documentation, and maintenance documentation is completed, which include software/system requirements and architecture/design related descriptions.

**TRL 9: Cyber Capability Beta Tested**

1. System is in its final form and operated under full range of operating conditions.
2. Tested in a real-world environment with target number of real users.
3. Sustainable software engineering support is in place
4. Final product operate over the full range of expected conditions.
5. Sustainable engineering, which includes maintenance and upgrades are in place.
6. Technology includes all security aspects in full form.
7. Cybersecurity aspects, their interoperation and their integration with other aspects of the technology has been tested.
8. Test results validate security functionality operability and security requirement satisfaction.

**TRL 10: Cyber Capability Successfully Deployed**

1. System is in use by its target users in real life conditions across multiple missions, operations and/or organizations.
2. System maintenance and upgrades are in continuous use and are functioning in real-life environments.
3. Security performance meets operational performance requirements and known issues are identified, tracked, and resolved using documented process.

**TRL 11: Cyber Capability in Successful Secure Persistent Use**

1. System is continuously in use by target users in real life conditions with increasing stress and traffic.
2. Technology is in wide use.
3. Security performance meets operational performance requirements and known issues are identified, tracked, and resolved using documented process.

### **9.3 Annex 3: IPR and Market Maturity Assessment Roadmap**

CRI assessment can be used hand in hand with assessing legal protection measures while continuously asking several questions that will help in the deciding the most effective intellectual property regime. Most IPR considerations happen during the CRI 1 or the pilot scale as any further CRI stage expects IPR to be settled for any commercial activity to occur.

The following questions are intended to help partners in examining their current situation, providing guidance from an IPR and market maturity perspective.

#### **CRI 1: The Pilot Scale, TRL 1 – 7**

1. Are you researching the topic exclusively academic purposes?
2. Are you planning to publish an academic paper as the result of the research?
3. Is the purpose of the research to develop a commercial application?
4. Is the ALPHA version tested on actual customers?
5. Are you planning to publish the results as an open-source software?
6. Are you using other open-source software in developing your software?
7. Do you know the restrictions of the open-source license used by the baseline technology?
8. Do you know how to protect proprietary license?
9. Have you signed NDA-s with your developers?

## 9.4 Annex 4: CRI and Business Model Assessment Roadmap

The CRI scale assessment questions are based on the assumption that the same entity that is responsible of the R&D process is also responsible for the exploitation activities. In case of a technology transfer to a spin-off, the exploitation activities might be transferred to an external party in a later stage of the R&D in which case the TRL is already higher. In this situation, the assessment questions that are present in the CRI phase 1, should be considered at the stage when exploitation partner is involved and not in the order listed above.

Depending on the current TRL level of the result, the following questionnaire can serve as a guide for partners to self-assess the commercial readiness of their technology and consider its exploitation from a Business Model perspective. The questions are designed to be self-explanatory. The questions are designed to facilitate internal discussion on the topics. Each question should have definitive answer that can be basis to a further decisions-making. The questions are open-ended and can be returned to in later stages.

### CRI 1: Pilot Scale – hypothetical commercial proposition phase, TRL-s 1- 6.

#### TRL 1

1. How is R&D process funded?
2. How investment-heavy is the R&D process?
3. Does R&D at this stage requires additional investments?
4. Which are the R&D IP considerations?
5. Should everyone involved in the R&D be covered with NDA?

#### TRL 2

1. How is R&D process funded?
2. How investment-heavy is the R&D process?
3. Does R&D at this stage requires additional investments?
4. Which are the R&D IP considerations?
5. Should everyone involved in the R&D be covered with NDA?
6. Can you state the problem clearly in 2 sentences?
7. Do you have first-hand experience with the problem?

#### TRL 3

1. How is R&D process funded?
2. Licensing decision should be made at this point
3. Commercial applications should be researched at this point
4. Problem you are solving, should be identified and clear at this point

#### TRL 4

1. Decision of commercial or non-commercial exploitation should be made by this point.
2. Potential commercial applications should be identified
3. Preliminary market research should be conducted
4. IPR of the software should be set, understood and reflected in the legal documentation
5. First round of investments should be conducted or considered
6. Product designation should be made
7. Strong core team should be in place or profile of each member of the core team should be in place. There should be a strategy in place to cover missing competencies.
8. Customer base should be researched. How can you reach your customers?
9. Core team should be committed to work full-time on the project
10. Ideal customer profile should be identified

**TRL 5**

1. Business model should be developed at this point
2. Letters of interests or first customers should be signed
3. Customer profile should be clear and identified at this point
4. Understanding of how often does the problem occur for your customers
5. Severity and intensity of the problem should be identified
6. How desperate is your customer to solve the problem your product is solving?

**TRL 6**

1. Pricing of the product should be made based on the severity of the problem for the customer
2. Can your customer afford your product?
3. Does your MVP actually solve the problem you want it to solve?
4. Feedback loop with customers should be in place and taken into consideration in further iteration of the products

**CRI 2: Commercial Trial Phase, TRL-s 7-8.**

1. First customers are signed up and using the product
2. Functioning feedback loop with customers in terms of meeting customer needs and fixing issues
3. Improving the understanding the problem you are solving
4. Market fit testing
5. Are you talking to your customer?

**CRI 3: Commercial Scale-Up Phase, TRL 9**

1. Are you talking to your customer?
2. Do you know what your customers are doing with your product?

**CRI 4: Multiple Commercial Application Phase, TRL 10**

1. Are you talking to your customers?
2. Do you have explosive usage?
3. What are your customers using your product for?
4. Are you expanding applications of your product?

**CRI 5: Market Competition driving widespread deployment, TRL 11**

1. Are you talking to your customers?

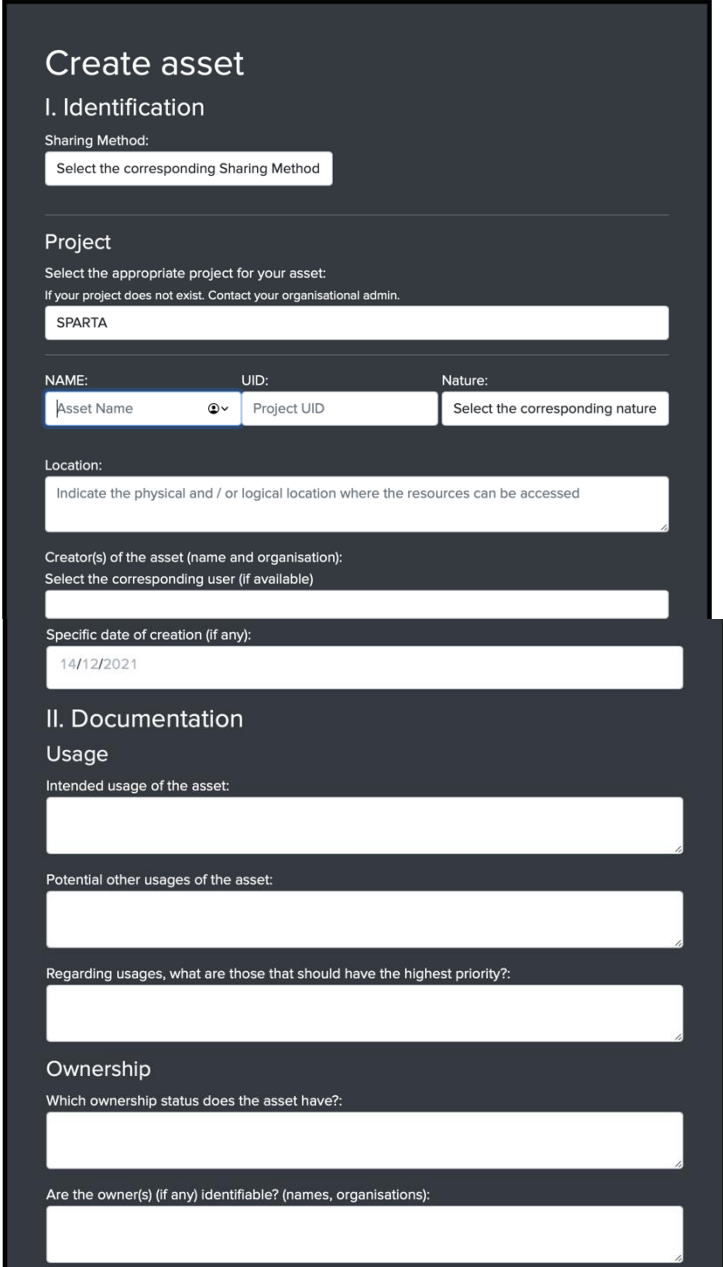
**CRI 6: “Bankable” commercially competitive asset, TRL 11**

1. Are you talking to your customers?

## 9.5 Annex 5: Exploitation support documentation in RAMP

Research Assessment Management Platform (RAMP) has been developed to simplify administrative burden required for EU projects. The following screenshots in this Annex 5 will illustrate the wide variety of assessments and mandatory form required for EU projects.

### 9.5.1.1 Generating an Asset in RAMP



**Create asset**

**I. Identification**

Sharing Method:

**Project**  
 Select the appropriate project for your asset:  
 If your project does not exist. Contact your organisational admin.

NAME:  UID:  Nature:

Location:

Creator(s) of the asset (name and organisation):  
 Select the corresponding user (if available)

Specific date of creation (if any):

**II. Documentation**

**Usage**

Intended usage of the asset:

Potential other usages of the asset:

Regarding usages, what are those that should have the highest priority?:

**Ownership**

Which ownership status does the asset have?:

Are the owner(s) (if any) identifiable? (names, organisations):

**Legal Status**  
Indicate the license type of the asset (if relevant):

Add any other element of information allowing to clarify the legal status of the asset:

**Meta-data**  
Detail the domain specific metadata scheme being used for the asset:

**Specific Documentation**  
Describe how to access the asset's documentation:

Is there specific documentation for the asset:

[Create](#)

### 9.5.1.2 Assessment of Pre-Existing Resources (APER)

**Create APER**  
Select the corresponding asset

Allocation of resources:

[Create](#)



### 9.5.1.3 Create a Data Management Plan (DMP)

RAMP Research Users Organisation Contact Administrator Logout

#### Create DMP

Select the corresponding asset

Select :

#### I. Summary

Name of the dataset:

Reference of the dataset:

Data purpose:

Next

#### Create DMP

#### II. Dataset Description

Origin of the dataset:

Data formats:

Purpose and usability of the dataset:

Data Re-Use:

Expected size:

Previous Next

### Create DMP

#### III. Dataset Localisation

How is the data locatable?:

Are standard naming conventions followed?:

Are search keywords that optimize possibilities for re-use provided?:

In case metadata standards do not exist in your discipline, please outline what type of metadata will be created and how?:

[Previous](#) [Next](#)

Progress indicator: 10 dots, 3rd dot active

### Create DMP

#### IV. Dataset Accessibility

##### Open Data

Indicate which data produced and/or used in the project will be made openly available by default:

Provide a description of this data:

##### Restricted Data

Indicate which data cannot be shared (or need to be shared under restrictions):

##### Access restriction explication

Explain the reasons why data is restricted, clearly separating legal and contractual reasons from voluntary restrictions :



### Create DMP

#### VI. Data re-use

##### Data re-usage description

Indicate which data and for how long it will remain re-usable:

If there is an embargo sought to give time to publish or seek patents, specify why and how long this will apply, bearing in mind that research data should be made available as soon as possible:

##### Data Licensing

Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability. If not, provide mapping to more commonly used ontologies:

##### Third-Party access to the data

Indicate about whether the data produced and/or used in the project is usable by third parties (in particular after the end of the project):

##### Time of reusability

Specify, if possible, the length of time for which the data will remain re-usable:

Previous Next

Progress indicator: 10 dots, 6th dot highlighted



### Create DMP

#### VIII. Data security

##### Backup Procedure

Describe procedures for data backup and recovery:

##### Data Securing Procedure

If any, describe the procedure for transferring sensitive data and secure storage in repositories for long-term preservation and curation:

Previous Next

Progress indicator: 8 dots, 7th dot active

### Create DMP

#### IX. Ethical aspects

##### Ethical Action

Describe actions taken related to privacy and ethical aspects of the data sets:

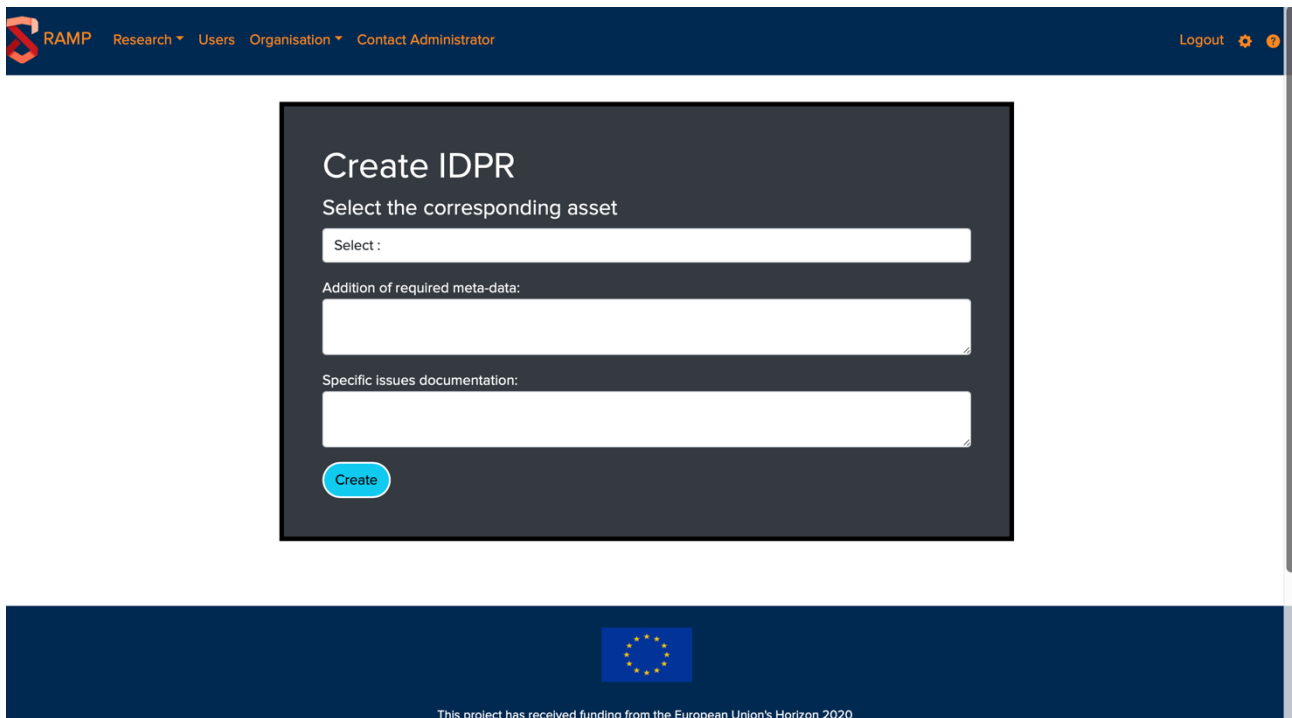
Create Previous

Progress indicator: 8 dots, 8th dot active





### 9.5.1.4 Create an Identification of Produced Results (IDPR)



RAMP Research Users Organisation Contact Administrator Logout

### Create IDPR


Select the corresponding asset

Select :

Addition of required meta-data:

Specific issues documentation:

Create



This project has received funding from the European Union's Horizon 2020