D8.4 Exploitation, Sustainability & Business Plans v1

WP8– Dissemination, sustainability and exploitation

Version: 1.00

SPHINX

A Universal Cyber Security Toolkit for Health-Care Industry

Disclaimer

Copyright message

Document information

Grant Agreement Number	826183	Acronym	SPHINX
Full Title	A Universal Cyber Security Toolkit for Health-Care Industry		
Topic	SU-TDS-02-2018 Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures		
Funding scheme	RIA - Research and Innovation action		
Start Date	1st January 2019	**Duration**	36 months
Project URL	http://sphinx-project.eu/		
EU Project Officer	Reza RAZAVI (CNECT/H/03)		
Project Coordinator	Dimitris Askounis, National Technical University of Athens - NTUA		
Deliverable	D8.4. Exploitation, Sustainability & Business Plans v1		
Work Package	WP8 – Dissemination, sustainability and exploitation		
Date of Delivery	**Contractual** M12	**Actual**	M12
Nature	R - Report	**Dissemination Level**	P - Public
Lead Beneficiary	VILABS		
Responsible Author	Vasiliki	**Email**	mova@vilabs.eu
	Moumtzi	**Phone**	+302310365185
Reviewer(s):	DYPE5, Polaris Medical		
Keywords	Sustainability, cubersecurity, e-health		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Document History

Version	Issue Date	Stage	Changes	Contributor
0.10	17/09/2019	Draft	ToC preparation	ViLabs
0.20	25/11/2019	Draft	Agreement on TOC and Partners' assignments	NTUA, ALL
0.30	18/12/2019	Draft	Deliverable preparation	VILABS
0.40	20/12/2019	Draft	Technical and quality review of pre-final draft	Polaris Medical
0.50	24/12/2019	Draft	Contribution and Reviewed by DYPE5, comments added	Fotios Gioulekas, Evangelos Stamatiadis, Konstantinos Gounaris, Athanasios Tzikas
0.60	28/12/2019	Draft	Deliverable update to reflect comments	VILABS
1.00	30/12/2019	Final	Submission of Final Deliverable to the EC	NTUA

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Executive Summary

This report presents the project outcomes, the overall exploitation plan that the entire consortium will follow to sustain the outcomes beyond the end of the project, and the sustainability plan that paves the way for SPHINX vision to maximise its expected impact. SPHINX platform is the main project outcome and the Business plan will be developed for its future commercialisation by industrial partners. This is the first version of the 'Exploitation, Sustainability & Business Plans' report that will be updated on an annual basis.

Overall, SPHINX will produce six (6) basic exploitation outcomes including; the project platform that will be deployed at the pilots, its individual components that potential future end users will be able to choose which to deploy, services necessary to deploy the platform at the end user sites (consulting services, installation, trainings), best practices and policy recommendations from the implementation of SPHINX platform in replicated real environments and the scientific knowledge that will be generated through the R&D activities.

The outcomes will be exploited by the different partner organisations, in IT Industry, Health Provision Organisations (end users), and Academia. Due to their different nature, each organisation will exploit various outcomes. To do so, SPHINX will develop three basic exploitation options; the business cases for the platform and its components, the replication plan to support Health Provision Organisations to deploy the SPHINX platform and concrete exploitation plans to secure the continuation of the scientific knowledge produced, after the end of the project. These exploitation options will be presented to the targeted audience in order to receive their feedback and engage them in the project activities. Different target audience groups (Industry, Health Provision Organisations, Research, Related EU funded projects, and Policy makers) will be engaged to exploit different outcomes. The image below depicts the SPHINX approach and shows the aforementioned links with the same colours.

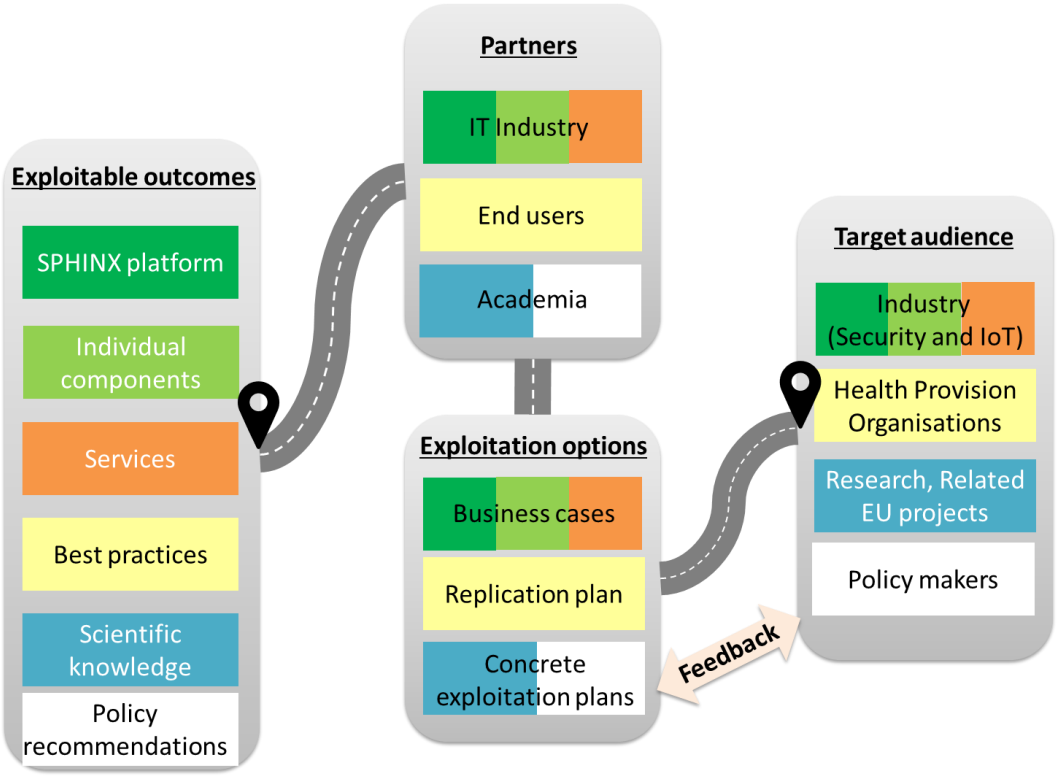

Figure 1: SPHINX overall exploitation approach

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Table of Figures

Table of Tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

1 Introduction

1.1 Purpose & Scope

This report is the initial version of the Deliverable **Exploitation, Sustainability and Business Plans** that will be updated annually and incorporates all actions involved in setting up the environment for commercialising the SPHINX solution and further exploit the outcomes developed, according to the Task 8.3: Exploitation, Sustainability & Business Plans.

In this context, this report aims to:

- Present the exploitable results focusing on the basic characteristics (type, owners, exploitation options, target audience).
- Outline the overall project exploitation plan justifying the goals and corresponding targets set until the end of the project.
- Define the individual exploitation plans that the different consortium organisations (industry, SMES, public authorities, universities etc.) will implement to sustain the different project outcomes, until the end of the project and after the contractual end.
- Identify the business cases for exploitation, including the market context and the business model approach.
- Define the sustainability plan that the consortium will follow to sustain the project outcomes, beyond the end of the project.

The forthcoming period the key outcome of the project, the SPHINX platform and its individual components will be implemented and deployed in pilot conditions. Therefore, the upcoming versions of this report will focus on the elaboration of the business models and the business plan to stimulate the further commercialisation of such results.

1.2 Structure of the deliverable

The first section of the present document introduces its content and the overall scope. The next section 2, presents the overall project exploitation plan, the project outcomes with their basic characteristics and the individual exploitation plans that project partners will implement. Then, Section 3 defines the business cases for the different target groups and the corresponding approach through the business models that the consortium members will develop. Finally, Section 4 presents the sustainability plan overall context and the specific methodology that will take place during the project progress.

1.3 Relation to other WPs & Tasks

This report stands as the outcome of Task 8.3: Exploitation, Sustainability & Business Plans, which is a horizontal action across all WPs. In particular, within WP8 Dissemination, sustainability and exploitation, all tasks are complementary. It is also closely connected with the different tasks related to IPRs (T7.4 Legal analysis evaluation of the SPHINX use cases and business model, T8.5 Knowledge Management and IPR Protection). Besides, this task aligns with the WPs (WP2,3,4,5,6) which are related to the software development of the project and therefore, the exploitation plan should be updated according to the developed project results. Finally, Task 8.3 is also aligned to WP7 Technology Validation Pilots and Privacy assessment, because it is focusing on the implementation of SPHINX application in replicated real environments which impacts to the exploitation of the results.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

2 Exploitation plan

2.1 Context

The exploitation goal is to achieve the wide distribution and use of SPHINX outcomes, especially the SPHINX platform and its individual components by Health Delivery Organisations (HDOs) and Industry (Security and IoT) stakeholders, to assess and reduce cyber risks in hospitals and care centres to protect privacy, data, infrastructures.

During the first project year, we **design** the exploitation plan and its potential added value, during and after the end of the project progress, based on:

- Discussions with project partners, during the physical meetings and online bilateral meetings.
- Material developed from SPHINX project, including mainly D2.1 Advanced Cyber Security threats digest and analysis, D2.3-SPHINX Architecture v1 and the research carried out for T7.1 Sites Surveys and Planning of Pilot Operations.

This exploitation plan will be verified the next year through the involvement of targeted stakeholders in terms of:

- SPHINX exploitable outcomes
- Business cases for SPHINX individual components future commercialisation (see chapter 3)
- Business plan for SPHINX platform future commercialisation
- IPRs of the entire SPHINX platform and individual components

Additionally, sufficiently work has been carried out to define the exploitation goals, which can be summarised as follows:

- **Set up the environment for the exploitation of the SPHINX results**. The consortium is comprised of the following different project organisations:
    - **2 IT Large Enterprises**: SIVECO (Romania), INTRACOM (Greece)
    - **7 IT SMEs:** FINT, ViLabs (Cyprus), KT (Ireland), AiDEAS (Estonia), PDMFC (Portugal), EDGE (Portugal), TEC Inspire (UK)
    - **3 End Users**: Private Hospital: Polaris Medical (Romania), Public Hospital: HES (Portugal), Regional Health Authority: DYPE5 (Greece)
    - **3 Universities**: NTUA, HMU (Greece), VUB-LSTS (Belgium)
    - **1 Research Institutes**: TECNALIA (Spain)
    - **1 Non-Profit Organisation**: INCM (Portugal)

  Section 2.2 presents the individual exploitation plans for every organisation.

- **Provide a major competitive advantage to private partners of SPHINX** to their nation but also EU market, by exploiting the SPHINX platform and its individual components, through advanced business models and a mature Business Plan. Chapter 3 presents the particular business cases identified and the process of building business models and the Plan.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

2.2 Outcomes and basic characteristics

Currently, the SPHINX outcomes have been designed and they have the potential to offer a wide range of exploitation opportunities, in terms of software, best practices, policy recommendations, or their combination.

The major exploitable outcome is the SPHINX platform, a **Universal Cyber Security Toolkit for the Health and Care Domain** that enhances the cyber protection of the healthcare IT ecosystem and ensures the patients' data privacy and integrity. Furthermore, it is comprised of **individual components** that are interoperable and reusable, adhering to commonly accepted best practices of object-oriented software design.

Strong demonstration of the SPHINX platform will take place at four pilot sites (General Hospital of Volos (Greece), University Hospital of Larissa (Greece), Hospital do Espírito Santo de Évora (Portugal), and POLARIS Medical Clinic (Romania). These demonstrations will result to valuable exploitable outcomes, including; the **success stories** that will stem from the pilot implementations, key **policy recommendations** at national and EU level, and the **replication guidelines** that external Health Delivery Organisations may follow to deploy the SPHINX platform.

Finally, several scientific papers with open access will be publicly available, allowing the maximum outreach and exploitation potential of the scientific and technical project knowledge.

The table below presents a list of the project outcomes that the consortium envisages exploiting in various terms. In particular, for every project outcome (second column 'Outcome) it presents its type such as integrated software solution, policy recommendations, services, etc. (third column 'Type'). In the following, it defines the owner(s) who developed each outcome (fourth column 'Owner(s)') and shows the means (sixth column 'Exploitation options') that the owners may use to exploit each result to the targeted audience (last column). The target audience is comprised of the following categories: Industry (Security and IoT), Health Delivery Organisations, Research, Related EU projects, and Policy makers.

A/A	Outcome	Type	Owner(s)	Exploitation options	Target audience
1	SPHINX platform	Integrated platform	TBD at 2nd version of IPR Plan & IPR Management (M36)	Business plan	Industry, Health Delivery Organisations
2	Pilot cases success stories	Results of demonstration pilots	Polaris, HES, DYPE5	Concrete exploitation plans	ALL
3	Replication guidelines	Guidelines	DYPE5	Concrete exploitation plans	Industry, Health Delivery Organisations
4	SPHINX policy recommendations	Policies	ALL	Concrete exploitation plans	Policy makers
5	Scientific and technical knowledge	Services, methodologies, models	ALL	Concrete exploitation plans	ALL
SPHINX individual components					

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

6.1	Decision Support System (DSS) & Analytic Engine	Individual component	KT	Business case	Industry
6.2	Anomaly Detection (AD)	Individual component	SIVECO	Business case	Industry
6.3	Forensic Data Collection Engine (FDCE)	Individual component	NTUA	Business case	Industry
6.4	Vulnerability Assessment as a Service (VAaaS)	Individual component	HMU	Business case	Industry
6.5	Cyber Security Toolbox (SCT)	Individual component	FINT	Business case	Industry
6.6	Real-time Cyber Risk Assessment (RCRA)	Individual component	NTUA	Business case	Industry
6.7	Blockchain Based Threats Registry (BBTR)	Individual component	TECNALIA	Business case	Industry
6.8	Artificial Intelligence (AI) Honeypot (HP)	Individual component	FINT	Business case	Industry
6.9	Sandbox (SB)	Individual component	PDMFC	Business case	Industry
6.10	SPHINX Application Programming Interface for Third Parties (S-API)	Individual component	EDGE	Business case	Industry
6.11	Machine Learning-empowered Intrusion Detection (MLID)	Individual component	AIDEAS	Business case	Industry
6.12	Encryption Techniques Homomorphic Techniques (HE)	Individual component	TEC	Business case	Industry
6.13	Security Information and Event Management (SIEM)	Individual component	PDMFC	Business case	Industry
6.14	Security Protocol Analysis (SPA)	Individual component	NTUA	Business case	Industry
6.15	Data Traffic Monitoring (DTM)	Individual component	SIVECO	Business case	Industry

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

6.16	Anonymisation and Privacy (AP)	Individual component	PDMFC	Business case	Industry
6.17	Interactive Dashboards (ID)	Individual component	SIVECO	Business case	Industry
6.18	Attack and Behaviour Simulators (ABS)	Individual component	NTUA	Business case	Industry
6.19	Knowledge Base (KB)	Individual component	FINT	Business case	Industry
6.20	Common Integration Platform (CIP)	Individual component	ICOM	Business case	Industry

Table 1: Exploitable results overview

Based on the project outcomes, SPHINX project has defined the following exploitation goals to **prepare the ground for its further sustainability**. For every exploitation goal, it has set a target to reach within the project duration. This information is summarised below:

Project overall

A/A	Exploitation goal	Justification	Target indicator
1	Maintain the pilot sites	The SPHINX platform that will be deployed in replicated real environments at four pilot sites and it is expected to continue after the project end. This could be achieved if pilot partners obtain funding (national/private) after the end of the project to cover any expenses needed (e.g. personnel, infrastructure, etc.).	Pilot partners will present the pilot demonstration and its impact on the persons who are responsible for local and/or national funding (e.g. ministries) or private investment companies. We envisage having at least **6 meetings** (2 per pilot partner)
2	Increase the potential to replicate the platform at external Health Delivery Organisations (HDO)	SPHINX vision is that HDO across Europe will adopt the platform. Replication plans will also be designed to accommodate this need. SPHINX will promote the pilot demonstrations to HDOs (especially at the pilot countries, and at the EU level) to attract their interest for adopting the SPHINX platform into their infrastructure.	The Pilot demonstration will be presented, along with the replication plans, to HDOs asking to express their interest and provide with feedback to the replication plans. We expect that at least **3 Health Delivery Organisations** (1 per

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

			pilot country) will express their interest.
3	Verify the business potential of the platform in the health sector	Develop specific business cases with companies in industry (Security and IoT)	Pilot demonstration, presentation of business cases and provision of insights for at least **3 companies** (1 per pilot country)
4	Dialogue with policy makers	Develop policy recommendations and support dialogues with policy makers at EU and national level, aiming to increase public investments for the cyber security protection of HDOs, and increase the potential that more HDOs will adopt the SPHINX platform.	**10 meetings** with policy makers (9 partner countries and at 1 at EU level)
5	Wider adoption of the individual components	Several business partners will develop individual components that they should include in their portfolio and promote them to their customers and reach direct business potential.	**9 industrial partners** developing individual components (FINT, ICOM, PDMFC, KT, SIVECO, TECHNALIA, EDGE, AIDEAS, TEC) should include that at their portfolio.
6	New and improved educational and scientific knowledge	The SPHINX project will build a wide property of scientific knowledge. Academic partners should take this advantage and improve existing education on cybersecurity.	**3 educational** infrastructures to be improved (1 per each University NTUA, HMU, VUB-LSTS)

Table 2: Overall project specific goals and target indicators

Moving beyond the project end, when all project outcomes will be at their final version, the business plan and replication plans will be finalised, and the above targets will be achieved, the SPHINX consortium, both private and public partners, envisage to exploit the outcomes. In this respect, they have defined the exploitation goals, for two years after the end of the project. The Tables below show for each partner type (private and public) the relevant information.

Partners from private companies (two IT Large Enterprises (SIVECO, INTRA) and seven IT SMEs (FINT, KT, ViLabs, AiDEAS, PDMFC, EDGE, TEC))

A/A	Exploitation goal	Justification	Indicator of success for the next 2 years after the end project
1.	SPHINX platform will be further developed to become a	The SPHINX business plan will have strong evidence from the pilot	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

	product ready to enter the market to assess and reduce cyber risks in Health Delivery organisations.	demonstrations. It will be also introduced in the market at external Health Delivery Organisations which will express their interest to replicate it. In addition, the business plan will be verified by the industrial stakeholders. Having this information**, partners from private companies agree to create a partnership** to seek for funding or further investments	Increase the customer base. Increase the revenues as a % of the total company profit on IT products/services. Expand the presence of the company into a new market. Sign a short- or long-term services contract agreement.
2.	Develop new **individual components** that assess and reduce cyber risks in Health Delivery organisations.	Enhance company's portfolio with new solution/software components which impact has been identified through its demonstration in replicated real environments. This may stimulate future clients. E.g. replicate the SPHINX platform at external Health Delivery Organisations.	
3.	Develop **new services (installation, training)** at Health Delivery Organisations for the replication of 1. and 2.	Expand the knowledge gained from the pilot deployment and implementation, also the lessons learnt from how different problems have been met.	
4.	Create, improve and sustain the **network of organisations** in collaboration.	Improve the company's relationships within its network and expand new ones, by informing them about SPHINX project and its use for their own needs. Disseminate the knowledge gained for expanding the company's offering, through its distribution channels.	A number of new collaborative organisations added to the company's network. New research and innovation projects generated with private and/or public funding.
5.	Employ **new personnel** through project participation	A number of new researchers have been employed, especially PhD students for practical training of their research application to replicated real environments.	A number of new personnel hired for the purpose of the project. Number of new employment positions sustained after the end of the project.
6.	Improve **potential and skills** of the **existing personnel**	Add value to the competencies of the existing staff through their involvement in the creation of new ideas and knowledge.	Number of existing personnel involved and specific skills acquired.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Partners from public organisations (three Universities (NTUA, HMU, VUB-LSTS), a Research Institute (TECNALIA), a Non-Profit Organisation (INCM), and three end users/Health Delivery Organisations (HDO) (DYPE5, POLARIS, HESE)

A/A	Exploitation goal	Justification	Indicator of success for the next 2 years after the end project
1	Maintain the pilot cases	The pilot partners having completed the demonstration, will have available the best practices that present the impact of its usage to minimise cyber security threads. Following the local and/or national funding (e.g. ministries) or private investment companies will act to receive the necessary funding and if needed (for example change of political party), additional meetings will take place.	Confirmation from local and/or national funding (e.g. ministries) or private investment companies to keep the SPHINX solution beyond the end of the project. Request for additional funding to sustain the technology (e.g. staff)
2	Increase the potential to replicate the platform at external Health Delivery Organisations	SPHINX vision is that HDO across Europe will adopt the platform. SPHINX will continue, beyond the end of the project, to promote the pilot demonstrations to HDOs (especially at the pilot countries, and at EU level) to attract their interest for adopting the SPHINX platform into their infrastructure.	The Pilot demonstration will continue to be promoted to HDOs motivating them to replicate it.
3	New and improved educational and scientific knowledge	The knowledge built through the project would support students and researchers to progress on novel IT solutions and services.	Additional scientific papers in this domain are expected to be produced. New courses are envisaged to be embedded in education.
4	Influence policies in the cybersecurity domain, at EU and national level	Impact generated through the pilot demonstration should be communicated with Policy Maker. The collaboration with relevant EU projects would increase the opportunities to reach a wider target audience.	SPHINX policy recommendations to be included within the upcoming policies on Cybersecurity.
5	New research collaborations	Apply SPHINX knowledge in new research projects in the future.	New research projects generated with private and/or public funding.

Table 3: List of potential Exploitation goals for private/public organisation partners for the next 2 years after the end of the project

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Following the above definitions, the next table summarises for every exploitation outcome, the planned exploitation goals to reach until the end of the project and the corresponding goals to reach after the contractual project end, for the estimated period of two years.

A/A	Result/Asset	Exploitation goals	Indicator of success/metric	
			Until the end of the project	After the end of the project (2 years)
1	SPHINX platform	Stimulate the business potential of the platform in the health domain.	Sign contracts among partners to collectively exploit the results after the project ends, seek for funding or further investments.	Increase the customer base. Increase the revenues as a % of the total company profit on IT products/services. Expand the presence of the company into a new market. Number of new collaborative organisations added in the company's network. New research and innovation projects generated with private and/or public funding. Number of new employment positions sustained after the end of the project. The Pilot demonstration will continue to be promoted to HDOs motivating them to replicate it.
2	SPHINX individual components	Expand the individual components, including them at business partners portfolio for direct business impact.	**9 industrial partners** developing individual components (FINT, ICOM, PDMFC, KT, SIVECO, TECHNALIA, EDGE, AIDEAS, TEC) should include that at their portfolio.	
3	Replication guidelines	Increase potential to replicate the platform at external Health Delivery Organisations	The Pilot demonstration will be presented, along with the replication plans, to HDOs asking to express their interest and provide with feedback to the replication plan. We expect that at least **3 Health Delivery Organisations** (1 per pilot country) will express their interest.	
4	Pilot cases success stories	Maintain the pilot sites	Pilot partners will present the pilot demonstration and its impact on the persons who are responsible for local and/or national	Confirmation from local and/or national funding (e.g. ministries) or private investment companies to keep the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

			funding (e.g. ministries) or private investment companies. We envisage having at least **6 meetings** (2 per pilot partner)	SPHINX solution beyond the end of the project. Request for additional funding to sustain the technology (e.g. staff)
5	SPHINX policy recommendations	Dialog with policy makers	**10 meetings** with policy makers (9 partner countries and at 1 at EU level)	SPHINX policy recommendations to be included within the upcoming policies on Cybersecurity.
6	Scientific and technical knowledge	New and improved education	**3 educational** infrastructures to be improved (1 per each University NTUA, HMU, VUB-LSTS)	Additional scientific papers in this domain are expected to be produced. New courses are envisaged to be embedded in education.

Table 4: Total Partners' exploitation goals and indicator of success/metrics before and after the end of the project

2.3 Intellectual Property Rights (IPRs)

The SPHINX results that will be exploited in the future, should be protected. To this end, the initial step has been the **mapping** of the **intellectual property options** and **tools** which provides project partners with a timely and comprehensive guidance on efficient and competent protection of their project-related IP rights (such as trademarks, patents, copyright and transfer and licensing agreements)*(see D8.1 SPHINX IPR Plan & IPR Management v1)*. A more concrete IPR management plan is scheduled for month 36 of the Project and shall be presented under Deliverable D8.11 SPHINX IPR Plan & IPR Management v1.

2.4 Individual exploitation plans

The SPHINX consortium overall exploitation plan will be achieved through the individual plans that each partner will undertake. During the first project year, as the project outcomes are defined, the corresponding individual exploitation plans are also defined. During the second and third project years, when the outcomes will be developed and deployed, it is expected that the individual exploitation plans will also be improved according to the knowledge gained.

2.4.1 NTUA, Greece

Partner Profile

NTUA is the most prestigious and competitive academic institution on engineering sciences in Greece. The Decision Support Systems Laboratory (DSSLab) is a multidisciplinary scientific unit within the School of Electrical

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

and Computer Engineering, operating for more than 25 years, with international experience and offers R&D activities providing management and decision support services on a wide range of complex business, societal and technical problems. The R&D services of DSSLab-NTUA are applied not only on research challenges but also on real life problems in industry, energy, trade, business, education, telecommunication, tourism, health and public administration.

Individual Goals of Exploitation

The activities of DSSLab-NTUA are well positioned to provide support for diploma, thesis and PhD dissertation on the field of management and decision support systems that have an applied inter-disciplinary orientation. The main purpose of those activities is the emergence of Researchers, Engineers and Scientists, who can take on a leading role in Research and Development on an international level. The academic work of DSSLab-NTUA includes provision of training to under- and post- graduate engineers, extensive research work and publication of scientific papers. The main goal of DSSLab-NTUA is to offer continuous and consistent knowhow to cutting edge technologies, hands-on experience and evolve platforms and infrastructure in order to foster research and innovation and disseminate knowledge.

Identified Exploitable Project Results

Result/Asset	Type	Exploitation options	Target audience
Scientific and technical knowledge	Services, methodologies, models	Concrete exploitation plans	Researchers
Security Protocol Analysis (SPA)	Individual component	Concrete exploitation plans	Researchers
Real-time Cyber Risk Assessment (RCRA)	Individual component	Concrete exploitation plans	Researchers
Forensic Data Collection Engine (FDCE)	Individual component	Concrete exploitation plans	Researchers
Attack and Behaviour Simulators (ABS)	Individual component	Concrete exploitation plans	Researchers

Value creation to the organisation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

- **New and improved educational and scientific knowledge**
  NTUA is an academic institution with research and educational activities. The knowledge acquired throughout the project's lifetime shall support students and researchers to progress on novel IT solutions and services. In this context, the exploitation of SPHINX results mostly refers to improving and extending the academia related services offered by the institution, focusing on the following:
    - Considering SPHINX as a basis for building or extending advanced research activities conducted in related scientific domains.
    - Attaching added value to on-going innovation, research and industry related projects in relevance to the SPHINX concept domains. Such collaboration with other related European research initiatives, projects and partners is envisaged to be bi-directional as information exchange from and to SPHINX shall offer harmonised results in related activities.
    - Accumulating and diffusing the knowledge that emerges from SPHINX (including results and areas for innovation and possible research) to be further used for educational purposes (seminars, post/undergraduate courses, etc.) and for exchanging ideas with the academic community.
    - Bringing pioneer ideas and knowledge to university students that will impact their academic work (PhD dissertation, post-Doc, papers, etc.) along with the practical experience obtained.
- **New research collaborations**
  The expected insights into emerging innovation areas shall envision future innovation and research projects based on the knowledge acquired during SPHINX implementation. New research projects generated with private and/or public funding.

2.4.2 FINT, Cyprus

Partner Profile

Future Intelligence (FINT) is a leading and highly innovative Group of Companies specialising in Information and Communication technologies (ICT). The Group was initially established in Greece in 2009, is privately held and its main facilities are located in Greece, the United Kingdom and Cyprus. FINT provides highly demanding solutions and business services covering a number of activities, beginning at the edge, with specialised hardware offerings in various verticals, including hardware acceleration, low-power sensors, ruggedized gateways, up to the Cloud with software suites (IoT Platform), middleware and big data analytics.

FINT is one of the leading IoT devices manufacturers in Europe. The company's objective is to build an IoT-enabled ecosystem (FINoT Platform) which can expand horizontally and vertically providing a playground for vendors, OEMs and software engineers.

Current commercial and research activities include next generation networks (network virtualisation), sensor adaptation and data interpretation techniques, data mining and data provision through cloud-based applications, cyber security services, distributed computing techniques (Edge computing) and AI.

FINT has a newly established department of Cyber Security Services focusing on Accelerated Services and trying to build an ecosystem friendly from cost and usability perspective for SMEs.

Individual Goals of Exploitation

FINT has already established a dedicated cyber security department with focus on automated deployed services on Accelerated Infrastructures but not limited to (based on its experience through FINoT platform on IoT devices management and services deployment experience). Main impact by the exploitable elements of FINT is to offer a key service that can result in enhancing European security apparatuses and lead to a safe environment for European citizens. Eventual productization of the technologies developed within SPHINX in

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

particular AI Honeypot, Cyber Security Toolkit and Knowledge Base. More specific FINT will exploit SPHINX results in the following concrete ways:

1. **AI Honeypot** will be exploited enhancing cyber security services of the company and more specific complementing Accelerated GW current services to provide a holistic cyber security service for organisations that want to include security and privacy by design into their operational process and this will be provided into 3 different flavours:
    - Lightweight Honeypot device (low processing capabilities for small organisations)
    - Accelerated Honeypot device (exploiting FPGA acceleration capabilities – for organisation with distributed needs and with higher processing expectations)
    - Virtual Honeypot appliance (for organisations using cloud infrastructure for their operational environment)

    FINT will also integrate AI honeypot into their IoT solutions portfolio in order to provide value added service to its current clients in Smart Cities domain, Smart Agriculture domain and finally to penetrate into Health domain.
2. **Knowledge Base (KB)** as part of SPHINX overall solution will be exploited in the ways mentioned below:
    - As Virtual Appliance (to be integrated to heterogeneous platforms providing security services). The virtual appliance will provide dedicated APIs that can be used from 3rd parties to create their own solution along with to integrated as is in their own platforms (e.g. cyber range tools/platforms)
    - As cloud service with 3rd parties that want to exchange knowledge through the knowledge base for different applications.

    FINT will integrate KB to its own IoT platform in order to provide better Cyber Security Knowledge to its clients.
3. **Cyber Security Toolkit (SCT)** will exploited mainly as cloud services providing an easy deployment mechanism for cyber security services.

The company first identifies and approach prospective light house customer and then work with them closely to derive the requirements for a product based on the SPHINX platform. It will then create a roadmap and work towards implementing it. Using this approach FINT has already identify potential individual exploitation elements from the early stages of the project and during the definition of the components phase and will continue investigating potential joint ventures within the consortium with complementary components. Moreover FINT will closely follow the needs of the end-users targeting first creating a useful solution for them within the project but also to create the environment for potential exploitation of its components with them directly and/or to create the appropriate references (success stories) increasing like this the prospect of penetrating the health domain.

Identified Exploitable Project Results

Result/Asset	Type	Exploitation options	Target audience
Artificial Intelligence (AI) Honeypot (HP)	Individual component	Business case	Industry
Knowledge Base (KB)	Individual component	Business case	Industry
Cyber Security Toolbox (SCT)	Individual component	Business case	Industry
Cyber Security Toolbox (SCT)	Individual component	Business case	Industry

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Value creation to the organisation

FINT is an organic growth company creating innovative products and services helping its clients and communities to achieve digital transformation easily and in a coherent way following European digital single market principles. By now FINT though EU and National initiatives is continuously growing by exploiting funded RnD initiatives to create its own products, hire new high skilled personnel, evolve them through EU research agenda, make its products EU and Globally adopted. Through this perspective FINT as a group has currently in the market three business lines providing certified products (one of the 1st FIWARE commercial platform for Agriculture, IoT platform for Smart Cities, Smart Lighting and Smart Agriculture IoT devices) in the domain of IoT and 1 production line of IoT devices. In the next months through its newly established cyber security department it will launch AGW (accelerated GW for SMEs). The Innovation department is divided into 3 concrete pillars: 1) create references in order to prove its future products functionalities and attract potential customers, 2) already selling solution adaptation for different domains (Health, Manufacturing), 3) incorporate innovative technological elements to the new strategically identified products (e.g. AI to IoT, AI irrigation systems) with a horizon to 2025. This principal will impact FINT to: Develop and market new **individual components** that assess and reduce cyber risks in Health Delivery organisations (see table 3 for further explanation) by signing a contract to directly with small/medium health organisations and provide its services through contract with large service provider to large health organisations, to Develop and provide **new services (installation, training)** at Health Delivery Organisations (see table 3 for further explanation), to create, improve and sustain the **network of organisations** in collaboration (see table 3 for further explanation) targeting at least 15 new collaborators (already 3 established collaborations existing from the beginning of the project), to Employ **new personnel** through project participation (target 3 new, already 1) and afterwards along with improve technical skills of existing personnel (please see points 5 and 6 on table 3)

2.4.3 KT, Ireland

Partner Profile

Konnektable Technologies is a technology research and development firm, based in the Republic of Ireland. Our vision is simple – to create connections – through technology, through the practical application of research, and through collaboration. Konnektable's principals have extensive experience in research work and in following that work through to the commercial marketplace.

Individual Goals of Exploitation

KT main exploitation goal is to bridge the current gap between its own services and the new technologies developed within SPHINX. KT will set up a close cooperation with its own clientele to develop and commercialise services using SPHINX. KT develops software for the health sector as well as a series of applications for a variety of domains (energy efficiency, transport, supply chain, mobile etc.). KT will take advantage of its clientele list and will promote SPHINX platform and its components.

Specifically speaking, the topics and domains of SPHINX that KT seeks to share and gain knowledge are mostly focussed on data management, data exchange and knowledge discovery technologies, service based architectures, IoT based services management and knowledge discovery through AI-enabled Decision Support Systems and Machine learning technology, with the aim of verifying the possibility to capitalise on both knowledge and technology and expand further its current commercial portfolio and business activities as these are displayed in the company's website http://konnekt-able.com/

Furthermore, KT will actively contribute to the overall Business activities of SPHINX: Technology itself is just a few interesting results if the business orientation is not considered. In this path the technologies are valorised,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

the risks are mitigated, the exploitation strategy is defined and, finally, a business plan is produced. The business activity path ends with a "mixed" activity, partially technological, focused on the commercialisation of the technology which is one of the core objectives of the company.

KT is a SME which means making profit is part of the process that keeps the enterprise up and running, but profit is a term that can take several meanings. Releasing a free, community version, of a software that will enable more users and facilitate their processes must also be viewed as profit, profit for society and its members. Not all profit can be measured in terms of revenue. Therefore, KT is proud of participating in European projects that, by definition, aim at enhancing the quality of life of its citizens, and proud of embracing Open Science protocols and procedures.

Identified Exploitable Project Results

Result/Asset	Type	Exploitation options	Target audience
Decision Support System (DSS)	Individual component	Business case	Industry
Analytic Engine (AE)	Individual component	Business case	Industry

Value creation to the organisation

The overall aim of Konnekt-able Technologies Ltd. is to exploit the results of SPHINX project as part of its core strategy in the marketing and selling of industrial projects and services. Through its participation in SPHINX and other European projects, KT strengthens its core business value which is enabling the users and creating connections utilizing technological solutions and data-driven insights. The practical application of research and the acquired knowledge will be incorporated to the business department, increasing its capabilities and the possibility of offering enhanced products and services during the project, with the aim of strengthening cyber security for health care, critical infrastructures and production lines; propelling an increasingly massive deployment of cyber security solutions and an increasingly intense use of those solutions in their respective fields. The results will strengthen KT's competence and will be transferred into industrial use via contract R&D projects and consultancy services and as plug-inns to the commercial platforms of the company. Furthermore, results that are not of commercial TRL will be exploited in current and forthcoming European R&D projects.

2.4.4 VILABS, Cyprus [SME]

Partner Profile

VILABS is an SME that acts both as a private research and innovation laboratory and as an innovation Hub for startups both in Greece and Cyprus. VILABS provides a wide range of **research, development and consulting services** to national as well as international enterprises and organisations, utilising a unique set of tangible and intangible resources, including knowledge, facilities, human and financial resources, supporting researchers and entrepreneurs to innovate. VILABS is active in the sectors of ICT, social innovation, health and entrepreneurship through all stages of Research, Technological Development and Innovation.

Individual Goals of Exploitation

VILABS main exploitation goal is to sustain the SPHINX platform and expand its use further to other European regions.

In particular, VILABS will be a member of the partnership that will maintain the platform in all pilots currently running and new ones that will join. The maintenance will include, bug fixing, helpdesk and users support. ViLabs will also promote the platform usage outside the project consortium and to new regions. It will promote the best practices and lessons learnt for the localisation and implementation of the platform, utilising the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

knowledge gained, when this is required. VILABS will investigate with the partnership for funding to undertake all the costs related to the maintenance of the platform and complementary services, as well as the promotion and replication.

Identified Exploitable Project Results

Result/Asset	Type	Exploitation options	Target audience
SPHINX platform	Integrated solution	Business plan	Industry, Medical organisations
Scientific and technical knowledge	Services, methodologies, models	ALL	Concrete exploitation plans

Value creation to the organisation

ViLabs envisages maintaining the platform, as well as the knowledge gained on replicated real environments, with the aim to increase the company portfolio of expertise and service offering, on the area of cybersecurity, by promoting SPHINX project as a best practice.

In addition, VILABS personnel will acquire new knowledge on cyber security and will enhance the current consulting services offering on startups, entrepreneurs and local initiatives/communities.

VILABS will offer the new knowledge acquired on services (installation, customisation, deployment) of a platform at Health Provision Organisations) offering new knowledge to startups, entrepreneurs that are already working in the cyber security field, but they want to improve it.

2.4.5 SIVECO, Romania [Industry]

Partner Profile

SIVECO Romania SA is a private shareholder company, established in 1992, located in Bucharest, Romania. During its existence, SIVECO has become the largest Romanian software development company and provider of software solutions like ERM L&M (Enterprise Resource Management License and Maintenance), eGovernment, eLearning, eHealth, eAgriculture, eCustoms solutions acting both on the internal and international markets, and one of the most successful software integrators from Central and Eastern Europe.

Individual Goals of Exploitation

SIVECO will integrate the project outcomes into its commercial offering by enhancing the existing products and services portfolio with new ones. In this regard, some of the modules could be integrated into the existing commercial software or licensed to be uses by third parties. SIVECO will also apply and further develop the methodology and individual software implementations of the project in subsequent contracted research projects, either in publicly funded research (national and EU) or funded through industry. Consultant services can be also offered as technical consultancy or business consultancy. Focusing on customisation and personalisation of the SPHINX solution while taking into consideration the methodologies and the business of the end-user, and simultaneously, the integration, training, technological support services can be offered within the framework of the consultancy services.

Identified Exploitable Project Results

Result/Asset	Type	Exploitation options	Target audience
Data Traffic Monitoring (DTM)	Individual component	Business case	Industry

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Anomaly Detection (AD)	Individual component	Business case	Industry
Interactive Dashboards (ID)	Individual component	Business case	Industry

Value creation to the organisation

The three components that will be developed by SIVECO during the project will strengthen the company's actual solutions portfolio by integrating them with existing applications and offering new market opportunities. The lessons learnt during the deployment and implementation of the Romanian pilot will enrich the company's knowledge base. The skills of the company's personnel will be improved through their work within the project.

2.4.6 AiDEAS, Estonia [SME]

Partner Profile

AiDEAS is a highly innovative technology and data solutions provider. The company is building machine learning and AI-power technology to unlock the value hidden in huge volumes of data, reducing the time to find, diagnose, comprehend and act at a speed that is impossible for humans, thereby generating new faster insights. AiDEAS portfolio is built on leading-edge AI technologies including data mining and machine learning/deep learning to (i) enable data-rich and knowledge-lean automation of valuable tasks of perception, classification and numeric prediction as well as (ii) collect, organise, analyse and discover hidden pattterns and value in voluminous amounts of structured and/or unstructured data. AiDEAS staff comes from different computer science backgrounds with over 15 years experience and a particular focus in developing novel algorithms as well as leading award-winning academic research for solving important existing and emerging problems in various industries such as Healthcare, Industry 4.0 and Oil & Gas.

Individual Goals of Exploitation

AIDEAS is a SME developing AI and Machine Learning services. The extension from the existing services will be provided as part of the new services portfolio.

Identified Exploitable Project Results

Result/Asset	Type	Exploitation options	Target audience
Machine Learning-empowered Intrusion Detection (MLID)	Individual component	Business case	Industry

Value creation to the organisation

SPHINX impact to the company is the increased knowledge of implementing ML powered cybersecurity algorithms. Being part of the SPHINX platform and partner network will promote the company internationally to both the cybersecurity and health sector.

In addition, the MLID module can be used as a stand-alone module and can be tailored to multiple usage scenarios. This will allow the company to market itself to additional customer segments in addition to the health domain.

2.4.7 HMU, Greece [University]

Partner Profile

It is a higher education and research organisation, founded in 2019 by the Hellenic Ministry of Education after the Universal takes over of the Technological Educational Institute of Crete. It is now comprised of 11

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Departments in a variety of scientific and technological disciplines including management and economics, health and welfare services, agricultural and environmental technology, electronics, mechanical engineering, computer and informatics engineering, while many of the curricula are multidiscipline in their structure. HMU is a thriving academic community with an expert faculty of Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures about 400 members, over 300 administrative and technical staff and approximately 12000 students.

Individual Goals of Exploitation

HMU intends to exploit its participation in the SPHINX project for exposing its graduate engineers and researchers in high-level technical work in the area of Network Resource Trading and Brokerage. In particular, MSc courses will be enhanced with tutoring on the specific concepts, and extensions on the related aspects will be offered for PhDs. In addition, PASIPHAE lab is to pursue further R&D along those lines based on the know-how obtained within the project. As experienced in the past, HMU put extreme value in its participation in high level research with manufacturers, industrial and other research partners, since this is the only way to be promptly acquainted with upcoming standards and major imminent technical and implementation decisions.

Identified Exploitable Project Results

Result/Asset	Type	Exploitation options	Target audience
Scientific and technical knowledge	Services, methodologies, models	Concrete exploitation plans	Researchers
Vulnerability Assessment as a Service (VAaaS)	Individual component	Concrete exploitation plans	Researchers

Value creation to the organisation

HMU work in SPHINX is coming as a natural continuation of our work within FP7 and H2020 EU projects dealing with eHealth and Cyber-security systems and applications. aims at continuously enhancing and keeping the up-to-date level of knowledge offered in its courses. The results obtained via SPHINX will be exploited by HMU for exposing its graduate engineers and researchers in state-of-the-art areas of Cyber Security, by offering them theoretical knowhow as well as practical and in-hands experimentation tools to be developed within the framework of SPHINX. MSc courses will be enhanced with tutoring on the specific concepts, and extensions on the related aspects will be offered for PhDs. HMU also puts extreme value in its collaboration via SPHINX with other research, civil-sector and industrial partners, since this is the only way to be promptly acquainted with upcoming standards and major imminent technical and scientific breakthroughs.

HMU exploitation focus also to promote SPHINX outcomes and practices in public health authorities in Greece (in particular the Ministry of Health) as well as in private hospitals with which it collaborates with. Among the SPHINX activities in which HMU is involved in, the patient safety cybersecurity framework constitutes its major exploitation interest, since patient safety is one of its strategic R&D areas, complementing various activities

2.4.8 PDMFC, Portugal [SME]

Partner Profile

PDMFC develops products in two complementary areas: Software development tools and High Speed Communication Hardware. In the software area PDMFC has developed, Tea, a scripting programming language, and I*Tea, an application server for the web.

Individual Goals of Exploitation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

PDMFC have developed several tools in the area of cybersecurity and it is interested to exploit SPHINX platform and individual components by incorporating them into the suite of Forensics, Intelligence and Foresight tools and by developing new tools specifically to address the needs of Critical Infrastructures CyberCrime prevention, detection and mitigation. PDMFC currently manages several large CSIRTs in Portugal for some Critical Infrastructures operators (both Public and Private) as consultancy work, and its participation in SPHINX will allow the company to provide clients with this cutting-edge technology.

Identified Exploitable Project Results

Result/Asset	Type	Exploitation options	Target audience
Security Information and Event Management (SIEM)	Individual component	Business case	Industry
Anonymisation and Privacy (AP)	Individual component	Business case	Industry
Sandbox (SB)	Individual component	Business case	Industry

Value creation to the organisation

PDMFDC will gain a competitive advantage over its direct competitors. Through the exploitation of SPHINX outcomes, it will improve the suite of tools for Identification and Access Management (SPA) and Anonymization. Eventually some of the research that PDMFC will conduct during the SPHINX project might lead to Patentable IP, which would further consolidate our position in Risk Assessment Tools, SIEM, Forensics, Threat Analysis, Anomaly Detection, Data Fusion, etc.

2.4.9 EDGE, Portugal

Partner Profile

EDGENEERING (EDGE) is a Portuguese start-up SME with a technology drive, dedicated to the design and development of high-performing solutions for intelligent healthcare and assisted living environments.

EDGE's solutions uniquely combine automation, data analytics and engineering to design and develop differentiating, reliable and high-performing smart solutions for specific societal challenges: to create safer societies, to contribute to healthier societies and to promote sustainable societies.

Leveraging the Internet of Things (IoT) paradigm, EDGE's ambitious vision has led the company to build a highly innovative and competitive smart technology portfolio for hospitals, private clinics, medicalised nursing and homecare environments, and to establish early-on a business model based upon strong partnerships with national and international partners, selected for their market value and capability to support EDGE making its vision a reality.

Individual Goals of Exploitation

The security technology developed and experience gained through the SPHINX project will be funnelled into EDGE's eCare Platform services, adding relevant improvements to the company's trusted security practices. EDGE's market competitiveness will also benefit from the verification of the new security technologies' usability and incorporation in its eCare Platform and commodity cloud platform. Further, the project will also provide valuable insight on the novel security techniques and technologies to bridge the existing gaps in IoT devices' security and protection. As an emerging SME, the reputation gained by EDGE from the SPHINX project will positively influence its future business development and sales activities, namely in Portugal, Portuguese-spoken countries and Europe.

Identified Exploitable Project Results

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Result/Asset	Type	Exploitation options	Target audience
SPHINX Application Programming Interface for Third Parties (S-API)	Individual component	Business case	Industry

Value creation to the organisation

Considering SPHINX exploitation, EDGE foresees the following value creation/impact:

- **Promotion of EDGE's solution portfolio, namely its eCare Platform, as it integrates specific cybersecurity tools developed within the SPHINX RIA framework:**

  The eCare Platform is EDGE's smart and personalised ambient intelligence platform that creates a welcoming assisted living environment for health and wellbeing at home. Fostering a non-intrusive, secure and individual-friendly experience, eCare enables a reliable and highly-scalable health status and quality of life monitoring environment, through the gathering of physiological and psychological health parameters of medical devices and IoT-based smart home sensors, ensuring the individual's safety on a continuous 24/7 basis and the early detection of health and wellbeing deterioration signs, improving on the level of care in living environments, including at home and in hospitals. Consequently, advanced cybersecurity features, including the certification of medical devices, are a value-added benefit to eCare's clients, thus improving eCare's competitive advantage in the market.

- **Endogenisation of cybersecurity knowledge and skills following the implementation of the SPHINX RIA:**
  EDGE will apply the new advanced cybersecurity knowledge and skills developed as a result of the SPHINX project in its own software development activities, reinforcing a key element of any IT solution. The participation in SPHINX and the resulting acquired experience and expertise provides an essential time-to-market advantage over EDGE competitors, rendering EDGE better prepared for new markets and services and able to position itself early on as a provider of healthcare IT solutions with beyond state-of-the-art cybersecurity features. Further, the SPHINX project will enable EDGE to build a solid know-how and expertise with respect to the cybersecurity needs of healthcare organisations and this new knowledge will be further explored by EDGE in EU-funded and national-sponsored dedicated research, innovation and development endeavours in the framework of smart healthcare solutions.
- **Participation in joint commercial exploitation efforts for the SPHINX Platform, contributing with the Third-party APIs:**
  As SPHINX partners align commercial strategies to bring into the market the SPHINX Platform, EDGE will take part in the effort, contributing with the Third-Party APIs that allow SPHINX clients to test and validate devices and systems for their cybersecurity compliance before introducing them into their own IT ecosystem.

2.4.10 TEC, UK

Partner Profile

Tech Inspire Ltd is a fast growing UK start-up company focusing on the security and privacy aspects of intelligent information infrastructure, mobile computing and Cloud computing.

Individual Goals of Exploitation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Tech Inspire is deeply interested in providing security and privacy solutions for the betterment of the society. It believes in empowering the users with the necessary control over their information. In this regard, TEC is working on developing a Homomorphic Encryption based searchable encryption and privacy prevention algorithm that would allow the user to perform search in the encrypted domain and will also anonymize data on the fly. This solution created for the SPHINX project would be rigorously tested throughout the project and would be refined in the form of a product at the end. The SPHINX project would act as the key platform required to pitch and portray the working solution presented by TEC. It would also help us highlight how efficiently it works and how it complies with all the latest regulations. The research aspect of the solution would help in refining the product and might eventually be used to file an IP which would further bring us the recognition and validation that is required.

Identified Exploitable Project Results

Result/Asset	Type	Exploitation options	Target audience
Homomorphic Encryption (HE)	Individual component	Business case	Industry

Value creation to the organisation

Tech Inspire intends to exploit the opportunity provided in the form of the SPHINX project to understand the deployment limitations set out by the healthcare industry. This would help us in tailoring our solution in the appropriate way that would fulfill these tightly set limitations and increase the size of our target market.

Our team at TEC would benefit by learning about modular development work where our solution needs to be modularly added into the SPHINX solution along with other modules. This would be a different set of development skills that would benefit us in the future. TEC will make this information available to new startups and developers in the form of blog posts and research papers as frequent as possible.

2.4.11 VUB-LSTS, Belgium [University]

Partner Profile

The interdisciplinary Research Group on Law Science Technology & Society at the Vrije Universiteit Brussel, which participates in SPHINX, is devoted to analytical, theoretical and prospective research into the relationships between law, science, technology and society.

Individual Goals of Exploitation

The motivation of VUB LSTS for the participation in the SPHINX project is the intrinsic interest to promote privacy, data protection and security in the emerging innovative solutions and the keenness to identify and facilitate the mitigation of data protection threats and risks. Apart from the unique opportunity to enhance and adapt the EU data protection legal framework, VUB does not only monitor legal compliance with the European legal framework, but also contributes to Privacy- and Security-by-Design SPHINX platform and upgrade its know-how. VUB intends to disseminate the results of the project to the annual CPDP conferences that it organises, where the audience is multi-disciplinary, including industry, academia, consumer associations, legal practitioners and others. Part of the dissemination will be the European Standardisation Bodies and the European Data Protection Supervisor. VUB will also publish relevant articles in prestigious journals, such as the International Data Privacy Law (OUP) and the Computer Law & Security Review (Elsevier).

Identified Exploitable Project Results

Result/Asset	Type	Exploitation options	Target audience

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Scientific and technical knowledge	Services, methodologies, models	Concrete exploitation plans	Researchers

Value creation to the organisation

VUB will gain significant scientific knowledge in the sector of cybersecurity, specialised in the health domain, which has also been the key motivation to join the project. The specialised knowledge presented through scientific papers and conferences will influence the relevant community and more opportunities to extend it through relevant research funded projects will arise.

2.4.12 TECNALIA, Spain [Research Institute]

Partner Profile

TECNALIARESEARCH & INNOVATION is a private, independent, non-profit applied research centre of international excellence.

Individual Goals of Exploitation

TECNALIA cybersecurity group is focused in placing into the market advance solutions or services which go beyond the state of practice. In this direction within SPHINX we are focusing in two areas, one is centered in Blockchain technologies, in which we find real market applicable scenarios where blockchain technologies make sense. As a recent example TECNALIA in 2018 patented a blockchain technology for traceability for Supply chains and segmented generation chains in which we sold the solution to Acciona Energia (Energy Guarantee of Origin) or Hazi (Food Supply Chain Traceability). Currently in 2019 we are focusing in looking for potential partners that can sell this product.

In the same direction within SPHINX we are looking into the creation a similar platform but focused in providing an additional level of first line action that can avoid unknown attacks. There are already solutions in the market such as MISP (non-blockchain solution) for exchanging attacks information between entities but is based in the trust among entities but does not validate the validity f the information exchanged. By introducing a blockchain solution we can ensure origin of the attack as well as provide an auditing mechanism to identify origin of the information and we can provide mechanisms to validate or not the nodes.

We consider that within SPHINX the Blockchain Based Threats Registry component will enable TECNALIA to reach cubersecurity organisations providing SIEM solutions that could benefit of the use of the BBTR component. This can happen also within the scope of the project if collaboration with other components is foreseen. This is so for the overall SPHINX solution proposed in which the component will be offered as a service within SPHINX Prototype Demonstrator and based on finding additional means for exploitation will be identified.

So as for the actual future exploitation form, in TECNALIA we usually address a license-based mechanism (15K€). But if identified within SPHINX maybe additional means such as pay per use, may also be considered. These is all to be decided in the Year 3 of the project when the overall SPHINX Prototype has been validated and the clear values of all the pieces is identified.

Identified Exploitable Project Results

Result/Asset	Type	Exploitation options	Target audience
Blockchain Based Threats Registry (BBTR)	Individual component	Business case	Industry

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Scientific and technical knowledge	Services, methodologies, models	Concrete exploitation plans	ALL

Value creation to the organisation

Even though it is still early for having a clear view on the values creation for TECNALIA, we can foresee that if we manage to create alliance with a cybersecurity company which values the BBTR module, we will consider to means of collaboration, one focused on a license base usage of the BBTR module by the cybersecurity organisation which will pay each time they deploy or module their customers. We also consider transferring the BBTR module and knowledge to a third party on a fair price basis.

Within TECNALIA another value creation target we have is the creation of Start-ups baes on the solutions/services we manage to create. In this direction currently an analysis is undergoing on the creation of a Start-up for selling the above mentioned TraceBlock product, which will mean that if this start-up is created it potentially will be the option by which the BBTR Component will be provided to the market. This start-up creation process is managed together with TECNALIA Ventures (https://www.tecnaliaventures.com/) an organisation focused in the creation of start-ups based on research results but is also focused in the generation of value from the research results. It is early to actually be able to identify the status since the implementation of the BBTR module is in 2020.

2.4.13 ICOM, Greece [Industry]

Partner Profile

Intracom Telecom is a global telecommunication systems & ICT solutions vendor operating for over 40 years in the market. The company develops and provides products, solutions and professional services primarily for fixed and mobile telecom operators, public authorities and large public and private enterprises.

Individual Goals of Exploitation

ICOM, as an IT systems vendor and solution integrator, considers the SPHINX toolkit as an integral component of the solutions it offers to the healthcare IT domain. ICOM's Information Security Management Initiative aims at assisting its customers to understand why, what, and how to spend on security. ICOM already today provides services to assist customers in the establishment of an adequate and robust security organization, alignment with business requirements, and formalization of the necessary security roadmap to mitigate security risks. Also, the company provides technical services intended to re-engineer the customers' infrastructures in reference to information security, assess the security posture and provide support throughout the information security lifecycle management. Another major offering relates to the provision of technologies for protecting the corporate infrastructure and data centres against external and internal attacks. In this context ICOM will explore the path to incorporation of SPHINX outcomes into its product / services offerings.

Another aspect that should be highlighted relates to the fact that, being a Cloud Services provider with embedded Security as a Service, ICOM will invest on shaping its Cloud offerings to become SPHINX-enriched. It is worth to mention that ICOM has already marketing and sales channels to Healthcare Service Providers and Pharmaceuticals, offering them private and hybrid cloud services, FW/IPS as a Service, WAF as a Service and Endpoint Security as a Service.

Identified Exploitable Project Results

Result/Asset	Type	Exploitation options	Target audience

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Common Integration Platform (CIP)	Individual component	Business case	Industry

Value creation to the organisation

Apart from the positive impact due to knowledge generation, SPHINX project comprises for ICOM the vehicle to enrich its products /services portfolio and establish strategic partnerships with project partners who are IPR owners. This comprises an invaluable positive impact for the company.

2.4.14 INCM, Portugal [non-profit]

Partner Profile

INCM´s mission is to develop, produce and supply products and services, with focus on security and authenticity features, essential for trust services (B2C, G2B, G2C), innovating and producing applications of high standards of security as a guarantee of their authenticity and trustworthiness.

Individual Goals of Exploitation

INCM intends to exploit its participation in the SPHINX project for exposing its engineers and researchers in high level technical work in the area of cybersecurity, which will help to boost their cybersecurity skills not only at the digital healthcare environment but also in other new fields such as mobile identification. The INCM engineers and researchers have the opportunity to get the knowhow on how to define a software architecture and the necessary steps to successfully implement and test it. INCM will exploit the project's findings in enhancing and strengthening its positioning within the EU market and research domain, establishing partnerships and agreements for further collaborations with the large corporations participating in SPHINX. Last, the presentation of the developed work in conferences and at INCM social media webpages will also help INCM to show to the society and to potential customers that INCM is committed to innovate and preparing a digital future.

Identified Exploitable Project Results

Result/Asset	Type	Exploitation options	Target audience
Scientific and technical knowledge	Services, methodologies, models	Concrete exploitation plans	ALL

Value creation to the organisation

INCM envisages to establish new research collaborations with SPHINX project partners with the aim to transpose the knowledge developed during the project activities in future cybersecurity research projects applied to different digital fields.

In addition, INCM personnel will acquire new knowledge on the cybersecurity field which will help to improve the current technical skills in this field.

INCM will also verify the business potential of the developed cybersecurity platform in the healthcare field and based on the business potential may sign contracts among partners to collectively exploit the results after SPHINX project ends.

2.4.15 Polaris Medical, Romania [End user]

Partner Profile

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

It is a private shareholder company, established in 2014, located in Suceagu village, 12 km away from Cluj-Napoca, Romania. The company is a private hospital specialized in medical recovery and rehabilitation with the capacity of 180 beds.

Individual Goals of Exploitation

Polaris Medical envisions to fully integrate the SPHINX platform to their core product. In this respect, after the completion of the project, in case SPHINX platform development continues and there is the appropriate funding, it is willing to continue the piloting. Its main goal is to install the platform as a final product and finally enhance the data protection of their services and equipment/devices.

In addition, Polaris Medical aims to promote the secure data exchange between their patients and will build trust with their partners by being proactive in their activity's domain.

Identified Exploitable Project Results

Result/Asset	Type	Exploitation options	Target audience
Pilot cases success stories	Results of demonstration pilots	Concrete exploitation plans	ALL
SPHINX policy recommendations	Policies	Concrete exploitation plans	Policy makers

Value creation to the organisation

Constant use of modern ICT technologies in all departments of Hospital raise the necessity of Cyber Awareness among hospital's personnel. Using and advertising SPHINX Toolbox, is one goal for POALRIS MEDICAL to share experience and raise awareness of cybersecurity in medical field.

Polaris Medical aims to demonstrate that using this tool, all patient's personal data that are processed, will not be at any time exposed to cyber risks.

One other goal is to maintain the pilot project and increase the potential to replicate the platform at external Health Delivery Organizations.

2.4.16 HES, Portugal [End user]

Partner Profile

HES is a reference hospital in the delivery of healthcare for the Alentejo region, serving more than 440,000 people with specialised medical services in the areas of maternity and paediatrics, cardiology, neurology, infecciology, nephrology, immunoallergology, rheumatology, physical medicine and rehabilitation, pathology, pneumology, otolaryngology, psychiatry and mental health, psychiatry, childhood and adolescence and dermatology.

Individual Goals of Exploitation

HES aims at deploying the SPHINX platform in replicated real environments. Thus, withing the project duration it will promote the pilot demonstration to policy makers and key persons related to national funding, in order to prepare the ground and apply for funding when the platform is ready. In this way, this action will influence more hospitals in the country to get also the funding and get benefit from SPHINX platform.

In the meantime, during the period that IT partners need to develop further the platform and deliver the final product, after the end of SPHINX project, the Polaris Medical is willing to continue the piloting so the infrastructure will be ready and the platform tailored to its needs. However, additional funding will be calculated as it should be necessary at this stage.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Identified Exploitable Project Results

Result/Asset	Type	Exploitation options	Target audience
Pilot cases success stories	Results of demonstration pilots	Concrete exploitation plans	ALL
SPHINX policy recommendations	Policies	Concrete exploitation plans	Policy makers

Value creation to the organisation

The growing increase in the use of technology in health poses several challenges in the security and encryption of information. With the development of this tool it is intended to ensure this security and enhance the use of technology, significantly improving certain processes and the reliability of information.

This will impact the entire patient circuit, enhancing gains for the hospital and the population.

It is the aim of HES to maintain the pilot project and increase the potential to replicate the platform at external Health Delivery Organisations.

2.4.17 DYPE5, Greece [End user]

Partner Profile

The Regional Health Authority of Central Greece is a National Organisation responsible for administering all public body health organisations that operate in two large regions of Central Greece (Thessaly and Sterea). These include 13 Hospitals (1 of which is a University Hospital) in 10 major cities and 60 Primary Care - Health Centers (urban and rural areas), covering a population of 2 million people.

DYPE5 provides 2 Pilot Sites (2 major public Hospitals) as testbed for testing and validating the SPHINX ecosystem and its technical components. These HDOs are:

- the University Hospital of Larissa
- the General Hospital of Volos

DYPE5 also leads WP7 and will be steering all pilot sites towards successful execution of the validation scenarios portfolio.

Individual Goals of Exploitation

DYPE5 acknowledges that this is a RIA project and the TRL will not be mature enough to produce market-ready cybersecurity products. Ergo, installing SPHINX components in the hospitals' actual production environments will not be sought, to avoid security and other operational malfunctions during the validating phase. Replicas of the Hospitals' premises, information systems and production business cases will be provided instead, establishing a simulated replicated real environment for the SPHINX technology components to be deployed and tested during the execution of the scenarios.

Following the above, DYPE5 aims (1) to opt for maintaining the pilot sites on a research level, after the project's completion, to support any further development of the SPHINX tools. Additionally, DYPE5 shall also aim (2) to increase the potential of replicating this research on external (to the SPHINX project) Health Delivery Organizations. These two goals can be facilitated if proper funding is sought. To enable this continuity, DYPE5 will take the necessary actions to seek for funding on Regional / National and European level. DYPE5's necessary actions include:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

1. pilot demonstration and impact presentation to Regional / National and European decision-making funding bodies and organizations
2. pilot demonstration, impact presentation and replication plans to external HDOs to raise their interest for adopting the SPHINX ecosystem and contributing to its research and development (starting from the Hospitals under DYPE5's jurisdiction)

This endeavour will be significantly reinforced if technical partners opt in to jointly exploit the SPHINX results, either by seeking the appropriate funding or investing (themselves) to further develop their products and expand their deployment. Depending on the pilot findings, the maturity of the technical components and the potential proper funding, DYPE5 shall explore the possibility of establishing contracts with the technical partners under the scope of continuing the research and development of SPHINX or pursue the preparation of proposing SPHINX as an IA.

Additional to the two aforementioned goals, DYPE5 aims (3) to raise the level of awareness and knowledge of cybersecurity amongst the workers and professionals in the HDOs. Capitalizing on the scientific/technical knowledge produced by academic and technical partners, DYPE5 will venture a two-facet approach:

1. Improve the level of awareness, knowledge and competency around the cybersecurity landscape, for the HDO's ICT personnel,
2. Increase/change the level of awareness on cybersecurity concepts and culture for the non-ICT personnel and upper management.

Lastly, another exploitation goal (4) that DYPE5 has set, is to engage in and support dialogue with policy makers, on a National and European level, to increase public funding for cybersecurity protection of HDOs. This includes policy recommendations based on evidence provided by the testing and validation, which should make the case for re-allocating sufficient financial, organizational and human resources to health ICT and especially cybersecurity technology.

Identified Exploitable Project Results

Result/Asset	Type	Exploitation options	Target audience
Pilot cases success stories	Results of demonstration pilots	Concrete exploitation plans	ALL
SPHINX policy recommendations	Policies	Concrete exploitation plans	Policy makers

Value creation to the organisation

The value expected to be created breaks down to the following aspects:

- **Awareness**: Cultivate, amongst the health professionals, a state of mind and perception that is aware of the potential cyberthreats in conducting their daily operations
- **Knowledge and Competency**: Fortify HDOs' cyber-defence by increasing the skills and knowhow of their ICT personnel
- **New Technology**: Capitalize on SPHINX innovation to pave the way for security improvement of the ICT infrastructures
- **Sufficient Funding**: Shift national and regional policy towards allocating funding to ensure the appropriate prerequisites (infrastructure, human resources, skillset) for building a secure e-health environment.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

3 Business cases for exploitation

3.1 Context

The SPHINX business cases outline why the target market would be interested in the exploitable results, what would be the benefit the market will gain from the results, and propose through business models, how and who will create the bridge between the consortium and the target audience, aiming to bring the results to the market.

3.2 Market context

SPHINX business potential can directly impact two different stakeholder groups on the health and cybersecurity domain; the Health Provision Organisations (HPO) and the Industry (IoT and security). The Regulators/Policy Makers will be also engaged because they are the key stakeholders who influence the market.

Health Provision Organisations

The current state of the art in cybersecurity for the hospitals utilises a top-down approach, aiming to protect the system from cyber at attacks but not to predict them. At the same time, there is a lack of tools for the modelling and prediction of cyber-attacks. For this reason, hospitals cannot efficiently monitor the network, and thus they are unable to protect patient data.

Naturally, the SPHINX platform will provide near-real time vulnerability assessment of HPO's operating IT Ecosystems. It will provide the means to HPOs to become aware and understand the cybersecurity risks (know or unknown threats and vulnerabilities) and to make informed decisions to choose only SPHINX certified devices, affecting their cyber-physical security and privacy. Naturally, the success of SPHINX platform is dependent also on the hospital staff's willingness to change the way they use the systems that will increase the data privacy and integrity.

The three project pilot sites (General Hospital of Volos (Greece), University Hospital of Larissa (Greece), Hospital do Espírito Santo de Évora (Portugal), and POLARIS Medical Clinic (Romania)) will evaluate the proposed business cases that will easily motivate the hospital staff to align with the alerts they receive from the IT department about possible Cyber security threats.

Industry (IoT and security)

Industry at the IoT and security sector are an important market actor in the sector. They can be from different fields, such as:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

- **Industry producing digital medical devices** (e.g., medication infusion systems, pacemakers) collecting personal health details are becoming more sophisticated and connected, allowing remote visualisation and the automatic incorporation of data in personal health records;
- **Industry producing digital wearables and IoT devices**, such as activity trackers, watches incorporating heart rate sensors, smart home sensors, albeit not rated as medical devices may produce data that is directly or indirectly relevant for purposes of assessing a patient's health and wellness status
- **Industry producing communication devices and enabling devices** such as tablets, phones which uphold info of patient, individual patient datagrams, patient photographs and variety of other sensitive info.
- **eHealth service providers**, software development industry producing the applications that analyse health data to visualise the tracking.
- **Cyber security service providers**, software development industry producing the services for cyber threads protection.
- **Cyber security practitioners**, experts in the security domain from software development industry.
- **Innovative start-ups, SMEs in the health domain** focusing on modern, digital critical infrastructures, and secure information systems

With revenue business-driven approach, they are supporting new business models to improve their positions in the markets. However, the industry lacks access at replicated real environments (e.g. hospitals) to evaluate the technology and forecast future needs, that constitutes a high market risk.

On the contrary, SPHINX will offer a platform and individual components that will be tested in three pilot sites and will also give industry the opportunity to test the medical equipment and get the detail compliant and certification report to assess if the device or service is vulnerable for misused or its attack surface is missing crucial security requirements and protects data privacy.

Complementary, the industry may provide valuable feedback to SPHINX on the proposed business plans to serve the targeted market needs.

Regulators/Policy Makers

The Regulators and Policy Makers in the cyber security for the Health sector are important lobbying actors because they can put pressure in decision-making procedures. On the one hand, they have to define long term regulations to ensure stability in the market while on the other hand, it is important that the business models are aligned with relevant regulations.

The most crucial information for Regulators and Policy Makers is how the market reacts from reliable simulations. The SPHINX project, through the application of technology in real environments, will be able to provide them with technical and financial information along with the social impact.

SPHINX will also investigate improvements and alternatives to current institutional and governance frameworks in order to improve cybersecurity awareness and stimulate the usage of the proposed solution aiming to empower patient data privacy.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

3.3 Business model

SPHINX will develop two (2) business models, one for every target group; the Health Provision Organisations (HPO) and the Industry (IoT and security) aiming to achieve the following exploitation goals:

- Verify the business potential of the platform in the health sector, providing the platform free as an open source or open architecture and sell the services
- Wider adoption of the individual components, using the components as an add-on of the existing software or service

The business model will be co-designed by the entire consortium through the Business Model Canvas. The co-design will follow three phases. The first phase will take place among the consortium members who belong to the two different target audience categories; industrial members who scientific and technological backgrounds in the field of cyber security and experience on business at the targeted audience, and members from the health sector who are aware of the real market needs. The business models will be evaluated during the second co-design phase through the involvement of external market stakeholders, who will provide their feedback. The revised business models will be further evaluated and finalised by the project consortium during the third co-creation phase. Each co-design phase will be implemented through workshops, which will take place mainly during the project meetings.

Turning to the content, two different business models should be developed for the public and private sector. Therefore, the following CANVAS requirements will be addressed from such two different perspectives:

Key partners:

- Who are your key partners/suppliers?
- What are the motivations for the partnerships?

Key activities:

- What key activities does your value proposition require?
- What activities are important the most in distribution channels, customer relationships, revenue stream…?

Value proposition:

- What core value do you deliver to the customer?
- Which customer needs are you satisfying?

Customer relationship:

- What relationship that the target customer expects you to establish?
- How can you integrate that into your business in terms of cost and format?

Customer segment:

- Which classes are you creating values for?
- Who is your most important customer?

Key resource:

- What key resources does your value proposition require?
- What resources are important the most in distribution channels, customer relationships, revenue stream…?

Distribution channel:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

- Through which channels that your customers want to be reached?
- Which channels work best? How much do they cost? How can they be integrated into your and your customers' routines?

Cost channel

- What are the most cost in your business?
- Which key resources/ activities are most expensive?

Revenue stream

- For what value are your customers willing to pay?
- What and how do they recently pay? How would they prefer to pay?
- How much does every revenue stream contribute to the overall revenues?

As a result, the available business models will empower the industrial partners to exploit the individual components. In terms of the SPHINX platform, a further **business plan will be developed for the partnership** that will be decided to exploit it commercially. The business plan will include the following key information:

- Market analysis (market context, segmentation, competition, positioning, SWOT)
- Unique selling proposition
- Description of the platform and service offering (packaging)
- Pricing model
- Commercialisation plan (marketing distribution channels)
- Costs
- Financial plan

3.4 Engagement

In order to reach the project exploitation goals, SPHINX consortium will engage the targeted audience through the dissemination activities *(see D8.2 SPHINX Dissemination Plan - M12, chapter 2)* to present the SPHINX **outcomes in the replicated real environments**, the **social benefits** and cross check with them their **benefit on the proposed business models**. Based on the engagement strategy, the table below summarises the dissemination activities planned to take place from the different project partners.

Stakeholders	Geographical range	Basic activities	Main partners involved
Industry (Security and IoT)	National level: all partner countries European level Global level	Workshops (Feedback and Training), Pilot Dissemination, Conferences, Media Publications	IT Large Enterprises IT SMEs
HPO	National level: pilot partner countries	Pilot Dissemination, Workshops (Feedback and Training), Conferences, Newsletters	End users Non-Profit Organisation
Policy	National level: all partner countries European level	Press releases, Workshops, Conferences, Scientific papers	End users Universities Research Institutes Non-Profit Organisation

Table 5: Target group engagement strategy overview

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

4 Sustainability plan

4.1 Context

SPHINX project will deliver an IT solution that will be tested and demonstrated in three different countries (Romania, Portugal and Greece) aiming to contribute to the expected impacts set out in the H2020 work programme '**Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures**'.

SPHINX will also develop the sustainability plan to maximise the impact and secure that the project results will remain active and even further expanded, beyond the contractual project end. The sustainability plan aim will be four-fold:

- **Pilot organisations maintain the SPHINX platform**. During the project progress, the four project pilot sites (General Hospital of Volos (Greece), University Hospital of Larissa (Greece), Hospital do Espírito Santo de Évora (Portugal), and POLARIS Medical Clinic (Romania)) will demonstrate the SPHINX platform in a replicated real environment but with limited data. After the completion of the project, the platform TRL will be increased but not ready to enter the market with real patient data. Therefore, a partnership will be created that will be comprised of some SPHINX partners to work in order to find further funding (e.g. IA) and proceed to continue the platform development while the pilots will be able to continue testing the SPHINX platform.
- **New Health Provision Organisations replicate the SPHINX platform**. The SPHINX platform is designed in a scalable manner in order to be used by different IT infrastructures that hospitals across Europe may have. In addition, the steps that project pilots will follow to deploy the platform will be generated into replication plans that any Health Provision Organisation will be able to follow to deploy SPHINX platform.
- **Verify the business potential of the SPHINX platform**. The business plan will be developed during the project to facilitate the business exploitation of the platform which will be evaluated by the stakeholders from the targeted market, to conclude on a mature plan of high potential. Partners will agree on a partnership to proceed and investigate to further funding, to develop this RIA result into a product ready to enter the market.
- **Proceed with the further usage of the other exploitable outcomes**. Industrial partners envisage to include the individual components at their portfolios. The partners from the public sector will expand the project results which apply in their activities (pilot cases success stories, replication guidelines, policy recommendations, scientific and technical knowledge).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

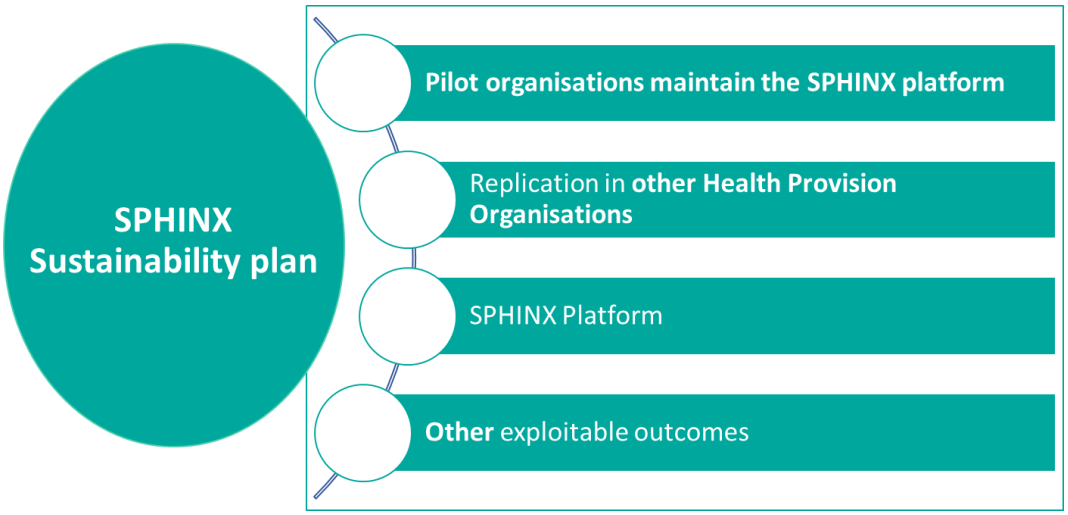

Figure 2: SPHINX sustainability plan approach

4.2 Methodology

The SPHINX consortium will implement the project with the vision to prepare the ground and reach the sustainability goals. The partner of common organisation types will work collaboratively towards the different goals:

Pilot organisations maintain the SPHINX platform: The IT private organisations will work collaboratively to develop the SPHINX platform that will deliver to the end-user partners. They will test the platform in their replicated real environments, against targeted risks and threats including combined cyber and physical attacks. In parallel, end-user partners will also monitor and control the cyber security and privacy risks, threats and incidents in terms of reliability of the real-time risk assessment, effectiveness in the prevention and mitigation of typical cyber security and privacy risks and user satisfaction. In this way, end-user organisations will validate the platform and communicate the findings of the pilot operation of the services with the IT private organisation to improve the SPHINX platform initial deployment to prepare an outlook for its large-scale usability.

As a result, by the end of the project the SPHINX platform will be tested in replicated real environment, but it will not be ready to be installed and run at hospitals with real data. Further research and development should be carried out to increase its TRL level. In this respect, during the project progress partners will agree on a partnership that will act to find the funding to continue the research work and pilot demonstration.

New Health Provision Organisations replicate the SPHINX platform: During the pilot preparation and deployment phase, the end-user organisations will develop the guidelines on how to replicate the hospital's ICT setup involving workstations, software applications, medical databases and connected medical devices, in order to adopt the SPHINX platform. As a next step, end-user organisations will take actions to communicate the successful deployment of the platform, the impact and the replication guidelines, with their existing network of Health Provision Organisations to attract their interest and motivate them to adopt later the mature SPHINX platform to their premises, when it will be a ready product.

Verify the business potential of the SPHINX platform: IT industry and SME partners will co-design with the exploitation manager the business models for the two targeted market segments: Health provision organisations and IT industry. To increase the business potential, they will take actions to present the business models at the targeted audience in order to receive feedback and verify that SPHINX proposed approach meets their needs. In addition, SPHINX consortium is aiming to get benefit of the strong demonstrations that will be implemented within the project timeframe, and present to the potential market the benefits of the SPHINX platform and its components in replicated real environment conditions.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Further usage of the other exploitable outcomes: A rich property of scientific knowledge will be produced during the project implementation through the mature research that experienced partners will carry out in this innovative discipline of cyber security in the health sector. Partners from Universities and research centres will take the necessary actions to expand this knowledge at new researchers and progress on this field. In addition, evidenced based policy recommendations will be outlined from the pilot demonstrations. Partners from public authorities will communicate such information at EU and national level.

4.3 Outcomes

It is expected that by the end of the project, the four pilot sites (sites (General Hospital of Volos (Greece), University Hospital of Larissa (Greece), Hospital do Espírito Santo de Évora (Portugal), and POLARIS Medical Clinic (Romania)) will pilot the SPHINX platform. Due to low TRL, the solutions cannot be operationally deployed in the productive environment and that goes for both pilots and potential external candidate HDOs. They should have done at least one meeting each with national funding authorities to investigate the way the potential to get the funds (redistribution of own/additional) needed (personnel, training services, platform maintenance, etc.), when the platform is a ready product.

It is also expected that at least three new Health Provision Organisations (one per pilot country) would be informed about the replication plan and received the training on how they would follow it to adapt it in their own needs. In addition, this outcome will be amplified through the ten meetings with policy makers (one in every consortium country) to present the impact aiming to influence the current policies.

Turning to the business potential of the platform, two business models for the targeted market segments (Health Provision Organisations and IT Industry) and the platform business plan, would be verified through a workshop in each pilot country with key stakeholders in order to receive their feedback.

A partnership will be created with the strong vision to find the funding and continue the research and development in order to release a final product. As a key priority, they will investigate for upcoming relevant Horizon Europe IA topics to apply.

Finally, the educational infrastructures of the three project Universities will be improved adapting the project scientific knowledge built through the research.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

5 Plan for the Dissemination and Exploitation of Results

5.1 Context

The Plan for the Dissemination and Exploitation of Results (PDER) is a detailed programme of the exploitation and dissemination activities for the different project partners. Its main scope is to investigate the potential impact of the exploitable results and evaluate the exploitation plan (overall and individuals) and the sustainability plan.

The PDER is divided into three parts, one for every project year which also represents the project phases:

- **Phase 1 – Preliminary Project Promotion phase (M1-M12)**:
  - Agreeing upon the communication strategy and future activities
  - Creating initial awareness in the markets related to the Project's objectives and scope
- **Phase 2 – Project Commercialisation phase (M13-M24):**
  - Create more "targeted awareness" regarding SPHINX technologies with key players and potential users
  - Inform the target market about the technological benefits of SPHINX
- **Phase 3 – Business Strategy phase (M25-M36):**
  - Maximising target market and industry awareness regarding the SPHINX solution
  - Thus, contributing to ensure the project sustainability and full exploitation

5.2 Plan for the Dissemination and Exploitation of Results and activities (M1-M12)

During the first project year, the consortium has focused the efforts to develop the exploitation and sustainability plans and prepare the ground for implementation through the introduction of SPHINX project to the targeted stakeholder groups.

A/A	Exploitation Plan	Activity this period	Partners involved	Duration
1	Design the exploitation strategy and individual exploitation plans	The overall and individual exploitation plans described in the proposal, have been enhanced during the project implementation.	VILABS, ALL	M6-M12
2	Design the sustainability plan	Along with the R&D progress, and the exploitation results definition, the sustainability plan is specified.	VILABS	M9-M12

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

3	Define the engagement strategy	The targeted stakeholders have been defined and therefore the strategy to engage them into project activities have been necessary. It is described as a part of D8.2 SPHINX Dissemination Plan.	VILABS	M3-M8
4	Monitor and review the SPHINX R&D towards the compliance with the project exploitation strategy	The requirements and specifications of SPHINX platform and its individual components, along with the use cases generated so far, are monitored to comply with the exploitation strategy	VILABS, VUB	M2-M12
5	Attend events and workshops to introduce SPHINX to the targeted audience	All the events and workshops that the consortium members participated were utilised to prepare the ground and introduce SPHINX project, especially for each partner exploitation plan. Apart from that, participation into synergy meetings have been done to enlarge further our network.	NTUA, DYPE5, FINT, EDGE, HMU, TECHNALIA, VILABS	M4-M12
6	Reporting the D8.4 Exploitation, Sustainability & Business Plans v1	Submit the D8.4. Exploitation, Sustainability & Business Plans v1	VILABS	M12

Table 6: PDER and activities of the first project year

The corresponding status of exploitable results during the first year is depicted at the following table.

A/A	Outcome	Status	Further work required	Deliverables/Reports
1	SPHINX platform	Requirements and specifications	Development, deployment and evaluation	D2.3-SPHINX Architecture
2	Pilot cases success stories	n/a	Pilot deployment, implementation and evaluation	D7.5 replicated real environment pilot demonstrators results and consolidation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

				including stakeholders experience evaluation and cost assessment (M36)
3	Replication guidelines	Requirements and specifications	Pilot deployment, implementation and evaluation	D7.5 Real-life pilot demonstrators results and consolidation including stakeholders experience evaluation and cost assessment (M36)
4	SPHINX policy recommendations	n/a	Pilot deployment, implementation and evaluation	Final report (M36)
5	Scientific and technical knowledge	Scientific Papers and Deliverables developed and published	R&D progress	All published scientific and technical knowledge are available at Zenodo.
SPHINX individual components				
6.1	Decision Support System (DSS) & Analytic Engine	Requirements and specifications	Development, deployment and evaluation	D2.3-SPHINX Architecture
6.2	Anomaly Detection (AD)	Requirements and specifications	Development, deployment and evaluation	D2.3-SPHINX Architecture
6.3	Forensic Data Collection Engine (FDCE)	Requirements and specifications	Development, deployment and evaluation	D2.3-SPHINX Architecture
6.4	Vulnerability Assessment as a Service (VAaaS)	Requirements and specifications	Development, deployment and evaluation	D2.3-SPHINX Architecture
6.5	Cyber Security Toolbox (SCT)	Requirements and specifications	Development, deployment and evaluation	D2.3-SPHINX Architecture
6.6	Real-time Cyber Risk Assessment (RCRA)	Requirements and specifications	Development, deployment and evaluation	D2.3-SPHINX Architecture
6.7	Blockchain Based Threats Registry (BBTR)	Requirements and specifications	Development, deployment and evaluation	D2.3-SPHINX Architecture

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

6.8	Artificial Intelligence (AI) Honeypot (HP)	Requirements and specifications	Development, deployment and evaluation	D2.3-SPHINX Architecture
6.9	Sandbox (SB)	Requirements and specifications	Development, deployment and evaluation	D2.3-SPHINX Architecture
6.10	SPHINX Application Programming Interface for Third Parties (S-API)	Requirements and specifications	Development, deployment and evaluation	D2.3-SPHINX Architecture
6.11	Machine Learning-empowered Intrusion Detection (MLID)	Requirements and specifications	Development, deployment and evaluation	D2.3-SPHINX Architecture
6.12	Encryption Techniques Homomorphic Techniques (HE)	Requirements and specifications	Development, deployment and evaluation	D2.3-SPHINX Architecture
6.13	Security Information and Event Management (SIEM)	Requirements and specifications	Development, deployment and evaluation	D2.3-SPHINX Architecture
6.14	Security Protocol Analysis (SPA)	Requirements and specifications	Development, deployment and evaluation	D2.3-SPHINX Architecture
6.15	Data Traffic Monitoring (DTM)	Requirements and specifications	Development, deployment and evaluation	D2.3-SPHINX Architecture
6.16	Anonymisation and Privacy (AP)	Requirements and specifications	Development, deployment and evaluation	D2.3-SPHINX Architecture
6.17	Interactive Dashboards (ID)	Requirements and specifications	Development, deployment and evaluation	D2.3-SPHINX Architecture
6.18	Attack and Behaviour Simulators (ABS)	Requirements and specifications	Development, deployment and evaluation	D2.3-SPHINX Architecture
6.19	Knowledge Base (KB)	Requirements and specifications	Development, deployment and evaluation	D2.3-SPHINX Architecture
6.20	Common Integration Platform (CIP)	Requirements and specifications	Development, deployment and evaluation	D2.3-SPHINX Architecture

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Table 7: Exploitable outcomes status during the first project year

5.3 Plan for the Dissemination and Exploitation of Results and activities (M13-M24)

During the second project year, especially after M18 the consortium will be able to disseminate at the targeted audience (mainly the industry) with the available SPHINX technologies and discuss on the proposed business plans to receive feedback.

A/A	Exploitation Plan	Activity this period	Partners involved	Duration
1	Update the exploitation strategy, sustainability strategy and individual exploitation plans	The overall and individual exploitation plans will be revised based on the relevant stakeholders' during dissemination activities and according to the reviewers' comments.	VILABS, ALL	M13-M24
2	Monitor and review the SPHINX R&D towards the compliance with the project exploitation strategy	The requirements and specifications of SPHINX platform and its individual components will be monitored to comply with the exploitation strategy	VILABS, VUB	M13-M18
3	Business plan	Identification of the basic business plan. Discuss with relevant stakeholders for real business scenarios.	VILABS	M14-M24
4	Attend events and workshops to introduce SPHINX to the targeted audience	Consortium members will participate in events and workshops to utilise knowledge on current project results and discuss and evaluate their exploitation potential, especially to each partner individual exploitation plan. Continue the participation in synergy meetings to enlarge the network.	ALL	M13-M24

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

5	Engage the targeted stakeholders and validate project results towards exploitation potential	Consortium members will engage the targeted stakeholders to verify the results and investigate deeper collaboration.	ALL	M13-M24
6	Reporting the D8.6 Exploitation, Sustainability & Business Plans v2	Submit the D8.6. Exploitation, Sustainability & Business Plans v1	VILABS	M24

Table 8: PDER and activities of the second project year

5.4 Plan for the Dissemination and Exploitation of Results and activities (M25-M36)

The third project year will be the most appropriate period for the consortium to present at the targeted stakeholders the exploitable results, the benefit and the business plan.

A/A	Exploitation Plan	Activity this period	Partners involved	Duration
1	Update the exploitation strategy, sustainability strategy and individual exploitation plans	The overall and individual exploitation plans will be revised based on the relevant stakeholders' during dissemination activities and according to the reviewers' comments.	VILABS, ALL	M25-M36
2	Organise and attend events and workshops to introduce SPHINX to the targeted audience	The final exploitable results will be disseminated to the targeted audience presenting also the evaluation results to present the impact. In the case of commercially exploited results, the corresponding business plan will be presented as well.	VILABS, ALL	M26-M36
3	Disseminate the Business plan	Discuss with relevant stakeholders for real business scenarios.	VILABS	M26-M36
4	Engage the targeted stakeholders and validate project results towards exploitation potential	Consortium members will engage the targeted stakeholders to verify the results and investigate deeper collaboration.	ALL	M26-M36

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

5	Reporting the D8.10 Exploitation, Sustainability & Business Plans v3	Submit the D8.6. Exploitation, Sustainability & Business Plans v3	VILABS	M36

Table 9: PDER and activities of the third project year

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

6 Conclusions

Within the first project period, the first version of the exploitable outcomes released, and therefore the initial exploitation plan enhanced accordingly. More specifically, the basic characteristics of the results are now described in more details to identify the exploitation approach. The individual exploitation plans are now defined with respect to the goals of exploitation and identified project results, while the value creation for each organisation has been added.

Moreover, the business cases for the targeted organisations (Health Provision Organisations and ICT Industry) are described and will be used during the communications with the corresponding members.

Finally, the sustainability plan has been outlined so partners during the implementation of their tasks during the project, will focus on the further sustainability of results.

The following important activity is to co-design the Business Plan of SPHINX platform and the Business models for the target audiences. The outcome will be illustrated in the next version 2 of the Deliverable Exploitation, Sustainability & Business Plans.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.