Horizon 2020 Programme

H2020-SU-TDS-02-2018
Trusted digital solutions and Cybersecurity in Health and Care

DATA-PROTECTION TOOLKIT REDUCING RISKS IN HOSPITALS AND CARE CENTERS

Project Nº 826284

ProTego

D8.6 Final exploitation framework: Project impact, exploitation actions and sustainability plan

Responsible:	ICE
Contributors:	All Partners
Document Reference:	D8.6
Dissemination Level:	Public
Version:	v1
Date:	31/12/2021

Executive Summary

This deliverable presents the final exploitation framework for ProTego. ProTego exploitation will be wide-ranging and high impact in sectors including hospitals and healthcare and many others. The exploitation actions undertaken have included a refinement of the list of exploitable assets, followed by market, PESTLE and SWOT analyses per exploitable asset per customer segment. Based on the Market, PESTLE and SWOT analyses, which constitute a detailed review of the potential market opportunities, each asset owner has selected which business models will be exploited. Each asset owner has then gone on to undertake a financial assessment to determine which particular customer segments are the best for them to focus on for their chosen business model. Open-source strategies are an important part of the ProTego exploitation framework, and are set out in detail. The exploitation actions conclude with an information campaign, which is based on a video introducing the main innovations and a set of white papers giving more detailed information. These materials are appropriate for use during the COVID-19 pandemic and beyond. Finally, we present the sustainability plan, which underpins our ability to deliver the information campaign and achieve wide-ranging high-impact exploitation.

Contributors Table

DOCUMENT SECTION	AUTHOR(S)	REVIEWER(S)
I Introduction	Colin Upstill (ICE)	María Perez (Inetum), Luis Carrascal (Inetum), Antonio J. Gamito (Inetum), Juan Luis García (Inetum)
II Project Impact	Colin Upstill (ICE); María Perez (Inetum), Luis Carrascal (Inetum), Antonio J. Gamito (Inetum), Juan Luis García (Inetum)	María Perez (Inetum), Luis Carrascal (Inetum), Antonio J. Gamito (Inetum), Juan Luis García (Inetum)
III Exploitation Actions	Eliot Salant (IBM); Colin Upstill, Noel Thomas, Kate Miller (ICE); Esteban Municio (IMEC); María Perez (Inetum), Luis Carrascal (Inetum), Antonio J. Gamito (Inetum), Juan Luis García (Inetum); Dave Singelee (KUL); Salvador García Torrens (MS); Diana Trojaniello (OSR); Carlos Cilleruelo Rodríguez, Luis de Marcos Ortega (UAH); Steve Taylor (UoS)	María Perez (Inetum), Luis Carrascal (Inetum), Antonio J. Gamito (Inetum), Juan Luis García (Inetum)
IV Sustainability Plan	Colin Upstill (ICE); María Perez (Inetum), Luis Carrascal (Inetum), Antonio J. Gamito (Inetum), Juan Luis García (Inetum)	María Perez (Inetum), Luis Carrascal (Inetum), Antonio J. Gamito (Inetum), Juan Luis García (Inetum)
V Conclusions	Colin Upstill (ICE)	María Perez (Inetum), Luis Carrascal (Inetum), Antonio J. Gamito (Inetum), Juan Luis García (Inetum)

Table of Contents

Table of Figures

List of Tables

Table of Acronyms and Definitions

Acronym	Definition
BSD	Berkeley Software Distribution
BYOD	Bring Your Own Device
CAGR	Compound Annual Growth Rate
CI/CD	Continuous Integration/Continuous Development
COTS	Commercially available off-the-shelf
GDPR	General Data Protection Regulation
GRC	Governance, Risk and. Compliance
KCSP	Kubernetes Certified Service Providers
KMS	Key Management System
MDR	Medical Device Regulation
MVP	Minimum Viable Product
NISD	Network and Information Security Directive
PESTLE	Political, Economic, Social, Technological, Legal, Environmental
SaaS	Software as a Service
SIEM	Security Information and Event Management
SSM	System Security Modeller
SWOT	Strengths, Weaknesses, Opportunities y Threats
UAH	Universidad de Alcalá

I. INTRODUCTION

This deliverable presents the final exploitation framework for ProTego. It begins with a consideration of the project impact, reports in detail on the exploitation activities undertaken in the project and summarises the plans for sustainability.

II. PROJECT IMPACT

ProTego exploitation will be wide-ranging and high impact. It will include commercial exploitation of products and services by all the companies which have participated in the project and by at least one university spin-off company, community exploitation of software release as open source using various channels and including one project already supported by the Apache Software Foundation, cybersecurity awareness consultancy services backed up by material which can be widely used for academic teaching and evangelism and awareness raising in hospitals and healthcare, and further funded research which will build on the strong foundations established by ProTego and range across all the ProTego technologies and human factors.

III. EXPLOITATION ACTIONS

In this section we report on the exploitation actions undertaken in the final year of the project.

In the first phase of the exploitation activities (reported in D8.2) the ProTego project partners determined which project outputs they thought had the potential to be exploitable assets. These were subsequently refined. The Key Management System and Access Control System are now being considered as one asset. Similarly, the Network Performance Slicing and Network Privacy Slicing are now being considered one asset. Cybersecurity Services in Healthcare was identified as an additional exploitable asset; this has been combined with the User Requirements Elicitation Service and named Cybersecurity Awareness. The final list is shown below.

Exploitable Assets
System Security Modeller
Apache Parquet Modular Encryption
Continuous Authentication System
Key Management & Access Control System
Security Information & Event Management
ProTego Toolkit Assembler
Network Performance & Privacy Slicing
Cybersecurity Awareness

Table 1 - Exploitable Assets

These exploitable assets are described in more detail in section III.1, below.

Each exploitable asset has been analysed according to the customer segments identified during the second phase of the exploitation activities (reported in D8.4). These are shown below.

Customer Segment
Big data owners & managers
Generic business with sensitive data and entities managing complex IT systems
Hospitals & healthcare
IT companies
Public administrations

Table 2 - Customer Segments.

These customer segments are explained in more detail in section III.2.2, below.

The exploitation strategies per exploitable asset per customer segment have been developed via detailed Market, PESTLE and SWOT analyses. The ProTego approach to Market Analysis is explained in section III.2, PESTLE analysis is explained in section III.3 and SWOT analysis in section III.4. The Market, PESTLE and SWOT analyses per exploitable asset are reported in section III.5. These analyses enabled partners to identify the most promising combinations of exploitable asset and customer segment, to consider what business models were appropriate, and to make financial assessments of the potential exploitation.

We consider open-source software and report on our Open Source strategies in section III.7, and in section III.8 we report on our plans for an information campaign in the context of the COVID-19 pandemic.

III.1. Exploitable Assets

III.1.1. System Security Modeller

The System Security Modeller (SSM) analyses a model of an information system to find both the threats to the system and the corresponding security controls. The analysis takes into account both threat cascades (where one problem leads inevitably to another) and attack paths (where one step enables another). Through this deep analysis, the context of each asset in the system is fully taken into account and the highlighted threats are therefore of high relevance. The user is able to configure the business impact of each type of problem and the SSM combines this information with likelihoods from the threat analysis to determine risk.

In ProTego the SSM has been developed in various ways, including additions to the underlying knowledgebase and integration with the SIEM. The SIEM integration provides a “runtime” or operational view on the risks to the information system and uses a heuristic to recommend additional security controls that could be implemented to address new and current problems.

III.1.2. Apache Parquet Modular Encryption

As part of ProTego, IBM developed the standard for Parquet Modular Encryption which was officially adopted by Apache and is now part of the official Spark code base starting with Apache Spark 3.2.

In addition to this significant contribution to the open-source community, IBM has been internally exploiting this technology as part of the IBM Analytics Engine and IBM Cloud Pak for Data products.

III.1.3. Continuous Authentication System

ProTego has covered mobile security solutions. Hospitals and other health care centres usually involve a BYOD policy and medical and private information ends stored in multiple mobile phones. Furthermore, health care centres are developing and using mobile applications focused on patient monitoring or making appointments. This system usually relies on common authentication methods based on passwords, that over the years has been proved to not be enough.

To cover BYOD policies and the health care app, ProTego has developed a Continuous Authentication solution centred on mobile phones. This solution is capable of monitoring the activity of a user without the necessity of any specific interaction, and transparently is capable of obtaining to learn and identify the user of a mobile phone. Through Machine Learning models the Continuous Authentication system is capable of learning the behaviour of a user. This way if a smartphone is stolen or an unauthorized user is using a mobile app, the Continuous Authentication system will be able to detect it.

The Continuous Authentication system also offers intrusion prevention capabilities. The system can raise alerts to the ProTego Security Information & Event Management system and lock a smartphone or log off a user from a mobile application.

III.1.4. Key Management & Access Control System

The key management and access control system consists of two components which are tightly coupled to each other. The first component in the framework is the Key Management System (KMS). It is based on the open-source software Vault. The role of this component is to securely store the cryptographic keys needed to unwrap the data encryption keys that are used by the Apache Parquet Modular Encryption algorithm in the Data Gateway. Therefore, it either stores the keys received by the Data Gateway, or it receives a request from the Data Gateway to send the required unwrapping key. The former happens in the process of a data producer uploading (writing) data to the system, while the latter happens when a data consumer is requesting to read

data from the system. This brings us to the second component in the framework, the Access Control System. Whenever a data consumer requests access to data, the access control system will evaluate this request. It will then either reject the request, or grant access. In case of the latter, it will instruct the KMS to send the unwrapping key to the Data Gateway. In other words, the Access Control System decides whether the KMS should transport the unwrapping keys to the Data Gateway or not.The Access Control System has been implemented by KU Leuven and deployed as a Docker container on the ProTego platform.

III.1.5. Security Information & Event Management

A SIEM implements a set of technologies able to help detect, respond, and neutralize cyber threats. The main objective is to give an organization a global vision of IT security, allowing to have its complete control. By collecting and managing information about events that take place it is easier to detect trends and focus on anomalies.

The underlying principle of a SIEM is that security-relevant data in an organization takes place in multiple locations. By being able to see all that data from a “single pane of glass” makes it a lot easier to detect trends and uncommon patterns.

The concept of a SIEM rises from combining the functions of two different kinds of systems:

- SEM: Security Event Management. A system that centralizes the storage of information and allows a near real-time analysis of what is taking place in security management, detecting and analyzing abnormal patterns.
- SIM: Security Information Management. A system that collects long-term data on a central repository to be analysed later, providing automated reports.

III.1.6. ProTego Toolkit Assembler

ProTego is an integrated toolkit which consists of six tools: System Security Modeller, Security Information and Event Management, Continuous Authentication, Data Gateway, Access Control Framework, and Network Slicing. The Toolkit Assembler is an integrated set of open-source tools including Rancher, Istio, Kubernetes, and docker, using GitLab, HELM and Longhorn. Together they provide end-to-end continuous integration/continuous development (CI/CD) and deployment support to DevOps teams. This allows for an updatable, continuously integrated platform to be deployed in each hospital. These are mostly deployed as Docker containers on a ProTego platform, but certain aspects can be deployed on mobile devices, or on public or private clouds.

III.1.7. Network Performance & Privacy Slicing

In order to add and additional security layer for the data in transit, IMEC has integrated different open-source tools to provide the data flows with performance isolation and privacy isolation.

On one hand, the network slicing in charge of the keeping a guaranteed end-to-end QoS, including radio Wi-Fi slicing, for the different traffic flows. This is done by virtually “slicing” the network resources and assigning one slice to each flow. While the slicing in the wired segment is done through traditional well known traffic engineering tools, the wireless slicing is done through 5GEmpower, an open-source framework for wireless networks virtualization. On the other hand, for the privacy isolation, we leverage standard IPSec techniques to encrypt the data per slice, using open-source libraries to encrypt and decrypt in the endpoints.

III.1.8. Cybersecurity Awareness

Jointly with the technical components of the ProTego toolkit, Cybersecurity awareness services have been developed with the objective of complementing the toolkit by enforcing the weakest link of the cybersecurity chain: the human factor.

These have been addressed to both healthcare staff and patients and designed in a way that covers the most common bad behaviours users perform while treating with medical data and electronical devices. The final shape has been an intuitive educational website with easy-to-

consume material, mainly videos, with a holistic approach that is suitable to be used across the EU healthcare organizations.

The dissemination of this content has been recognized as a relevant factor for the success, so it has been described the correct way to spread the material by involving clinical managers in the process.

III.2. Market Analyses

A Market Analysis is a complete assessment of the size and nature of a market for a product or service It takes into account both quantitative factors, such as the volume and value of the market, and qualitative factors, such as competition and regulation. It can be simple and brief or very detailed, depending on the intended purpose and the information available. For more background see e.g. Wikipedia [1], NetMBA [2] and also pestleanalysis.com [3], [4].

In ProTego we undertook market analyses per exploitable asset per customer segment.

III.2.1. Dimensions of Market Analysis

Figure 1 - The many possible dimensions of market analysis.

There are many possible dimensions of market analysis. Those chosen for ProTego to help us better understand our markets and customers for ProTego assets were as follows.

Market volume: Size of the given market (e.g. number of participants or sales per year). Together with market value, this helps illustrate the scale of a market.

Market value: Size of the given market in terms of the monetary value of products or services exchanged per year. Considered alone, market value gives a better insight into the size of a market than volume.

Market growth rate: Extrapolated from historical data (if any; otherwise estimated based on comparable examples), and considering growth drivers.

Market profitability: How easy is it to make money in the market? Consider e.g. customer power, supplier power, barriers to entry, product or service USPs, threat from alternative products or services.

Market need: Customer need for particular products or services within the given market. Typically, the higher the need, the more attractive the market.

Competition: Competition created by other businesses offering comparable products or services in the given market.

Regulation: Regulation affecting entry to and operation within the given market, including EU Directives, national laws, and regulations defined by industry bodies (for ProTego, these include e.g. GDPR, the Network and Information Security Directive (NISD), the Medical Device Regulation (MDR), and various ISO and ETSI standards).

Key success factors: Things that are necessary to achieve exploitation objectives.

III.2.2. Customer Segments

The following table details the customer segments used in the Market, PESTLE and SWOT analyses. The customer segments were identified in a workshop-based Market Opportunities exercise, reported in D8.4.

Customer segment	Customer types	Description
Hospitals & healthcare entities	Hospitals including management and IT system administrators; Clinics including management and IT system administrators; Primary assistance including management and IT system administrators	In this segment of customer are Hospital Centers (public and private), specialty centers (X-ray and MRI centers, medical specialties, etc.), primary care health centers, dental clinics, aesthetic clinics, residences medicalized of elderly.
Public administration	National/Regional Health Service; Public Administration IT systems administrators	The clients of the public administration are all those ministries or public entities, such as the Ministry of Transport or the Ministry of Education ... or city councils of large cities.
Generic business with sensitive data and entities managing complex IT systems	Areas providing Wifi services e.g. Commercial Centres; Transportation operators including essential infrastructure i.e. airports and ports; Financial Entities including Banking and Stock markets; Insurance Companies; Marketing Companies; ISP; Universities (student portal); Entities providing corporate intranet	In this generic group of customers who manage sensitive data and have complex IT systems we find large shopping centres, airports, train stations, insurance companies, marketing companies, banks, universities ... They are not clients that handle health data, but they are personal data of users.

Big data owners & managers	Client database owners and managers, both public and private sectors; Entities performing Big Data analysis in cloud environment, both public and private sectors	These clients are large corporations that store a large amount of user data, such as AWS or Google or all those companies that have a storage cloud.
IT companies	Complex IT systems administrators; Telcos (incl. 5G); Security consultants; Mobile app developers; Online shopping; Social media networks	In this type of customer (IT companies) we can find consultants, ICT service companies, software development companies, e-commerce portals, etc. They are a type of customer who have some specialization in ICT and are aware of cybersecurity, but due to the importance of their data, their protection is very necessary.

Table 3 - Details of Customer Segments.

III.3. PESTEL Analyses

PESTEL is a mnemonic which in its expanded form denotes P for Political, E for Economic, S for Social, T for Technological, E for Environmental and L for Legal (the last two are often reversed, with the mnemonic PESTLE).

Figure 2 - The dimensions of a PESTLE Analysis

A PESTEL analysis [5] is a framework to analyse the key factors (Political, Economic, Sociological, Technological, Legal and Environmental) influencing an organisation from the outside.

A PESTEL analysis is about the asset owner's organisation, in the context of a market, so it follows on from the ProTego market analysis.

The analysis was per exploitable asset and per customer segment, for each dimension of the PESTEL analysis.

The key question for each dimension of the PESTEL Analysis was "what are the trends that influence the exploitation success of ProTego outcomes?".

III.4. SWOT Analyses

A SWOT analysis considers the Strengths, Weaknesses, Opportunities and Threats of some endeavour.

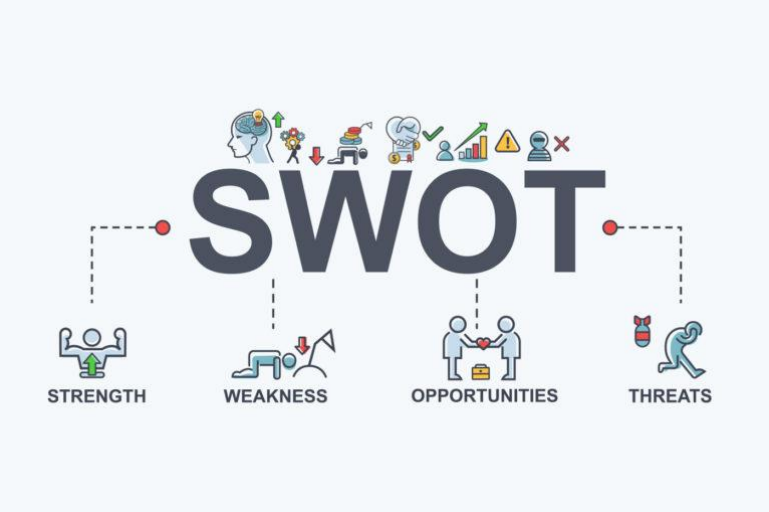

Figure 3 - The dimensions of a SWOT Analysis.

The analysis was per exploitable asset and per customer segment, for each dimension of the SWOT analysis

We considered the Strengths, Weaknesses, Opportunities and Threats in respect of the asset owner's organisation exploiting their ProTego asset in each customer segment.

III.5. Market, PESTLE and SWOT Analyses per Exploitable Asset

III.5.1. System Security Modeller

III.5.1.a. Market Analysis

The System Security Modeller (SSM) is placed in governance, risk and compliance (GRC) market sector, the global market for which was valued at $35.1 billion in 2020 with an expected CAGR of 13.7% to 2028. Risk management software accounted for 25% of this market [6].

The SSM is positioned partly as a tool to assist in ISO 27001 compliance work. Data for ISO 27001 certification is available [7] and is a useful measurable surrogate for the market growth rate. The compound annual growth rate (CAGR) for ISO 27001 certification since 2006 across all sectors worldwide is 21% and since 2018 is 19%. Of the customer segments identified above, they are all broadly similar apart from "public administration" which has experienced a (still encouraging) CAGR for ISO 27001 certification since 2006 of 21% and since 2018 of 7%.

The market need and profitability are both considered to be high in businesses where there is sensitive data, with hospitals and healthcare being a good example of this.

The increasing regulation of companies (e.g. GDPR, NIS) will increase demand for the SSM.

Finally, key success factors are a Minimum Viable Product (MVP) and case studies.

III.5.1.b. PESTLE Analysis

The key factors from the PESTLE analysis are as follows.

- Political: strong lead and investment from UK government into cyber-security.
- Economic: interest rates are likely to increase (from a very low level) increasing cost of capital. Brexit has potentially changed the cost of providing services to EU member states.
- Social: Increasing social awareness of cyber-security and data-protection leading to increased demand on companies to secure their systems and increased reputational and business damage to those that fail.
- Legal: Increasing regulation of companies (e.g. GDPR, NIS) will increase demand.

III.5.1.c. SWOT Analysis

The key factors from the SWOT analysis are as follows.

- Strengths: market-leading threat and risk analysis software.
- Weaknesses: product is not yet ready for market and it is an unknown and unproven proposition for customers.
- Opportunities: increasing awareness of cybersecurity means that companies are willing to spend and there is a trend towards risk-based approaches.
- Threats: there are several competitors in the software space who can adapt, and a new product in particular must strive to overcome the ‘do nothing’ inertia of businesses.

III.5.2. Apache Parquet Modular Encryption

III.5.2.a. Market Analysis

The key success factor is that this result from ProTego has already been accepted as a standard by Apache and integrated into the official Apache Parquet code base.

The technology has already been incorporated into two IBM offerings and it is expected that with its official release as part of Apache Spark 3.2 we will see a lot more offerings from many different vendors using this technology in the future.

III.5.2.b. PESTLE Analysis

Using PME should meet any compliance directives for storing data in encrypted format in all customer segments. As the code is open source, there are no licensing fees.

III.5.2.c. SWOT Analysis

The key factors from the SWOT analysis are:

- Strengths: Parquet is widely used today for storage of Big Data but is missing encryption for extra security.
- Weakness: Requires extra software, including a Key Management System.
- Opportunity: Integration into Spark opens the door for this technology to widely used.
- Threats: Other encryption techniques exist.

III.5.3. Continuous Authentication System

III.5.3.a. Market Analysis

Multiple companies with a BYOD policy could be interested in a Continuous Authentication solution in order to improve their mobile security. Also, mobile device manufacturers could be interested in this solution and integrate it into their own mobile device management solutions. This offers a huge market volume, value, and growth rate. Also, it is necessary to mention the lack of competitors focused on mobile devices, most of the existing technologies and companies only offer continuous authentication solutions to computers.

Key success factors are the ease of installation and integration.

III.5.3.b. PESTLE Analysis

Further political regulations are being studied to be approved in the near future (e.g. NIS2). These new regulations will force the investment of companies in cybersecurity measures. Mobile device security is and will be a central factor of companies' security that will increase over the coming years.

III.5.3.c. SWOT Analysis

Due to the lack of standards and multiple manufacturers in the mobile world, creating an adaptative and universal solution for mobile phones is not feasible. Furthermore, restricted systems like iOS make almost impossible the development of any Continuous Authentication solution, without the cooperation of apple.

UAH has developed a multidevice solution based on Android, without the necessity of any special requirements or modifications in the system. Any modern Android device, version greater than 10, can use the developed system. The developed system is a software solution and can be installed like any normal mobile app.

The support of mobile devices presents a huge opportunity, due to the fact that most company employees used a mobile phone is their daily basis.

III.5.4. Key Management & Access Control System

III.5.4.a. Market Analysis

The exploitation strategy of KU Leuven is to initiate new research projects, either bilateral contracts with government/industry or funded research projects through open calls (i.e., local projects in Flanders or EU projects). Therefore, the Key Management & Access Control System developed in ProTego is not the asset that will be exploited, but rather a means to improve the visibility of the group and increase the chances of acquiring new research projects.

In the market analysis, it is important to distinguish between both types of research projects (bilateral or funded through open calls). The latter strongly depends on the amount of research funding available in Flanders and Europe, and policy decisions on the scope of expected research and innovation projects (i.e., the content of the call texts). For bilateral projects, the story is different, as market volume and value do influence the exploitation strategy. The market analysis shows that the total market value is average compared to the bilateral funding required to have a good project portfolio. Generic IT companies and big data companies might be the best targets to engage in bilateral research projects.

The key success factors are research excellence and visibility. The research group should have the right technical and scientific expertise available that the company/government is looking for. Moreover, the company/government has to know that it can find this required expertise in the research group. This visibility can be increased by scientific publications, but even more by other dissemination means. The latter also includes the outreach via existing/finished research projects (such as ProTego), for example by releasing Open Source software of the Key Management and Access Control System.

III.5.4.b. PESTLE Analysis

The need for cybersecurity and privacy protection is clearly increasing. The reasons for this are twofold. First, multiple recent legislation changes mandate that products and services should have mandatory cybersecurity and privacy protection. Second, also users are increasingly demanding that the products and services they buy, are secure and protect their privacy.

The competition is twofold. First, there are other research groups which also have expertise in cybersecurity and data protection. Second, there is competition from commercial-of-the-shelf solutions. These conventional cybersecurity solutions are already available and offered by commercial entities. In several use cases, there might be the need for security designs that advance the state of the art. The companies that have such use cases are the target entities for starting new joint research projects.

Despite the high demand for innovative cybersecurity solutions, the budgets of smaller organisations might be a blocking factor for starting new bilateral projects with a research group

.

III.5.4.c. SWOT Analysis

The SWOT analysis has shown the following insights.

- Strength: KU Leuven – COSIC has a strong track record in cryptography and cybersecurity research.
- Weakness: The outcome of cybersecurity research will be new insights and concepts, but not a finished product. This might conflict with the needs of companies that want a market-ready solution on a short time-horizon. This should be considered when initiating new research initiatives together with companies.
- Opportunities: Advanced cybersecurity solutions might not be a top priority for many organisations. However big data is clearly very sensitive, so there is a need for increased awareness of cybersecurity and privacy issues.
- Threat: The lack of cybersecurity awareness and an underestimation of the need for more advanced and stronger cybersecurity and data protection measures might hinder the technology transfer in cybersecurity and hence also the opportunities to start new research projects. This underestimation is often caused by an incorrect risk estimation.

III.5.5. Security Information & Event Management

III.5.5.a. Market Analysis

- Good market volume and growth rates.
- Market need highest in hospitals and healthcare.
- Competition is considerable.
- Added value of the ProTego SIEM is the integration with the SSM and the dynamic recalculation of risks.
- A key success factor is understanding the needs of the client.

III.5.5.b. PESTLE Analysis

- Globalization makes it necessary to have secure systems and be proactive regarding cybersecurity threats.
- Essential that companies and governments invest in these cybersecurity tools.
- People are increasingly aware of the importance of cybersecurity.

- Open Source code so no acquisition cost for Inetum, however the cost of user customisation is high.

III.5.5.c. SWOT Analysis

- ProTego's SIEM has artificial intelligence.
- Configuration is complex, is continuously evolving.
- Numerous business opportunities (for cybersecurity tools) on the market.
- There are a multitude of SIEM platforms (from different manufacturers) on the market.

III.5.6. ProTego Toolkit Assembler

III.5.6.a. Market Analysis

The Toolkit has a remarkably high market volume, value and growth rates for containerisation. Containers and Kubernetes are in high demand and there are many companies which are willing to move to these and will require consulting services and the know-how.

Key success factors would include the implementation of experts in this field and what the cost to different businesses would be.

Competition from Kubernetes Certified Service Providers (KCSP) is already around two hundred companies, including the likes of Canonical, Microsoft, SAP and VMWare, and numerous SMEs.

Having a service from a smaller company as opposed to companies like Microsoft would be that you get a more personal service which is very appealing to many customers.

III.5.6.b. PESTLE Analysis

Kubernetes is the new trend; many organisations want to move to it. However, smaller companies may not be willing to invest or have the money to do so.

The Toolkit is of considerable utility. However, some companies may not want to spend.

Targeting companies which may have a smaller IT infrastructure or department and want experts to come in and design what meets their needs best could be the best strategy.

III.5.6.c. SWOT Analysis

There are a lot of companies that require help moving to the cloud and Kubernetes.

ICE have not provided these services yet so it might be hard to get involved, however with the proper infrastructure in place this should be achievable.

The market is there, we need to make sure that ICE have the consultancy side right to be able to compete with other companies offering similar services.

We will be offering an installation kit for Kubernetes as a quick way for customers to get started using the toolkit and as a way to know about our services and offering.

III.5.7. Network Performance & Privacy Slicing

III.5.7.a. Market Analysis

While many generic companies, health care providers and public administrations could all leverage ProTego’s network slicing, their interest is still low, wireless slicing may not be priority

for them yet. This makes the market volume, value and growth rate generally low. However, in those niches that require such strict slicing capabilities, the profitability is high.

The key success factor is in the cost-effectiveness. SMEs, hospitals, public administrations may only be interested in wired QoS policies and big IT companies, and data owners can achieve network slicing through cellular networks (e.g., 4G/5G) with much higher OPEX costs. In this sense, by providing effective network slicing capabilities at lower prices would make the asset competitive.

III.5.7.b. PESTLE Analysis

The cost of implementing network slicing is negligible compared with infrastructure and operation. Only few COTS devices (e.g., access points and switches) are required. This contrasts with the high operational and infrastructure cost required by alternative 4G/5G-based solutions.

With the growing of new connected devices (IoT devices, smartphones, etc.), users may demand not only additional privacy in their communications but also guaranteed performance for their different flows.

Continuous evolution of technologies will require network slicing to be able to adapt to new algorithms, interfaces, and protocols without re-deploying the whole system.

III.5.7.c. SWOT Analysis

The ProTego network slicing solution provides performance and privacy isolation over standard, widely deployed Wi-Fi networks. This makes it very attractive for both public and private wireless local networks.

However, some (rather conservative) companies, hospitals or public administration may be more interested in wired networks.

While it is currently limited to only Wi-Fi, with no 4G/5G integration (which could be an issue when seamless connectivity is needed), it is however much cheaper than their competitors 4G/5G Femtocells.

III.5.8. Cybersecurity Awareness

III.5.8.a. Market Analysis

Cybersecurity awareness services are oriented to a low growth and high-volume market, represented by the healthcare organizations. With an increasing market need motivated by the latest regulations (mainly GDPR) that demand due diligence in the appliance of organizational and technical measures to mitigate cyber-risks. Our cybersecurity awareness services are especially aimed at supporting the organizational measures.

Competition exists as there are private organizations offering such services, but they usually fail on a key success factor: the engagement of clinical managers to avoid the view that cybersecurity is only a technical issue.

This success factor has been addressed in the cybersecurity awareness program developed in ProTego with positive results.

III.5.8.b. PESTLE Analysis

The improvement of healthcare services through digitalization is yet a reality. This trend is bringing new tools to cope with health data and allowing the patient empowerment, as they want to be involved in their healthcare processes and even decide about the use of their data.

All the previous is widening the attack surface and institutions are regulating in order to keep the new services and tools safe from a cybersecurity point of view.

This offers a lot of room to grow for cybersecurity awareness services, in order to mitigate risks and potential impacts of an eventual cyber-attack, but to minimize the economical penalties to afford as well if such situation would ever occur.

III.5.8.c. SWOT Analysis

There is an increasing market need leaded by regulators and social trends.

The contents developed in ProTego are appropriate to be used all across the EU healthcare organizations.

The penetration of these cybersecurity awareness services requires real engagement of final users, that in case of health staff needs the participation of clinical managers, to remove the “IT issue” label surrounding cybersecurity.

III.6. Business Models and Financial Assessments

Based on the Market, PESTLE and SWOT analyses, which constitute a detailed analysis of the potential market opportunities, each asset owner has selected which business models will be exploited.

Each asset owner has then gone on undertake a financial assessment to determine which particular customer segments are the best for them to focus on for their chosen business model.

III.6.1. System Security Modeller

The business model is best described by the business model canvas reported in D8.2.

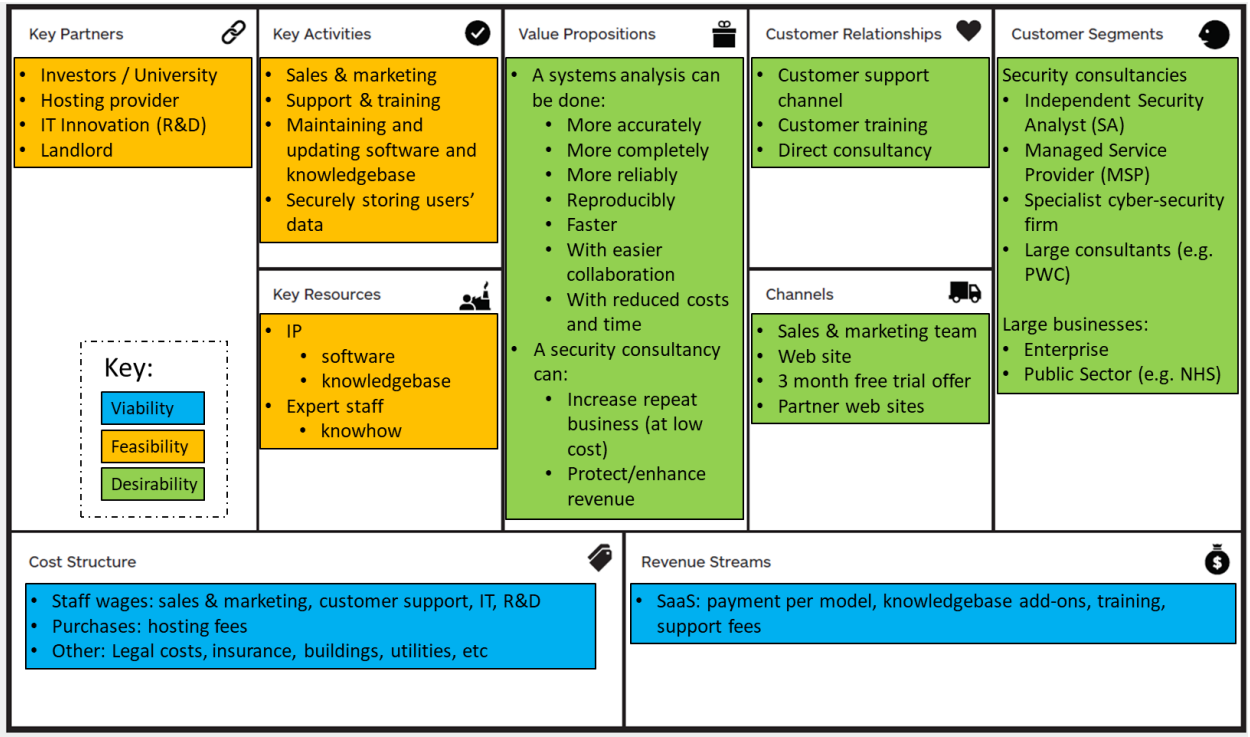

Figure 4 - SSM Business Model Canvas.

The SSM requires the user to have some cybersecurity expertise and so can either be provided directly to a larger enterprise with the expertise in-house (B2B) or can be provided in to a security consultancy which would use it to help them in their analysis of a customer (B2C).

Without further market validation it is unclear precisely what the best initial direction for the SSM is and what investment will be needed. Some seed funding will be necessary.

III.6.2. Apache Parquet Modular Encryption

In addition to releasing Parquet Modular Encryption to the open-source community, IBM has already been exploiting this technology as part of the IBM Analytics Engine and IBM Cloud Pak for Data products.

III.6.3. Continuous Authentication System

The Continuous Authentication solution developed by UAH in ProTego will offer the possibility of further research and industry projects. On one hand, the accuracy and detection rate of any Continuous Authentication system can be improved, leaving ways for further research in this aspect. On the other hand the creation of a Continuous Authentication system can motivate the creation of a spin-off company inside the university ecosystem.

UAH, as a university and research centre, is interested in further Continuous Authentication developments motivated by two possibilities and also the current increase of mobile devices.

However, the UAH's research team considers that the Continuous Authentication component is not mature enough for commercial exploitation in its current form for all the segments identified. Several needs must be addressed and improved, like further tests in different market devices and the improvement of detection and speed rates offered by the current approach.

UAH will pursue additional public and private research sources, including the following.

- Public calls for research and innovation projects (local, national and international).
- Private sponsorships and other forms of patronage, including the possible creation of a spin-off for external financing.
- Internal university resources.

III.6.4. Key Management & Access Control System

The exploitation strategy of KU Leuven – COSIC is to start new research projects on cybersecurity and cryptography in order to continue the research activities related to these topics and further expand our expertise. Starting new research projects requires funding to pay the researchers that are performing the research activities, as well as the direct and indirect costs related to these activities (e.g., consumables, test setups, etc.). These need to be covered by the incomes gather from new research project, both bilateral and funded projects.

The ambition is to have an organic growth in the domain of key management and cryptographic protocols for authentication and access control and have 3-4 researchers working solely on this topic. This is expected to be a heterogeneous team consisting of junior and more senior researchers. To cover the costs of the research projects, i.e. staffing and direct costs, one would need an active pool of about 2-3 funded projects on key management, authentication and access control, each of the projects with a mid-size budget. Strictly speaking, bilateral projects would not be needed. However, it gives a financial buffer, allows for more direct costs (e.g. consumables for lab experiments) and potentially even expanding the key management and access control team beyond 3-4 researchers.

.

III.6.5. Security Information & Event Management

The business models defined for SIEM are as shown in the following figure.

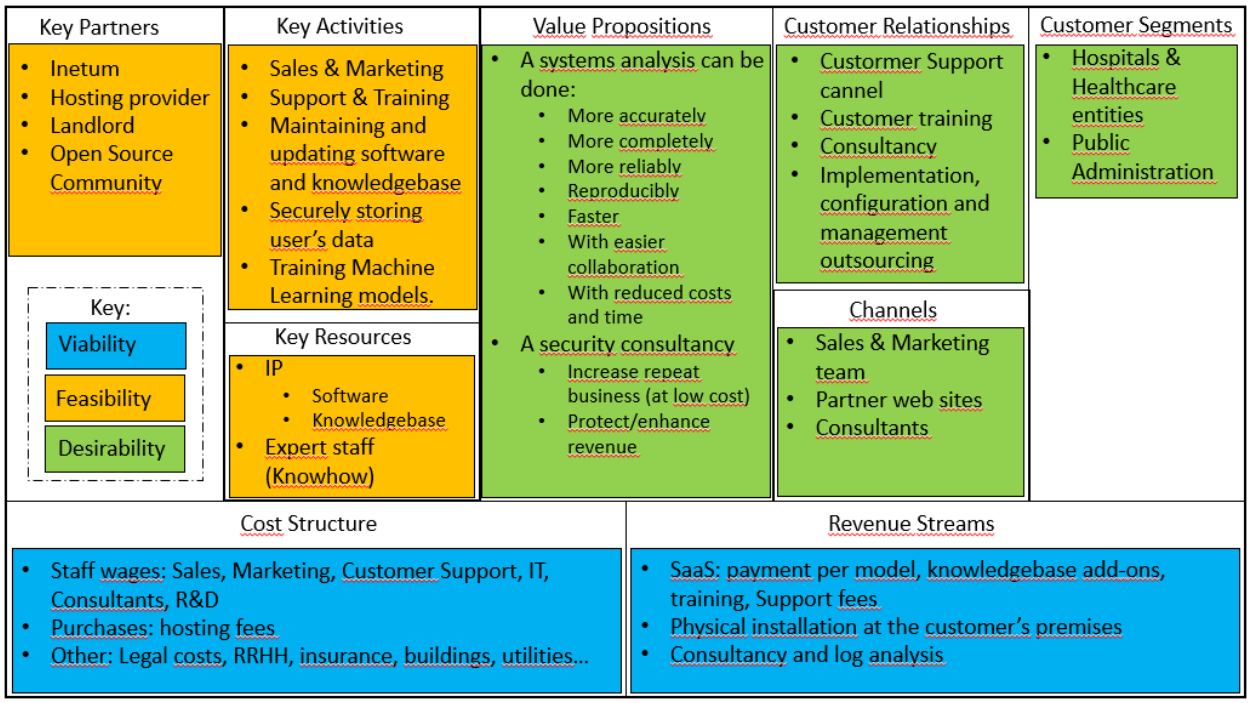

Figure 5 - SIEM Business Model Canvas.

From the beginning of the project, Inetum was strongly interested in analysing the commercial possibilities of ProTego results.

As global ICT provider, the idea of developing a new cybersecurity product related with cybersecurity in Hospitals and Care Centres was always considered, as the company found that the market opportunities in the sector were very promising (which has in fact been evaluated and confirmed during the execution of the project).

Hence, Inetum is interested in commercializing ProTego's results, relying on collaboration with ProTego partners.

At Group level (approx. 27.000 consultants, 26 countries - https://www.inetum.com.es/en/index.html), there are 2 main business units involved in the project results exploitation (BU Health and BU Cybersecurity). In fact, Inetum has already incorporated to their offering portfolio the ProTego results, both in terms of technical results and knowledge.

Figure 6 - Inetum overview

Inetum plans to capitalize on the technology developed and the knowledge acquired in the project by two sectors:

- Product
    - Open Source Strategy – Licensing and tool use (SIEM – Security Information and Event Management)
    - Commercialization of premium SIEM Components
        - Machine Learning module.
        - Integration with SSM.
        - Integration with other ProTego modules (Data Gateway, continuous authentication….)

- Consulting services in the Cybersecurity and Health area. Applying and putting into practice all the knowledge and experience acquired in the ProTego project.
    - Previous diagnosis of the situation
    - Analysis
    - Implementation and execution of the proposed measures
    - Evaluation

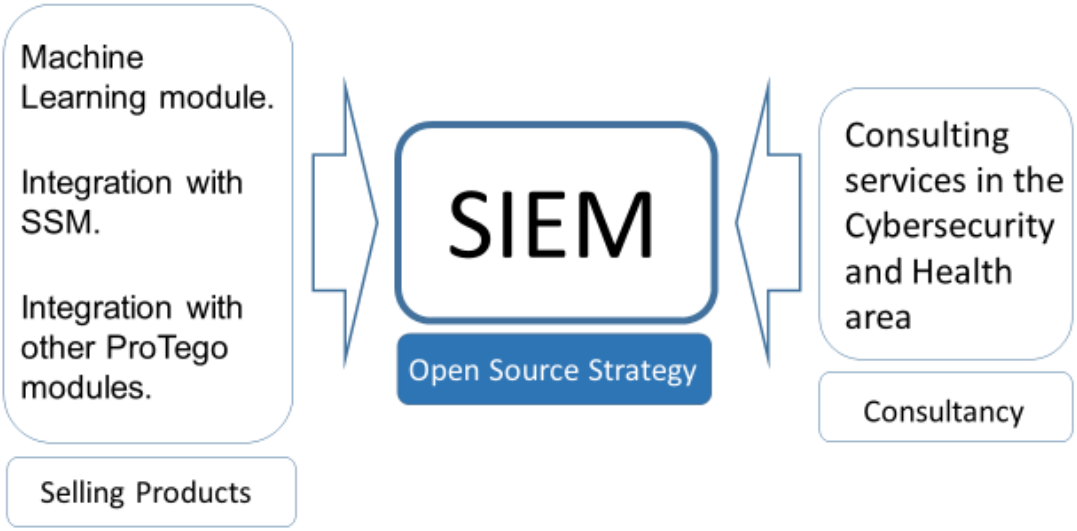

Figure 7 - SIEM strategy

After the ProTego project, Inetum will add the resulting network outage solution in ProTego to its portfolio of expertise in the secure healthcare ecosystem. Initially, Inetum will invest efforts, both technical and commercial, to reach agreements with industrial clients in the eHealth sector.

III.6.6. ProTego Toolkit Assembler

ICE will be providing consulting, customer support and training services and we have identified 4 possibilities that companies would need.

- Training - providing customers with specific training to meet the needs of their business.
- Specific consultancy - identifying how the customers will use the toolkit and doing the design work for them. This would include tailoring to the customers' needs and their specific business. Following our consultancy work, their own IT departments would take over installing and using the platform.
- Installation and providing consultancy - tailoring the installation to the customers' needs and their specific business and installing it for them, and providing related consultancy services.
- Providing ongoing support - some customers especially SMEs do not have IT departments to provide ongoing support so this is a service that will be needed by many.

Customer support, consultancy and training will be at the heart of the business plan.

III.6.7. Network Performance & Privacy Slicing

The network slicing solution demonstrated in ProTego will help IMEC to set up future projects with industry. This asset could be exploited by either a spin-off company (boosted through IMECs Incubation & Entrepreneurship programs) or through organic growth. The activities that would provide revenue would specially focus on validation, feasibility testing and rapid prototyping of our network slicing solution for the different interested entities.

IMEC, as a world-leading independent research centre in nano-electronics and digital technology, is interested in further applying the ProTego results, as its main goal is to bridge the gap between fundamental research at universities and technological development in industry.

At global level, (with presence in Belgium, Netherlands, Taiwan, USA, China, India and Japan, and staffing more than 3500 people), IMEC leverages its world-class infrastructure and its ecosystem of partners across a multitude of industries to create innovation in different application domains, including healthcare. Thus ProTego is completely aligned with the interest and expertise of IMEC.

IMEC plans to capitalize on the ProTego results on network slicing through providing added services to the tool, rather than through licensing. This means that the IMEC solution would not be commercialized directly. Instead, it will be released as open source.

However additional revenue can be generated through on-demand consultancy, this includes, support and training services, implementation of extra customized features and assistance in integration, testing and rapid prototyping for the specific requirements of the interested industry/government partner.

After the ProTego project, IMEC will add the network slicing solution resulted in ProTego to its portfolio of expertise on the secured health ecosystem. Initially IMEC would invest efforts, both technical and commercial, to reach agreements with industrial customers in the eHealth sector. Once a certain number of agreements has been achieved (e.g., with budgets larger than 1M euro in 2 years) and actual interest of the market on IMEC's network slicing solution has been demonstrated, IMEC would try to further exploit the solution through a spin-off, boosting it through IMECs Incubation & Entrepreneurship programs, or other external incubation funding programs.

III.7. Open Source Strategy

Open Source strategies are an important part of the ProTego exploitation framework. However, the framework does not preclude other models of software licensing (e.g. SaaS, proprietary), especially if this helps exploitation.

The drivers of open source include:

- optimizing the cost of an ICT solution;
- fostering the extensive reusability of code;
- democratizing access to essential and basic software for everyone, by removing barriers to access technology, empowering people;
- speeding up ICT innovation by allowing others to build up on prior work (this is very similar to the process of science, where researchers base their work on earlier findings);
- sharing knowledge and practices to speed up software development;
- fostering interoperability by using standard and open technologies (when more and more software systems are built on many different technologies); and
- building a successful business by offering services based on Open Source software, often including a freemium strategy in which software with enhanced functionality is made available under a paid-for licence.

It should be noted that using open source does not necessarily come without cost, it is not always free, and it does not always fit into all business models. The license terms must be followed, and it may not fit completely to all needs.

With open source, choices for support include building up know-how internally, contracting a third party, or relying on an active community.

ProTego exploitable assets will utilise a variety of licensing strategies, as set out in the following sections. In each case we explain how Open Source licensing is being used and why, or why it was rejected.

III.7.1. System Security Modeller

The SSM is closed-source and is in the process of being licensed by the University of Southampton to SPYDERISK Ltd. (a spin-out company). SPYDERISK Ltd. will then be in a position to develop, market and support the SSM in healthcare and other sectors as appropriate, may pursue a partnership with Inetum around the SIEM integration, and will also be able to continue working with the University of Southampton in further collaborative research projects. Open sourcing the software is not compatible with the SPYDERISK Ltd. commercialisation strategy as protection of the IP is a vital competitive advantage.

III.7.2. Apache Parquet Modular Encryption

As previously noted, IBM's Parquet Modular Encryption has been officially adopted by Apache, and is part of Apache Spark, released by Apache under the Apache Open Source License.

In addition, Fybrik [8], which is the advanced topic that IBM have been working on this year, is also being released as Open Source under an Apache v2.0 license.

III.7.3. Continous Authentication System

UAH's objective is to facilitate the development and introduction of new generations of technologies. Therefore it is planned to release the code of the Continuous Authentication solution in 2022 under the Apache License, version 2.0.

III.7.4. Key Management & Access Control System

The exploitation strategy of KU Leuven – COSIC is to start new research projects on cybersecurity and cryptography in order to continue the research activities related to these topics and further expand our expertise. Therefore the ProTego research outcomes themselves are a means to increase the chances to acquire new projects. The software developed in this project should therefore also be seen as a sort of 'research publication'. To increase the visibility, the code for the key management and access control framework will be open source. Moreover, this code has been developed in the ProTego project specifically to be combined with the data gateway. Therefore, it will use the same Open Source license model as the open source code for the data gateway.

The access control framework developed within ProTego will be released under a BSD license. The reason is that the access control code is solely used to increase the visibility of KU Leuven's research work on this topic, i.e. similarly as a research publication. Therefore, there is no need for more restrictive open-source licenses. Moreover, there are also no dependencies on external open-source components that would require the use of other open-source license models.

III.7.5. Security Information & Event Management

The SIEM will utilise the freemium approach. Inetum will offer services based on the open source or 'Lite' version and premium services alongside the enhanced paid-for 'Premium' version.

The Open-Source projects being used in the 'Lite' version and their licenses are as follows.

- OpenSearch - Apache 2.0.
- Logstash and Beats - Apache 2.0.
- Wazuh - GNU GPLv2.
- GVM - GNU GPLv2, ODbLv1, AGPLv3, PostgreSQL.
- Kafka - Apache 2.0.

The ‘Premium’ version will include the components that have been developed by Inetum specifically those that connect with the SSM and the Machine Learning tasks.

III.7.6. ProTego Toolkit Assembler

All of the software is open source. The components of the ProTego Toolkit are bundled, not modified, and thus retain whatever licences have been imposed by the copyright owner. Regarding containers, we are distributing unmodified binaries, and the same applies [8].

III.7.7. Network Performance & Privacy Slicing

The ProTego network slicing tool will be released as open source, maintaining the open-source licenses of its components (GPLv3, Apache-2 license and an MIT license plus a clause taken from the W3C license).

III.8. Information Campaign

III.8.1. Background

From the outset the project had planned an Information Campaign as a key part of the Exploitation Framework. This was to have been centred around inviting stakeholders to pilot events and other scheduled project demos, and Partners participating in relevant industry and academic events, variously giving demos on booths, talks, presenting papers and showing posters to further their exploitation strategies.

Due to the COVID-19 pandemic, little of this has been possible (see D8.7 for a report of the virtual events at which partners have disseminated ProTego). Therefore we have had to think outside of the box.

III.8.2. Horizon Results Booster

We explored using the services of the Horizon Results Booster [10], in the hope that they could avail us of some experience of facilitating exploitation actions in the conditions of the pandemic.

The Horizon Results Booster is a new initiative backed by the European Commission which aims to maximise the impact of research projects funded by FP7, Horizon 2020 and HE. The Horizon Results Booster consortium offers three services:

- Portfolio Dissemination & Exploitation Strategy,
- Business Plan Development, and
- Go To Market.

Services can be requested "à la carte”. We considered the service offers carefully and concluded that elements of the first and third could be relevant. However, during email exchanges with the Booster it became apparent that their offers and rules of engagement were much more arcane than we had understood from their published material, and that there was no service which could include an information campaign and no advice or support that they could offer us.

III.8.3. Campaign Strategy

The information Campaign strategy we devised in concert with the ProTego dissemination actions was to make a short video discussing the main innovations delivered by the project, and why this is helpful for hospitals and healthcare. It will also contain some interviews with staff in the ProTego

hospital partners. We will use this video in social media campaigns, in virtual events, and in virtual meetings between individual partners and potential customers.

The video is backed up by a number of White Papers [12] giving the next level of detailed information about the main innovations delivered by the project:

- ProTego Cybersecurity Educational Framework for healthcare organizations,
- ProTego Cybersecurity Risk Mitigation Tools for Hospital and Care Centers,
- Creating a SIEM with the Elastic Stack or with Open Search,
- Autenticación Continua (in Spanish),
- ProTego-ACC: Access control and key management for healthcare systems, and
- The ProTego Integration Toolkit – A Kubernetes Journey.

As well as being valuable collateral material to follow up on virtual meetings, these White Papers will be equally useful when we emerge from the pandemic and are able to promote the ProTego results at physical events and meetings.

IV. SUSTAINABILITY PLAN

Section III (Exploitation Actions) described the plans from partners towards ProTego results once the project is finished. In summary there are different approaches for exploiting the project results depending on partners' nature, mainly:

- Commercial exploitation
    - Solutions and services
    - Consulting
- Scientific / Research Purposes including R&D projects that support the further evolution of project results
- Academic Teaching

Currently the ProTego platform is hosted in cloud infrastructure, Kimsufi provider, under the following setup:

The four servers make up the virtualization environment that supports the following infrastructure:

- Centralized Authentication Service
- VPN Service
- Several VMs for development, testing, and demos
- A private GitLab Environment
- A Kubernetes cluster for development
- A Kubernetes cluster for integration, testing, and demos

The current contract was created by ProTego as coordinator of the project, with a cost of 89.96€/month:

- One server (ns301299.ip-94-23-49.eu): 24.99 €/m
- One server (ns3046222.ip-188-165-238.eu): 19.99 €/m
- One server (ns360877.ip-91-121-165.eu): 24.99 €/m
- One server (ns365958.ip-95-23-7.eu): 19.99 €/m

From 1 January 2022 Inetum will take over the cost of the hosting of the integration environment, keeping the platform running and available for all partners for at least 6 months (June 2022).

Regarding the tools that support ProTego, Inetum will continue supporting SharePoint (including project results description, publications, deliverables, etc) and the source code and KU-Leuven the project website both in internal servers. It will remain active and available for at least one year after the end of the project.

V. CONCLUSIONS

The ProTego project has delivered numerous innovations to help reduce cybersecurity risks in hospitals and healthcare. Eight exploitable assets have been identified and their exploitation potential has been analysed considering a wide range of customer segments, including hospitals and healthcare and many others. Business models and their financial basis have been considered in depth, together with open-source strategies. This has led to the selection of the most appropriate business model in each case. The final exploitation action in the project has been to devise an information campaign based on materials appropriate for use during the COVID-19 pandemic and beyond. The sustainability plan underpins our ability to deliver the information campaign and achieve wide-ranging high-impact exploitation.

VI. REFERENCES

[1] https://en.wikipedia.org/wiki/Market_analysis

[2] http://www.netmba.com/marketing/market/analysis/

[3] https://pestleanalysis.com/what-is-market-analysis/

[4] https://pestleanalysis.com/market-analysis-example/

[5] https://pestleanalysis.com/what-is-pestle-analysis/

[6] https://www.grandviewresearch.com/industry-analysis/enterprise-governance-risk-compliance-egrc-market

[7] https://www.iso.org/the-iso-survey.html

[8] https://github.com/fybrik/fybrik/

[9] Hemel, A. Docker Containers for Legal Professionals. The Linux Foundation. Available at https://www.linuxfoundation.org/wp-content/uploads/Docker-Containers-for-Legal-Professionals-Whitepaper_042420.pdf

[10] https://www.horizonresultsbooster.eu/

[11] https://protego-project.eu/white-papers/

[12] https://zenodo.org/communities/protego/


ProTego