Ref. Ares(2019)7931732 - 30/12/2019

Horizon 2020 Programme

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

ProTego

DATA-PROTECTION TOOLKIT REDUCING RISKS IN HOSPITALS AND CARE CENTERS

Project Nº 826284

ProTego

D8.2 Initial market analysis and first standardization actions

Responsible:	ITInnov
Contributors:	Stephen C. Phillips, Mike Surridge, Kostas Kouvaris (IT Innov), María Perez Ortega, Antonio Jesús Gamito González (GFI), Eliot Salant (IBM), Carlos Cilleruelo (UAH), Dave Singelee (KUL), Salvador Garcia Torrens (MS), Arturo Arriaga, Philip Usher (ICE), Johann Marquez-Barja, Bart Lannoo (IMEC), Grassi Stefano Fabrizio (OSR)
Dissemination Level:	Public
Version:	1.0
Date:	31/12/2019

Executive Summary

The ProTego project partners have enumerated ten potentially exploitable assets, some proprietary, some based on open source components, and performed an initial analysis of the market opportunites following the Market Opportunity Navigator approach. This results in a strategy for each asset, varying from creating products for security consultancies or general cyber-security, writing research publications, applying the technologies developed to the healthcare sector, and taking developments into other sectors and further R&D projects.

Where appropriate at this stage, the analysis is continued to look at the value proposition and business model. Some standardization objectives and customer/user personas are also described.

This document, the first iteration, will be extended in the subsequent two exploitation deliverables as additional understanding is gained.

Contributors Table

DOCUMENT SECTION	AUTHOR(S)
I	Stephen C. Phillips, Mike Surridge, Kostas Kouvaris (IT Innov)
II, III	Stephen C. Phillips, Mike Surridge, Kostas Kouvaris (IT Innov), Eliot Salant (IBM), Carlos Cilleruelo (UAH), Dave Singelee (KUL), María Perez Ortega (GFI) Antonio Jesús Gamito González (GFI), Philip Usher (ICE), Johann Marquez-Barja, Bart Lannoo (imec)
IV, V	Stephen C. Phillips, Mike Surridge, Kostas Kouvaris (IT Innov), Grassi Stefano Fabrizio (OSR)
VI	Eliot Salant (IBM)
VII	Salvador Garcia Torrens (MS)
VIII IX	Stephen C. Phillips (IT Innov)

Table of Contents

I. INTRODUCTION 6
II. EXPLOITABLE ASSETS 7
III. MARKET OPPORTUNITIES 9
III.1. System Security Modeller 9
III.2. Apache Parquet Modular Encryption 11
III.3. Continuous Authentication System 12
III.4. Key Management and Access Control System 13
III.5. Security Information and Event Management (SIEM) 15
III.6. ProTego Toolkit Assembler 18
III.7. Network Performance and Privacy slicing 19
III.8. User Requirements Elicitation Service 20
IV. VALUE PROPOSITIONS 22
IV.1. System Security Modeller 22
V. BUSINESS MODELS 23
V.1. System Security Modeller 23
V.2. Requirement Elicitation Service 24
VI. STANDARDISATION 26
VII. PERSONAS 27
VIII. CONCLUSIONS 29
IX. ACKNOWLEGEMENTS 30
X. REFERENCES AND INTERNET LINKS 31

Table of Figures

Figure 1. Market attractiveness map for the SSM. 11
Figure 2 Value proposition of System Security Modeller 22
Figure 3 Business model canvas of System Security Modeller 23
Figure 4 Business model canvas of Requirement Elicitation Service 25

List of Tables

Table 1. Exploitable Assets 7

Table of Acronyms and Definitions

Acronym	Definition
KMS	Key Management Systems
SIEM	Security Information and Event Management
QoS	Quality of Service
LAN	Local Area Network
RFC	Request for Comment
SSM	Security Sistem Modeller
CPD	Continuing Professional Development
ISO	International Organization for Standardization
SME	Small and Medium Enterprises
MSP	Managed service providers
HL7	Heatlh Level Seven
FHIR	Fast Healthcare Interoperability Resources
BYOD	Bring your own device
IAM	Identity Access Management
R&D	Research and Development
ELK	Elasticsearch, Logstash and Kibana
IPR	Intellectual Property Rights
OS	Operating Systems

I. Introduction

This document is the first of three exploitation documents to be written over the course of the ProTego project:

- D8.2: Initial market analysis and first standardization actions
- D8.4: Initial description of the project impact and business models definition
- D8.6: Final exploitation framework: Project impact, exploitation actions and sustainability plan

Each document will extend the previous analysis where appropriate, developing he plans as the value of the assets, the state of the various markets and the appetites of the partners for different activities is explored.

The first step is to enumerate the exploitable assets owned or being developed by the project partners (see Section II). For each asset, we then follow (at most) two schemes:

1. The recently developed Market Opportunity Navigator [1].
2. Value Proposition and Business Model canvasses of Ostewalder [2].

The Market Opportunity Navigator is a tool for understanding “where to play”. If you have a potential product it provides a thinking tool to look at the different opportunities and determine which is the primary market opportunity (which you would then analyse in more detail) and which to hold in reserve in case the business needs to pivot. This analysis can be found for all assets in Section III.

Osterwalder’s Value Proposition and Business Model canvasses are well-accepted tools for the next stage of analysis and help create an understanding of whether there is a genuine need for a product and how a business can be constructed to support it. Most of ProTego’s assets are not yet at the stage of being ready for a detailed analysis and some partners’ preferred route is an academic one of writing publications which does not directly fit with the Value Proposition and Business Model tools. Those assets that may already be analysed in this way are presented in Sections IV and V.

A route to enhance a product’s market value is standardization and this is explored in Section VI. In later documents we expect to add in further information analyzing chosen markets and any other environmental factors (e.g. regulation) which may have an impact on any of the exploitation opportunities but these are not presented in this first iteration.

Finally, to help in the analysis of opportunities we present some Personas of some of the people who would interact with some of the exploitable assets in Section VII.

II. Exploitable Assets

The following table lists the individual assets which the consortium thinks has the potential to be exploited, and summarises the intellectual property ownership and constraints for each.

Table 1. Exploitable Assets

Partner: Asset	Licence	Patent	Constraints
IT Innovation: System Security Modeller	Current: proprietary Future: proprietary	None	None
IBM: Apache Parquet Modular Encryption	Apache 2.0		IBM is driving the standard for Apache Parquet Modular Encryption. The implementation of this code is being carried out by IBM and the Open Source Parquet community, and will be distributed by Apache Foundation.
UAH: Continuous Authentication System	Current: proprietary Future: proprietary	None	None
KU Leuven: Key Management System (KMS)	Current: Vault by Hashicorp Future: proprietary	None	The current KMS system is not developed by KU Leuven, but an open source component (Vault) developed by Hashicorp. Future versions of the KMS in ProTego might be integrated with the access control system.
KU Leuven: Access Control System	Current: Apache Future: proprietary	None	Current version is based on Apache Tapestry and hence open source.
GFI INFORMATICA: Security Information and Event Management (SIEM)	Current: Based on Elasticsearch and Wazuh Future: proprietary	None	Current version is based on Elasticsearch and Wazuh and hence open source. Future versions of SIEM in ProTego will include machine learning and integration with all ProTego components.
ICE: ProTego Toolkit Assembling	Apache License 2.0	None	ICE ProTego Toolkit Assembling platform is an integrated set of open source tools such as Rancher, Istio, Kubernetes, docker. Provide end-to-end development-deployment support to DevOp teams.
IMEC: Network Performance slicing	Current: Based on 5GEmpower which is released under Apache License 2.0 Future: propietary	None	The current network slicing in charge of the keeping the QoS guaranteed including radio Wi-Fi slicing (performance isolation) is based on the 5GEmpower system. The main components of the network performance slicing are mainly placed and distributed along the local network components (switches and access points).

IMEC: Network Privacy slicing	Current: Based on OpenvSwitch which is Apache License 2.0 Future: propietary	None	Regarding the privacy isolation within the networks slices, the current system is based on VxLAN techniques (RFC 7348), in particular based on OpenvSwitch under Apache License 2.0The network privacy slicing solution is deployed in both local network and cloud component, isolating the traffic within the slices that goes within the local network towards the cloud.
OSR: user requirements elicitation service	None	None	None

III. Market Opportunities

For each asset we follow the approach of the Market Opportunity Navigator and:

- describe the core capabilities;
- consider how those capabilities could be used to create a product in a market;
- for each potential market evaluate the challenge and potential;
- determined an exploitation strategy based on this.

The extent of the analysis varies depending on the maturity of the asset.

III.1. System Security Modeller

The System Security Modeller (SSM) provides a web-based interface for modelling systems (constructing a diagram of assets and their relationships), finding threats to the system and calculating their risks. The user interface builds on an underlying knowledgebase which encodes the particular asset types, permitted relationships, threats and controls. The knowledgebase is adaptable to different domains but the most advanced knowledgebases (and that used in ProTego) contain IT assets and model cyber-security threats.

The core abilities of the software and knowledgebase are:

- Modelling socio-technical assets connected by defined relationships
- Finding cyber-security threats to the assets along with related controls
- Calculating threat likelihood
- Calculating risks
- Supporting the ISO 27005 process
- Presenting data from the model in a variety of reporting formats

III.1.1. Applications and Customers

Given the core capabilities described above, there are a variety of potential applications and customers. They fall into two broad categories: using the SSM for education/training and using it for actually modelling a system to find threats and risk.

For education, this could be at a University level or as part of a CPD course.

There are various scenarios where the SSM could be used for modelling real systems:

- Security consultancies using the SSM to help their customers.
- Large companies who have cyber-security expertise in-house using the SSM directly on their own system.
- SMEs (who do not have cyber-security expertise) using the SSM directly on their own system.
- Managed Service Providers who provide IT services to their customers using the SSM to provide an enhanced secure service to their customers.
- We could set up a new cyber-security consulting firm, using the SSM as our own special tool to out-compete others.

Within this non-educational sector, the application of the SSM can be further segmented. For instance, the SSM can be used to analyse existing systems or systems under design. It can be used to find threats to improve security or to help with compliance activities such as ISO 27001 where documenting the situation is key rather than actually fixing all the issues.

III.1.2. Market Potential Attractiveness

We have evaluated the potential markets described above in terms of "challenge" as follows:

- Security consultancies and large business have the necessary expertise to use the tool so they are low challenge.
- SMEs do not have the expertise so further research would be required to simplify the interface and process to make the SSM usable by these non-expert users, hence high challenge.
- Managed service providers (MSP) may have some security expertise so mid-challenge.
- Adapting the SSM for education/training would require investment in additional training materials to wrap-around the tool, so mid-challenge.

In terms of "potential" we think:

- There are many existing security consultancies and they could really be helped by the SSM so high potential.
- Large businesses offer a more difficult market to enter, so mid potential.
- There are a great many SMEs but they do not have much money to spend on cyber-security so mid to high potential.
- It's not clear that the MSP market is a good fit and the volume and price would be low so mid potential.
- Education and training does not make a lot of money so low potential.
- Setting up a new cyber-security consultancy is low potential because it cannot scale.

These thoughts are summarized in Figure 1.

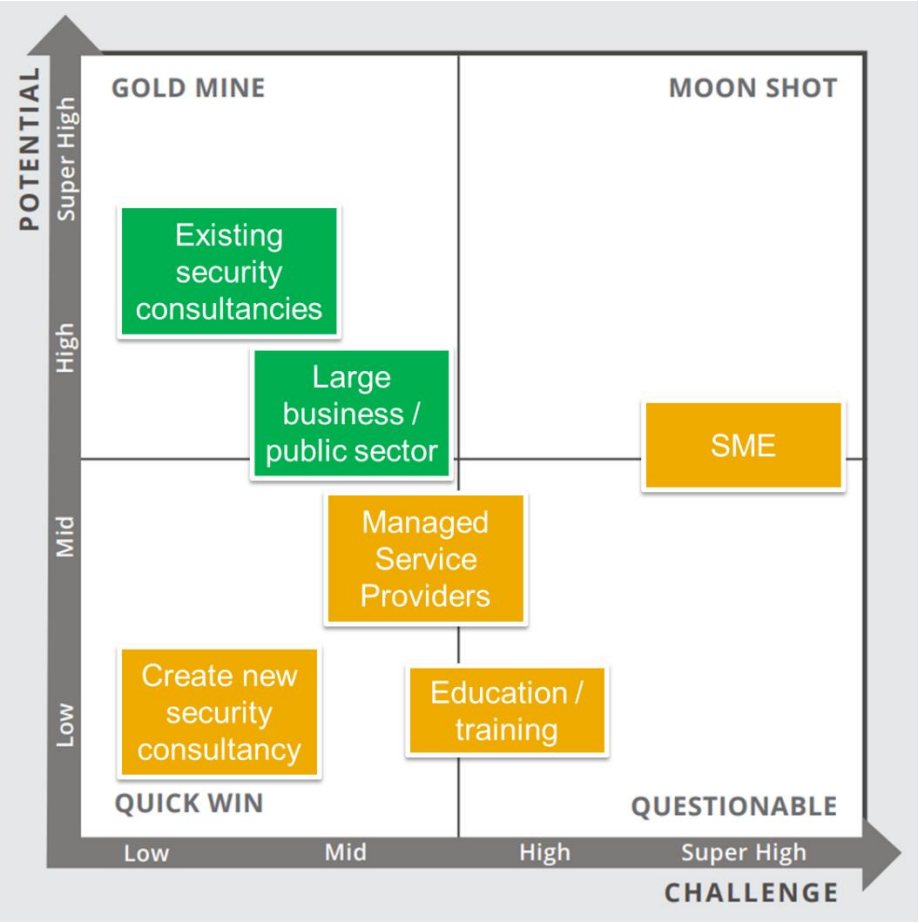

Figure 1. Market attractiveness map for the SSM.

III.1.3. Strategy

Given the market attractiveness described in the preceding section, our strategy for commercialization is first to target security consultancies (of all sizes). A back-up option is direct sales to large business. The application of the SSM will primarily be for assisting with ISO 27001 certification.

III.2. Apache Parquet Modular Encryption

IBM is leading the definition of modular encryption for Apache Parquet files and will continue to be a driving force in its development. Parquet is the format most widely used today in big data analytics, and the addition of encryption to Parquet files will allow for secure storage of sensitive data in public clouds, as well as extra security from external hackers or insider attacks in private clouds.

Modular Parquet encryption allows for the protection of stored data files from unauthorized access, as well as guarantees against tampering of encrypted data. Parquet is a highly efficient format which allows for columnar access of data, predicate push down, and data compression – all of which make it ideal for big data analytics. Parquet is being used today by all major technology companies, and the addition of encryption stands to only strengthen its attractiveness in the world of cloud computing.

Encrypted Parquet integrates with the Apache Spark analytics engine without requiring any changes in Spark code.

III.2.1. Applications and Customers

In ProTego, we are highlighting how Parquet encryption can be used in in our health care use cases, and in particular, looking at the integration of support for Parquet files for big data with the

emerging HL7 FHIR standard for the exchange of medical data. This will serve two purposes in the healthcare world – not only will it supply security for sensitive medical data-at-rest, but it will also allow for an efficient way of providing analytics on the stored data, such as might be done for medical studies.

While the storage (and potentially, transfer) of FHIR data in Parquet format is specific to the world of healthcare, ProTego's core work on Parquet encryption is applicable to a wide range of fields and applications and is expected to be adopted by a wide range of commercial sectors.

III.2.2. Market Potential Attractiveness

Keeping sensitive data-at-rest encrypted is crucial not only for securing low-cost storage in the cloud, but to also prevent data leakage or theft from insider attacks for on-prem storage. Additionally, Parquet encryption can detect when data files have been tampered with – which guarantees the integrity of the original data. Coupled with its very low impact on performance, virtually any application which uses big data can benefit from the use of Parquet encryption.

Additionally, Apache Parquet is open source, and already has a broad support base in industry. We expect this only to increase with the implementation of Parquet encryption as part of the official Apache release.

The IBM-led Parquet encryption format has already been accepted as a standard by the Apache Parquet community and has recently been announced as an offering as part of the IBM Analytics Engine. [1]

III.2.3. Strategy

ProTego is exploring ways that encrypted Parquet can be brought into the world of health care as a means for not only expanding its influence, but also to bring genuine benefit in terms of increased security for sensitive medical data. With two use cases being provided by hospitals, ProTego will be developing reference solutions for integrating the storage and access of medical data in Parquet format with the emerging HL7 FHIR standard for the exchange of medical data. In particular, using an open source, commercial FHIR server, we will show how encrypted Parquet can be used for backend storage, not only increasing the security and privacy of the data, but also show how the data can now be more efficiently used for big data analytics.

Additionally, ProTego will research methods for authentication along with key management and distribution as part of an overarching solution (see Section III.4.).

III.3. Continuous Authentication System

University of Alcalá (UAH) is developing new methods of continuous authentication. These new methods could allow the detection of a device used by an unauthorized user. Someone could steal and use a mobile phone or use an unlocked computer. UAH is developing and designing algorithms that use behavioral biometrics in order to continuously authenticate users.

In ProTego, UAH are focusing in BYOD (Bring your own device) security problems. Hospitals allow doctors and patients to connect to Hospital networks using their mobile phones. Also, numerous mobile apps centered in health care are being developed and used on mobile phones. In order to offer continuous authentication and protection services, UAH is developing an app that incorporates these functionalities.

Core abilities and technological elements of the continuous authentication system:

- Identify the user based on behavior and not passwords
- Early detection of stolen devices
- Detecting threats and security incidents
- Force security responses if a security incident is detected

- Reporting alerts to the SIEM

III.3.1. Applications and Customers

The continuous authentication system allows the protection and early detection of unauthorized access or usage of devices. Mobile devices usage is increasing, and they store a lot sensitive information. Furthermore, mobile devices contain critical mobile applications that hospitals are offering to their patients and doctors.

For these reasons, BYOD (Bring your own device) has become a problem for many companies. It is necessary to protect mobile devices, and continuous authentication could provide a new layer of security. Every company that needs to address mobile device security could be a potential client of continuous authentication.

III.3.2. Market Potential Attractiveness

Continuous authentication has already been proved useful for computers. There are several companies offering continuous authentications systems based on computer keyboards. Addressing the mobile market could provide a great attractiveness, because of the lack of competitors right now.

The goal is to achieve a working and reliable prototype that can offer continuous authentication to mobile devices.

III.3.3. Strategy

The University of Alcalá main goal is to perform research and produce research publications. The development of new continuous authentication techniques would allow our research group to opening new research paths. The default exploitation strategy is to publish the research outcomes, but we are also considering possible collaborations with final users.

We do not want to close any possible future opportunities, the advances in continuous authentication could give us:

1. The development of a prototype which proves the effectiveness of the algorithms and techniques developed in order to offer continuous authentication. This allow us to present and publish conference and scientific publications.
2. There are already products that are offering continuous authentication services. Most of them are focused in offering continuous authentication with computers. Our approximation is based in mobile devices, we are exploring a market that is not already fulfilled by a commercial solution. It is our ambition to create a prototype that could fill the mobile security necessities.

III.4. Key Management and Access Control System

KU Leuven is developing two components that need to be integrated with Parquet Modular Encryption to allow for the protection of stored data files from unauthorized access. In the current version, these are two separate components. However, the goal is to combine these two building blocks into a single component during the next development stages. Moreover, these components are particularly developed to be integrated with the Parquet Modular Encryption in the data gateway. Therefore, the ambition of ProTego is to design and develop an overarching solution that combines all these different functionalities.

The current version of the Key Management System (KMS) is not developed by KU Leuven. To allow for rapid prototyping of the other ProTego components, the consortium initially chose to use an open source solution available on the market: Vault (developed by Hashicorp). Obviously, this sole component from Hashicorp cannot be exploited on the market by any of the ProTego partners. However, as mentioned above, the research ambition is to enhance the access control solution such that key management functionality is implicitly embedded. Therefore, in the

subsequent (sub)sections, we will consider the key management and access control solution as a single exploitable asset.

Core abilities or technological elements of the KMS:

- Store encryption keys securely
- Deliver encryption keys to the Apache Parquet Modular Encryption (gateway) on demand

Core abilities or technological elements of the access control solution:

- Define security rules (i.e. security policies) in the system
- Enforce security rules (i.e. security policies)
- Determine if a particular user should be able to retrieve a particular data object; i.e. act as 'gatekeeper' of the data gateway.
- Access control decision is based on certain attributes of the user, attributes of the data object and security policies in place
- Reporting alerts to the SIEM
- Interaction with authentication system (to know the identity of the user) and the data gateway (where data objects are encrypted and decrypted by the Apache Parquet Modular Encryption).

III.4.1. Applications and Customers

A first important observation is that access control solutions are typically never sold on the market in isolation. Instead, companies typically sell IAM (identity and access management) products or services to their customers. These mostly combine multiple core functionalities:

- Identity management: creation, management and deletion of identities of users in the system
- Authentication: assessing claims of users regarding their identity
- Access control: assessing if a user (with particular identity and attributes) should get access to a digital resource or data object.

Most organizations and companies rely on IAM solutions to manage and protect their digital assets and resources.

There are already many mature and widely-used IAM solutions on the market. Therefore, it is definitely not our ambition to compete against these products and develop yet another IAM solution. Instead, we aim to develop a key management and access control module that is specifically targeted towards enhancing the data gateway and the encryption functionality it is running. Indeed, the goal is to develop a security component that can be used by the data gateway to decide if the result of a query on decrypted data files in Parquet format should be forwarded to the entity that launched the query (or even more, to decide whether the query should even be executed at all). In theory, this could be done with commercial IAM solutions on the market. However, we want to research more innovative solutions that can be easily integrated with Apache Parquet Modular Encryption and are hence more tailored towards the latter.

III.4.2. Market Potential Attractiveness

Due to the tight coupling between (1) Apache Parquet Modular Encryption and (2) the key management and access control solution developed in ProTego, one should mainly consider the market potential of the overarching solution (so Apache Modular Encryption enriched with key management and access control functionality), and not the isolated key management and access control component on its own. The true market potential attractiveness can be found in an integrated solution that combines secure external encrypted storage of sensitive data with fine-grained IAM functionality. This combination, which is realized in the ProTego project in a data gateway, allows one to control who gets access to which data, and ensures that one cannot get

access to the plaintext data by bypassing the data gateway. One could envision multiple applications of such an integrated component. Healthcare is one of the most prominent applications, but one could use similar functionality in IoT applications where sensitive data needs to be stored and exchanged.

One of the challenges of putting an integrated solution for secure data storage, exchange and access control on the market is the integration with other components in the system. In this respect, the Apache Parquet Modular Encryption is important here, as Apache Parquet is open source, and has a broad support base in industry.

III.4.3. Strategy

First of all, as an academic partner, our main outcome are research publications. This does not only strengthen our scientific expertise, but indirectly also strengthens our valorization potential. Scientific research papers are a good approach to demonstrate our knowledge and competences in specific domains and enable future R&D collaborations with industry and other research partners. Therefore, unless there is a very clear and promising market potential, the default exploitation strategy is to publish the research outcomes and engage in research collaborations with industry on local and international level.

This default exploitation strategy is also the most preferred one for the key management and access control solutions that will be developed in the ProTego project. The reason is twofold:

1. There are already many IAM solutions on the market. It would be very challenging to compete against these products, unless a unique value proposition would be offered. Although our goal is to deliver an innovative and novel key management and access control solution for healthcare applications within ProTego, customers typically demand an integrated solution that does not only offer access control, but also many other functionalities. Extending our access control component to such an integrated IAM solution would require significant resources and is beyond our ambition.
2. Even more important, the goal is to develop an access control component – with key management embedded – that is particularly tailored towards the Apache Parquet Modular Encryption. This is the most important novelty. Most likely, it will be possible to generalize the research outcomes and integrate it with other encryption schemes. But even then, the isolated access control component itself has little value, the main strength and innovation is the overarching solution that combines encryption with access control and key management.

III.5. Security Information and Event Management (SIEM)

GFI is developing a SIEM (Security Information and Events Management) that allows monitoring, not just the security of IT infrastructures in general, but also the specific security events that are detected by the rest of the components of the toolkit, to be precise the Cybersecurity Risk Mitigation Tools. This provides an integrated security perspective as a whole.

In addition, the integration with other Cybersecurity Risk Assessment Tools, such as the SSM (System Security Modeller), through mutual feedback between them, allows a continuous update of current risks. And what's more the SIEM intends to be a security analytics platform that can be used with machine learning techniques over the security big data collected, giving the possibility of detecting complex attacks and in some cases even predict them.

In Cybersecurity environments, the SIEM tools is widely used (in this link [1] shows the Top 10 SIEM Cybersecurity Software Tools and Companies for 2019).

SIEM has become a core security component of modern organizations. The main reason is that every user or tracker leaves behind a virtual trail in a network's log data. SIEM systems are designed to use this log data in order to generate insight into past attacks and events. A SIEM

system not only identifies that an attack has happened but allows you to see how and why it happened as well.

As organizations update and upscale to increasingly complex IT infrastructures, SIEM has become even more important in recent years. Contrary to popular belief, firewalls and antivirus packages are not enough to protect a network in its entirety. Zero-day attacks can still penetrate a system's defences even with these security measures in place.

SIEM addresses this problem by detecting attack activity and assessing it against past behaviour on the network. A SIEM system has the ability to distinguish between legitimate use and a malicious attack. This helps to increase a system's incident protection and avoid damage to systems and virtual property.

The use of SIEM also helps companies to comply with a variety of industry cyber management regulations. Log management is the industry standard method of auditing activity on an IT network. SIEM systems provide the best way to meet this regulatory requirement and provide transparency over logs in order to generate clear insights and improvements.

The SIEM included in the ProTego project is based on the Open Source platform Elasticsearch [2]. This is composed of the entire suite of ELK components (Elasticsearch, Logstash and Kibana). In addition, ProTego's SIEM is complemented by two tools that add task automation: Wazuh [3] and Ossec [4]. The evolution of this SIEM within the ProTego project will be within the scope of Machine Learning.

III.5.1. Applications and Customers

The GFI SIEM (Security Information and Events Management) allows monitoring, not just the security of IT infrastructures in general, but also the specific security events that are detected by the rest of the components of the toolkit, to be precise the Cybersecurity Risk Mitigation Tools. This provides an integrated security perspective as a whole.

In addition, the integration with other Cybersecurity Risk Assessment Tools, such as the SSM (System Security Modeller), through mutual feedback between them, allows a continuous update of current risks.

And what's more the SIEM intends to be a security analytics platform that can be used with machine learning techniques over the big security data collected, giving the possibility of detecting complex attacks and in some cases even predict them.

Within health environments, whether hospitals or health centers, a SIEM is an ICT tool managed and administered by ICT departments. Therefore, the direct clients that acquire a SIEM tool are the ICT departments of hospitals or health care centers themselves. The users who use this tool are the members of the ICT departments, especially those dedicated to cybersecurity. The beneficiaries of the tool are the hospital patients or health centers themselves, as well as all hospital or health center staff (nurses, doctors, administrative staff, laboratory staff, radiology staff...).

Although SIEM is being parameterized and adapted to health environments (within the ProTego project), any medium or high-sized entity would potentially be a client of SIEM.

III.5.2. Market Potential Attractiveness

Currently, in the market there are several SIEM tools both commercial and OpenSource [2] although the market in these tools is constantly changing.

In our case (ProTego project) the SIEM that is being developed includes machine learning as a differential market value.

We have evaluated the potential markets described above in terms of "Potential" as follows:

Potential

Compelling reason to buy

The SIEM developed for ProTego although it is a very important tool in itself and provides great value in terms of cybersecurity within the environment in which it is deployed, the important value of the SIEM is the integration with the other components of ProTego and especially the customization of the SIEM in particular and ProTego in general to a hospital ICT environment (although with the possibility of implementing it in any medium or high-sized company, not only in health settings).

Another reason to buy the ProTego SIEM is its core developed in Open Source, this means periodic updates of the core by the community.

Market Volume

The volume of the market is the hospital centers of the European Union. There are currently 4929 hospitals throughout the European Union [6].

Of course, the SIEM can also be implemented in any type of organization.

Economic Viability

Healthcare organizations have the highest cost per data loss or theft of any organization [6]. Therefore, the economic viability of implementing a SIEM is more than justified.

This link [7] explains the 4 basic pillars of success for the ROI of a SIEM.

In terms of “Challenge” we think:

Challenge

Implementation obstacles

Implementing tools to reduce cybersecurity risks is a complex process. Parameterization of these tools is not an automatic process and requires a great deal of time and effort.

Time to revenue

However, although the process of implementing and implementing tools to reduce cybersecurity risks is a complex process, the return on investment time in both time and money is very small.

External risks

- Hospital applications not adapted to the requirements of cybersecurity tools.
- Low awareness of work staff and clients.
- Obsolete or deficient infrastructures.

III.5.3. Strategy

The SIEM exploitation strategy as an independent asset within the ProTego toolkit will be based on different critical aspects:

- Context characterization and interactions involving strong market and stakeholder analysis, engagement of stakeholder community, end-users and standardisation activities.
- Preparing exploitation during development to avoid R&D death-valley by performing competence assessment to match features with needs, identifying the beneficiaries of each result with associated responsibilities and protecting IPR.
- Entering the market strongly supported by solid exploitation plan and business model for commercialisation enhanced by end-users’/stakeholder’s education and training through multi-channel dissemination activities.

The ProTego Exploitation Strategy includes revision of the potential ProTego stakeholders and market opportunities.

First, the potential market for the SIEM is analysed:

- Generic market
- Hospitals and health care centres in Europe

The markets affected by the SIEM approach which therefore have to be analysed and the strategic overlap identified are the following:

- Emerging markets of cybersecurity, with tools going beyond the state of the art and reaching a higher level of prevention and protection against cyberattacks.
- European IT market related to the provision of specific tools for the health sector.
- Emerging markets for connected devices devoted to health sector, such as remote care programmes, throughout Europe as potential candidates for early adopters.

III.6. ProTego Toolkit Assembler

ICE, as a commercial SME focused on IT products and services development, will focus on: i) promotion of project outcomes in relevant markets; ii) improving its product portfolio (particularly ProTego Toolkit Assembler features) with new software tools, services and features coming from the execution of ProTego; iii) interacting with the ProTego technical community to develop opportunities for joint exploitation, new business models and market value.

In ProTego, the integration of open-source tools plus the extra layer of security and network slicing (using Docker containers) will allow the integration platform to easily deploy applications and services and as an innovation action to enhance the technology readiness level towards productisation and commercialisation.

Core abilities or technological elements:

- Integration to provide further expansion.
- Reduce time in implementation.
- Control the flow of traffic, and API calls between services.
- Secure Services.
- Control over the deployment and orchestration of distributed services.
- Observe what is happening in all services with tracing, monitoring and logging.

III.6.1. Applications and Customers

ProTego Toolkit Assembler will allow potential customers to cater their needs for easy deployment, management and maintenance (including security aspect) of distributed applications and services. The customers will benefit from its ease of use, portability, scalability deployment, flexibility of use and control and management over all its components, plus the specialised networking capabilities.

ICE envisages the Toolkit Assembler being used by systems integrators particularly in the area of healthcare. It may also be of use to other SMEs for integrating distributed general distributed systems. Ultimately this demand will be driven by healthcare providers, which need an integrated system to manage multiple different functionalities, but can also be customised for their individual needs, regulations, and environments.

ProTego Toolkit is involved in different use cases, configuring network slices, logging mechanism, application access control, correlation rules.

The ProTego Toolkit Assembler will offer customers a dedicated toolkit for easily combining these industry standard open source tools. ProTego creates a product focused on a domain specific employment for example in healthcare. However, this software is not limited to healthcare applications and can be deployed in other situations, for example manufacturing.

III.6.2. Market Potential Attractiveness

There are several tools in the market that offer different solutions that can be implemented separately. It takes time and effort to link them together which hinders their use. The ProTego Toolkit Assembler provides networks and security for distributed functionality in a single interface.

With the availability of necessary DevOps support features (see the list below) in a single platform, the users will be able to easily deploy and manage their solution in a distributed environment.

Docker containers are a secure industry standard containerisation system. The use of containers reduces resource costs due that the isolation they provide and only including the applications needed to run. Multiple containers can share the same OS and network connection. Due to their lightweight design, they save on hardware and data centre costs. The isolation of features achieved by the containers enables the solutions to run across environments and gives the ability to respond quickly to customer requests for bug fixes or new feature releases.

Kubernetes is open source and it has a very mature and proven architecture. It can be deployed on any infrastructure. It eases container management and helps to reduce the delay in communication. It can replicate containers and, with the use of a load balancer, decide which nodes are less loaded, so it shares the load with other nodes. Kubernetes also automatically handles networking, storage, logs, alerting, for all containers.

Istio is open source. It provides multiple layers of security by integrating with other security systems. It provides visibility within the system by using automatic tracing, monitoring and logging of all services. Istio intelligently controls the flow of traffic and API calls between services, it conducts a range of tests and can provide gradual upgrades with red/black deployments.

Rancher is an open source platform that provides the capability to build a container services platform from scratch. It manages Kubernetes clusters running anywhere. It provides load balancing, multi-host networking, and volume snapshots amongst other things.

III.6.3. Strategy

ICE's strategy is to use this Toolkit Assembler within ICE as part of internal infrastructure as well as to exploit this in future R&D projects. ICE will also look to exploit this commercially as when the technology is mature enough to do so.

ICE will utilise market analysis and research done within ProTego to help understand the better commercial realisation of this product and to increase our commercial opportunities.

III.7. Network Performance and Privacy slicing

IMEC is developing two components, including algorithms, in order to provide network slicing, targeting operational networks within the hospitals, guaranteeing both QoS performance and privacy for the exchange of medical data.

III.7.1. Applications and Customers

Within the Protego project, the customers are the hospitals installing the data protection toolkit. Using the network slicing solutions will guarantee to customers (hospitals) with QoS performance and privacy isolation among slices for exchanging different types of data traffic, including the different access control levels (e.g patience information will be accessed only via patience slices, isolated from the information that medical personnel should access)

III.7.2. Market Potential Attractiveness

To estimate the market potential, a more profound investigation of the hospital network infrastructure is required to have a better view on the pertinent need for imec's network slicing solution. Note that slicing is typically investigated for future licensed networks, and more specifically 5G. However, the same concept will definitely have its benefits in a Wi-Fi context as well.

III.7.3. Strategy

Imec's solution can be interesting for the hospitals installing the Protego toolkit (guaranteeing them a reliable wireless network infrastructure, guaranteeing performance and privacy via isolated network slices), but this will be rather in consultancy mode to advise them with best practices. The network slicing solution is independent of the Toolkit, and its need will highly depend on the specific wireless network infrastructure at the hospital.

Further imec will use the network slicing concepts developed in ProTego for its internal research and progress into other new topics that build on top of slicing.

III.8. User Requirements Elicitation Service

OSR analysis provides a rich set of methods and best practices for user requirements elicitation and use cases definition. To productively adopt a user-centered approach in the design and development of a product/service, one of the pillars is to rely on an ecosystem where insights, ideas and feedbacks are generated involving the possible users in a process of open innovation. To this extent, the Persona's analysis has been deployed in a living-lab based cross-disciplinary and countries environment, where patients, caregivers, technicians, developers, researchers and domain experts where easily accessible and involved in the project lifetime.

III.8.1. Applications and Customers

Hospitals like the San Raffaele are populated daily by thousands of people, counting the patients who come for medical examinations, hospitalized patients, families of patients, clinicians and researchers.

The policy with which their devices are handled is supposed to be codified by a set of rules dictated by the hospital's administration department.

However, in several cases the rules developed for the correct management of security measures are not respected:

- Patients come to the hospital with their medical devices and their cables and these devices (brought from home and containing patient data) are connected to one of the desktop computers with which the doctor can interact;
- Staff access data from home, using their mobile devices, and exchange data via e-mail or via USB devices (eg Pen drive or hard disk);
- Staff connect their mobile devices (mainly smartphones) to desktop computers via cable or Bluetooth.

With the fact that health information is an attractive target and difficult to defend against cyber criminals, this entails a very specific risk.

The ProTego project will develop a toolkit and guidelines to help health care systems users address cybersecurity risks in this new environment by introducing 3 main advances over current approaches:

- Extensive use of machine intelligence
- Advanced data protection measures
- Innovative protocols for stakeholder education

Among the potential customers, we can mention the main health service providers including:

- Public health, hospitals, outpatient and high-tech health infrastructures
- Health service providers for electro medical and research equipment
- Insurance companies for reimbursement of medical expenses

- Medical informatics referred to health services

III.8.2. Market Potential Attractiveness

OSR requirements elicitation service productively adopt an user-centered approach in the design and development of a product/service, relying on an ecosystem where insights, ideas and feedbacks are generated involving the possible users in a process of open innovation.

To this extent, the Persona's analysis has been deployed in a living-lab based cross-disciplinary and countries environment, where patients, caregivers, technicians, developers, researchers and domain experts where easily accessible and involved in the project lifetime.

Healthcare service providers who have the opportunity to carve out new market shares providing personalized services on users' needs, may take benefit from this analysis who take into consideration also the ProTego KPI's used to measure the expected impact of the project:

- #1 to #5 will improve security of health and care services, data and infrastructures
- #6 to #8 will provide a specific mechanism to reduce the risk of data privacy breaches
- #9 and #10 will increase patient trust and safety

III.8.3. Strategy

Clinical Engineering Service and IT/HR Dep are the contact point with healthcare service providers because they have the chance to propose a new demand for personalized services:

- An internal Clinical Engineering Service is present at San Raffaele Hospital: this service is dealing with the electro medicals and research equipment used within the hospital, most of them are connected with the IT network. According to the GDPR 2016/79 an adequate level of IT security has to be reached: for that reason the Clinical Engineering Service has defined a Gold Standard to which all equipment suppliers must be compliant. This Standard is depending on the hospital that means different hospitals have different Gold Standards. The ProTego KPIs have the chance to improve the existing Gold Standard and also to generate new ones in different departments, as the IT Dep.
- The San Raffaele Hospital organizes online training courses and awareness campaigns for all those who have access to the IT system (mainly employees): these courses, taking into account the KPI's dedicated to improve trust and safety, can be customized based on the real behavior of all the users.

IV. Value Propositions

IV.1. System Security Modeller

The primary market opportunity is to use the SSM with security consultancy customers.

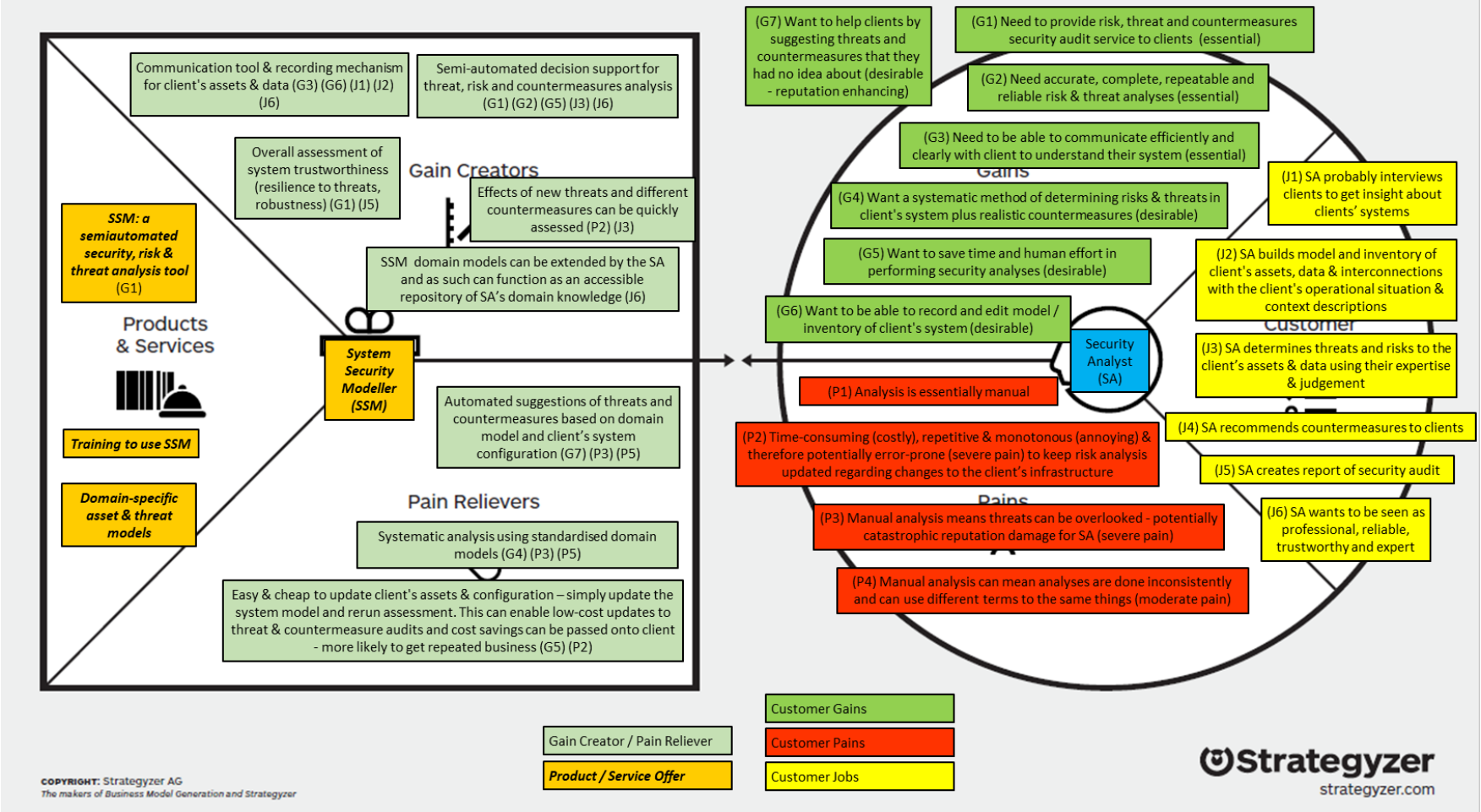

Figure 2 Value proposition of System Security Modeller

V. Business Models

V.1. System Security Modeller

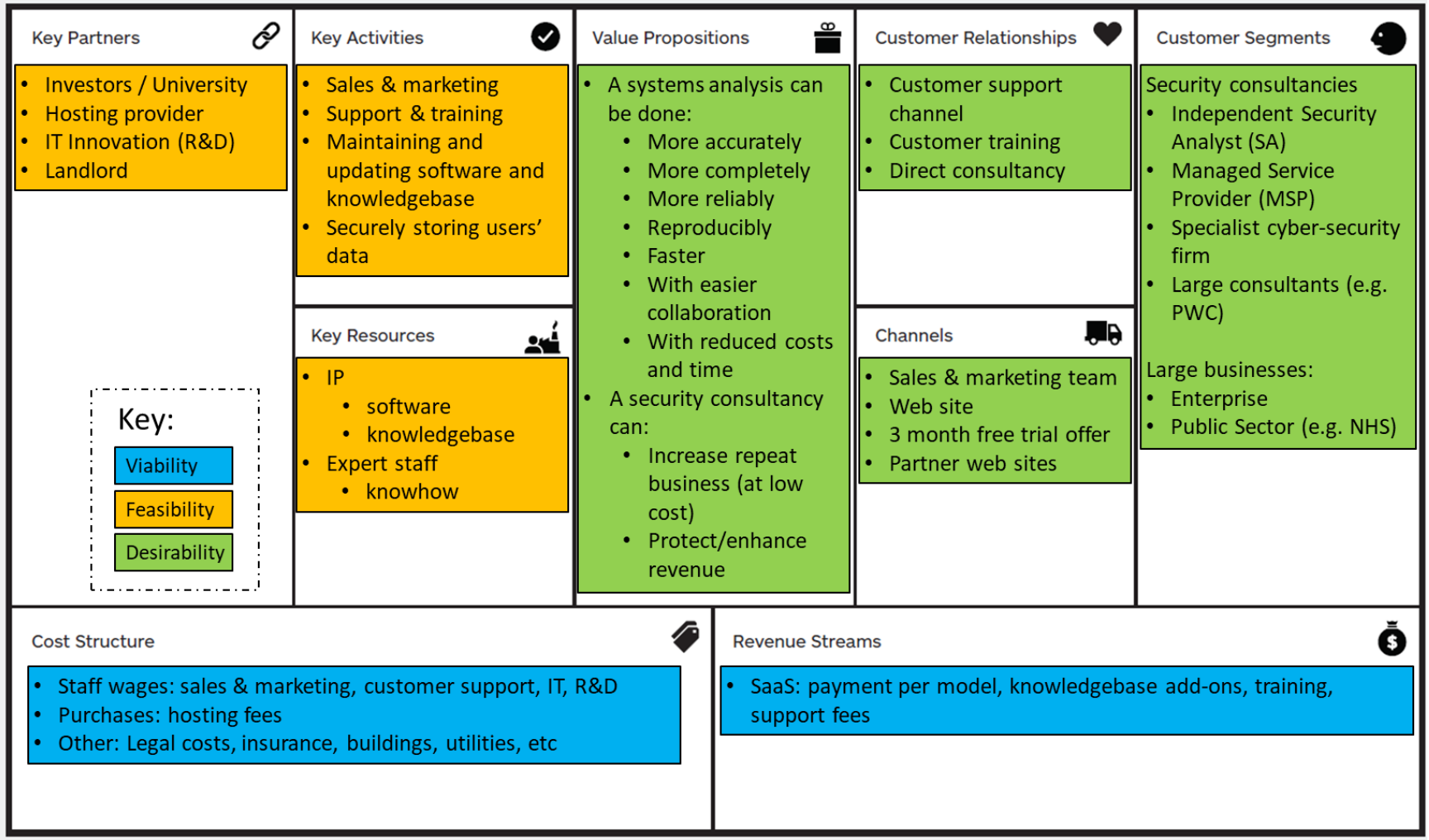

Figure 3 Business model canvas of System Security Modeller

V.2. Requirement Elicitation Service

(1) Problem	(4) Solutions	(3) Unique Value proposition	(6) Unfair Advantage	(2) Customer segment
The clinical functionality of devices as smartphones increase daily. Processes that were traditionally implemented using expensive electromedical devices installed in hospitals can increasingly be transformed by using small, cheap devices Bluetooth or Wi-Fi to a Smartphone, where an application records and processes the acquired data and sends the results to a corporate EMR. The cybersecurity challenge, already difficult, is becoming more complex due to this introduction of more devices with access to health data, often not directly under the control of a hospital.	Consultancy service Multi-party requirements elicitation will be conducted involving end-users (e.g., IT and management staff, clinicians, patients). The involvement of professional users (IT and management staff) ensures that also non-functional requirements are taken into account.	OSR analysis provides a rich set of methods and best practices for user requirements elicitation and use cases definition. To productively adopt an user-centered approach in the design and development of a product/service, one of the pillars is to rely on an ecosystem where insights, ideas and feedbacks are generated involving the possible users in a process of open innovation. To this extent, the OSR analysis suite has been deployed in a living-lab based cross-disciplinary and countries environment, where patients, caregivers, technicians, developers, researchers and domain experts where easily accessible and involved in the project lifetime.	Making a multi-party requirements elicitation at the San Raffaele's Science Park is quite unique: an Health-centric Ecosystem contained within an area of 300,000 sqm, can be described as a tertiary urban area or a compact urban district where all daily and typical operations are concentrated in a reduced space. Thus, its structures allow to access, understand, study and measure the daily interactions among an estimated 25,000+ community of the San Raffaele daily Users (20,000+ a day turnover of inpatients, outpatients and visitors of all ages and needs; 5000+ on site employees, researches, etc.; 2000+ students) and a whole range of services available in an area that includes new and retrofitted buildings with very different destinations	Service providers who have the opportunity to carve out new market shares providing personalized services on users' needs • Healthcare providers specialized in chronic diseases, such as diabetes. • Professionals dealing with lifestyle-associated disorders, such as hypertension, cardiovascular disorder and obesity. • Public health, hospitals, ambulatory, high-tech healthcare infrastructure, insurance companies, medical informatics referring to health services

<table>
<tr><td></td><td>(8) Key Metrics

Number of consultancies</td><td colspan="2"></td><td>(5) Channels

First of all we can take into account our IT healthcare providers</td><td></td></tr>
<tr><td colspan="3">(9) Cost structure

Personnel costs: administration, sales / marketing, service design and professionals as needed (in this case IT and doctors).</td><td colspan="3">(7) Revenue Streams

Consultancy revenues</td></tr>
</table>

Figure 4 Business model canvas of Requirement Elicitation Service

VI. Standardisation

The specification of Parquet Modular Encryption has been released in October 2019, becoming an important part of the Apache Parquet open standard, backed by the community. IBM work on this had been partially funded by the ProTego project.

We are working on a reference implementation of this standard. A significant part of the Java implementation will be developed during the ProTego project and tested with its use cases in the domain of healthcare security.

In addition, we have started to discuss with the HL7 community a possibility to extend the HL7 FHIR standard to include Parquet as a secure and efficient Bulk Data format. We have presented the Parquet-based data management approach at the HL7 FHIR conference, and together with the community leaders, have opened a formal channel for this topic at fhir.org discussion streams, where we will use the ProTego work to demonstrate the performance and security benefits of such extension to the FHIR standard. This is a long-term goal, with no guarantees of timelines or success, as with any standardization activity.

VII. Personas

The project is collecting personas to better understand the customers and beneficiaries of the ProTego tools.

PERSONAS

PERSONA NAME:

Carlos

AUDIENCE SEGMENT:

Technical services

WHO AM I

Head of Networking and communications at Hospital de Denia. As this a paper-less Hospital, most workflows are based on IT systems and need to integrate many systems and devices. Suitable communication channels are needed for each scenario (performance and security).

3 REASONS FOR ME TO ENGAGE WITH YOU

Be able to isolate communication channels, ensuring performance needed.

Be able to make secure communications between on-premise and cloud, as we have systems in both sides.

Be able to make risk assessment during the network design phase

3 REASONS FOR ME NOT TO ENGAGE WITH YOU

Not possible to use network functionalities isolated from the rest of ProTego tools.

The cost of HW elements I should buy is so expensive.

It's not compatible with my current network systems.

MY INTERESTS

Technology

IoT

MY PERSONALITY

High education level

For me technology is a hobby in addition to my job

MY SKILLS

Well organized

Able to manage based on priorities

MY DREAMS

A safe and interconnected world

MY SOCIAL ENVIRONMENT

Use to go to professional meetings about cyber security.

PERSONAS

PERSONA NAME:

Miquel

AUDIENCE SEGMENT:

Technical services

WHO AM I

Head of Technological Infrastructure at Hospital de Denia. I manage the data center and I'm responsible of the continuity of service of the applications in the Hospital. As this is a paper-less Hospital its dependency of the IT systems is very high, and the Hospital can't afford a downtime for more than a few

3 REASONS FOR ME TO ENGAGE WITH YOU

Possibility to have a SIEM tool that will help us to monitor systems on production to detect abnormal activity

Introduce safe access control over data, in the self-developments we may do to complement our core system maps

Be able to use ProTego tools in hybrid cloud scenarios, defining where each component should be used (on-prem or cloud)

3 REASONS FOR ME NOT TO ENGAGE WITH YOU

Obligatoriness to install all components in the same system, not covering hybrid cloud scenarios

Incompatibility with market systems, as they are working in the Hospital

Difficult to use so it's needed to increase the costs, by extending the staff

MY INTERESTS

Technology

Integration

Continuity of service

MY PERSONALITY

High education level

For me technology is a hobby in addition to my job

MY SKILLS

Well organized

Able to make protocols for any action or service anybody demands from my department

MY DREAMS

Feel that the Hospital IT systems are completely safe and all the threads are managed

MY SOCIAL ENVIRONMENT

In addition to the personal relations, I'm part of some online communities with similar interests

VIII. Conclusions

We have presented an intitial analysis and plans for the exploitation of ten ProTego assets using the frameworks of the Market Opportunity Navigator and the Value Proposition and Business Model Canvasses. In addition we have described an initial engagement in standardization activities (which influence markets) and some personas of potential users and customers.

Not every asset will become a product in the market and so not every asset requires the entire analysis chain from market opportunity to business model. It is important to understand what the opportunities are though and so every asset has been represented in that part of the analysis.

Of the exploitable assets, the System Security Modeller is closest to being a product in the market and so its analysis is most extensive. As the project proceeds we expect to add additional analysis around many of the assets as the value and markets are better undersood.

IX. Acknowlegements

The Market Attractiveness Map is reproduced from www.wheretoplay.co under the Creative Commons Attribution-NonCommercal-ShareAlike 4.0 International license.

The Value Proposition Canvas and Business Model Canvas diagrams are reproduced from strategyzer.com under the Creative Commons Attribution-ShareAlike 3.0 Unported License.

The Business Model Canvas concept was initially proposed by Alexander Osterwalder.

X. References and Internet Links

[1] [Online]. Available: https://wheretoplay.co/.

[2] [Online]. Available: https://www.strategyzer.com/.

[3] [Online]. Available: https://cloud.ibm.com/docs/services/AnalyticsEngine?topic=AnalyticsEngine-parquet-encryption.

[4] [Online]. Available: https://www.elastic.co/.

[5] [Online]. Available: https://wazuh.com/.

[6] [Online]. Available: https://www.ossec.net/.

[7] [Online]. Available: https://www.msspalert.com/cybersecurity-services-and-products/siem/top-10-software-tools/.

[8] [Online]. Available: http://hospitals.webometrics.info/es/ranking_europe/european_union?page=49.

[9] [Online]. Available: https://www.eventtracker.com/blog/2014/july/siem-and-return-on-investment-four-pillars-for-success/.


ProTego