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

D3.3 Final description of educational framework: Protocols and methodologies for health staff and patients

Responsible:	MS (Salvador Garcia)
Contributors:	MS, OSR, Inetum (GFI before 2021), IBM, KUL, IT Innovation
Document Reference:	D3.3
Dissemination Level:	Public
Version:	1.0
Date:	30/06/2021

Executive summary

This document contains the final description of the Educational framework developed as part of the ProTego project. It offers an overview of what should be the process of implementation of cybersecurity in a healthcare organization. Among the different aspects and phases, it focalizes in those referred to user awareness, explaining in detail a user awareness training program created as part of ProTego and that will be deployed in MS and OSR. This awareness training program has been designed in alignment to the conclusions of the Deliverable 3.1 within this project and is intended to improve situational awareness and increase the good behaviours in terms of cybersecurity. It is based on the people centric security paradigm and aims to achieve that users apply cybersecurity principles in any situation even outside the work environment.

ProTego includes the development of a technical toolkit that will reduce cybersecurity risks. Regarding that toolkit this educational framework will describe how this toolkit is aligned with the cybersecurity standards: based on the NIST CSF, the items that the ProTego toolkit helps to accomplish have been identified.

The section devoted to the IT staff has been designed to serve as a first contact point with the ProTego toolkit for such stakeholders, as they are the main users of the offered platform. It offers the information needed to assess the ProTego adoption by explaining the basics of each component, features, requirements to be provided and how they should be included as a part of the IT map of the healthcare organization.

The educational needs of external providers have been also covered, by depicting how external applications may integrate with each component of the ProTego toolkit, what is necessary to take advantage of the benefits it offers in terms of risk assessment and risk mitigation.

IoT concerns have been tackled by dividing them in two different sections, representing each of them different types of devices used in healthcare: a section devoted to wearables has been included in the educational contents addressed to the external providers, showing how those IoT devices should add functionality to integrate with the ProTego toolkit. And a section dedicated to medical devices has been included in the section devoted to the IT staff. Such separation is needed as those two types of devices have significant differences that make that suitable, as it can be understood by reading those sections.

Contributors Table

DOCUMENT SECTION	AUTHOR(S)	REVIEWER(S)
I	Pietro Vismara (OSR) Salvador Garcia (MS)	Antonio Jesús Gamito (Inetum), Fernando José Rendón (Inetum), Luis Carrascal (Inetum), Steve Taylor (IT Innovation)
II	Antonio Jesús Gamito (GFI), Dave Singelee (KUL), Eliot Salant (IBM), Salvador Garcia (MS)	Antonio Jesús Gamito (Inetum), Fernando José Rendón (Inetum), Luis Carrascal (Inetum), Steve Taylor (IT Innovation)
III	Vicent Moncho (MS) Salvador Garcia (MS)	Antonio Jesús Gamito (Inetum), Fernando José Rendón (Inetum), Luis Carrascal (Inetum), Pietro Vismara (OSR), Steve Taylor (IT Innovation)
IV	Pietro Vismara (OSR) Salvador Garcia (MS)	Antonio Jesús Gamito (Inetum), Fernando José Rendón (Inetum), Luis Carrascal (Inetum), Carlos Cilleruelo (UAH), Boki Ashmore (ICE), Steve Taylor (IT Innovation)
V	Salvador Garcia (MS)	Antonio Jesús Gamito (Inetum), Fernando José Rendón (Inetum), Luis Carrascal (Inetum), Boki Ashmore (ICE), Steve Taylor (IT Innovation)
VI	Salvador Garcia (MS)	Antonio Jesús Gamito (Inetum), Fernando José Rendón (Inetum), Luis Carrascal (Inetum), Carlos Cilleruelo (UAH), Noel Tomas (ICE), Steve Taylor (IT Innovation)
VII	Pietro Vismara (OSR) Salvador Garcia (MS)	Antonio Jesús Gamito (Inetum), Fernando José Rendón (Inetum), Luis Carrascal (Inetum), Steve Taylor (IT Innovation)

Table of Contents

I. OVERVIEW OF PROTEGO EDUCATIONAL FRAMEWORK 8

I.1. BACKGROUND 8
I.2. STAKEHOLDERS 8
I.3. SCOPE 10
I.4. STRUCTURE 10
I.5. RELATION TO THE SURVEY IN D3.1 12

II. ADHERENCE TO STANDARDS AND REGULATIONS 14

II.1. ISMS: INCORPORATING INFORMATION SECURITY 14
II.2. NIST CSF 15
II.2.1. Background 15
II.2.2. Structure and implementation 16
II.3. NIST CSF IN PROTEGO 21

III. PEOPLE-CENTRIC SECURITY MODEL 30

III.1. EVOLUTION OF INFORMATION SECURITY 30
III.2. CYBERSECURITY IN THE ORGANIZATION 31
III.3. PEOPLE-CENTRIC SECURITY MODEL 34

IV. EDUCATIONAL MATERIAL FOR HEALTH STAFF 36

IV.1. PROTEGO EDUCATIONAL WEBSITE 36
IV.2. EXECUTION OF THE TRAINING PROGRAM 40
IV.3. CONTENTS OF THE TRAINING PROGRAM 41
IV.3.1. Block 0: Introduction 41
IV.3.2. Block 1: The good employee 43
IV.3.3. Block 2: Safe passwords 43
IV.3.4. Block 3: Social engineering 44
IV.3.5. Block 4: Mobile devices 45
IV.4. STORYBOARD 46
IV.5. ASSESSMENT OF THE TRAINING PROGRAM 49
IV.5.1. Impact on the Risk Awareness Profile 50
IV.5.2. Assessment of the material provided 60

V. EDUCATIONAL MATERIAL FOR PATIENTS 66

VI. EDUCATIONAL MATERIAL FOR IT STAFF 68

VI.1. INTRODUCTION 68
VI.1.1. Personas 69
VI.2. ASSESS PROTEGO ADOPTION 70
VI.2.1. Overview of the ProTego toolkit 70
VI.2.2. Modularity and versatility for easy adoption 74
VI.3. PROVISION OF REQUIREMENTS 76
VI.4. DEPLOYMENT AND CONFIGURATION 77
VI.5. USE OF THE PROTEGO TOOLKIT 78
VI.6. SUMMARY 79
VI.7. OPPINION ABOUT THE PROTEGO TOOLKIT 81
VI.8. MEDICAL DEVICES - IO(M)T 83
VI.8.1. Diagnose of current situation 83

VI.8.2. Proposal 85
VI.8.3. ProTego for IO(m)T procurement 90
VII. EDUCATIONAL MATERIAL FOR EXTERNAL PROVIDERS 91
VII.1. INTRODUCTION 91
VII.2. SYSTEM SECURITY MODELLER (SSM): 91
VII.3. DATA GATEWAY (DGW) + ACCESS CONTROL FRAMEWORK (A.C.) 92
VII.4. CONTINUOUS AUTHENTICATION (C.A.) 94
VII.5. NETWORK SLICING (NSL) 95
VII.6. SIEM 95
VII.7. IOT DEVICES 96
VII.7.1. Connected IoTdevice 96
VII.7.2. Non connected IoT device 98
VIII. REFERENCES AND INTERNET LINKS 101
APPENDIX A. INTRODUCTION TO CYBERSECURITY AWARENESS 102
APPENDIX B. FORM FOR MEDICAL DEVICES MAINTENANCE 106
APPENDIX C. SSM TUTORIAL 108
APPENDIX D. SURVEY TO ASSESS THE TRAINING PROGRAM 136

Table of Figures

Figure 1: Stakeholder map of the ProTego toolkit 9
Figure 2: Structure of educational framework 11
Figure 3: NIST CSF Functions 18
Figure 4: NIST CSF Categories 18
Figure 5: NIST CSF Subcategories and informative references 19
Figure 6: NIST CSF Profiles 20
Figure 7: Three waves of Information security 31
Figure 8: Cybersecurity scope 32
Figure 9: Concept of Gartner's People-Centric Security 34
Figure 10: Screenshots of the educational videos 37
Figure 11: Printable tips 38
Figure 12: Dissemination posters 40
Figure 13: Risk Awareness Profile - MS 52
Figure 14: Risk Awareness Profile - OSR 58
Figure 15: Effectiveness of the material 60
Figure 16: Perceived usefulness 61
Figure 17: Perceived clarity 62
Figure 18: Perceived motivation 63
Figure 19: Perceived efficiency 64
Figure 20: Satisfaction 65
Figure 21: User interaction with the ProTego toolkit 68
Figure 22: Phases for ProTego adoption 68
Figure 23: IO(m)T systems 84
Figure 24: Dataflow for authorization in data access 93
Figure 25: IOT first request for data 97
Figure 26: IOT subsequent requests for data 97
Figure 27: Non connected IoT device 99

List of tables

Table 1: Educational framework stakeholders 9
Table 2: Stakeholders and document sections 11
Table 3: Conclusions of the Health Belief Model survey in D3.1 12
Table 4: Examples of EU NIS transpositions 16
Table 5: ProTego-related items within the NIST CSF 23
Table 6: Educational external links 39
Table 7: Phases of awareness program for health staff 41
Table 8: Carlo, the “Network operator” persona 69
Table 9: Andrew, the “IT Infrastructure Manager” persona 70
Table 10: Resumed functionality of the ProTego toolkit components 74
Table 11: Catalogue of possible configurations of the toolkit 75
Table 12: Requirements - IT Infrastructure Manager 77
Table 13: Requirements - Network Operator 77
Table 14: Deployment - IT Infrastructure Manager 78
Table 15: Deployment - Network Operator 78
Table 16: Summary - IT Infrastructure Manager 80
Table 17: Summary - Network operator 81
Table 18: Interview for IT staff 83
Table 19: Assessment of medical devices 87
Table 20: Examples of Medical Device Systems 88
Table 21: Data requested for the SSM model 92

Table of Acronyms and Definitions

Acronym / Definition	Explanation
BYOD	Bring Your Own Device
CDSS	Clinical Decision Support System
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technologies
COSO	Committee of Sponsoring Organizations
DPIA	Data Protection Impact Assessment
EMAR	Electronic Medical Administration Record
EMR	Electronic Medical Record
EMRAM	Electronic Medical Record Adoption Model
ENISA	European Union Agency for Network and Information Security

ENS	Spanish National Security Framework
FDPA	French Data Protection Act
FHIR	Fast Healthcare Interoperability Resources
GDPR	General Data Protection Regulation
IAM	Identity & Access Management
ICT	Information and Communications Technologies
IO(M)T	Internet Of Medical Things
IS	Information Security
ISMS	Information Security Management System
JWT	JSON web token
MDS	Medical device system
MS	Marina Salud
NIS	EU Network and Information Security directive
NIST	National Institute of Standards and Technology
NIST CSF	NIST Cyber Security Framework
OSR	Ospedale San Raffaele
PCS	People-Centric Security
TTL	Time To Live
USC	User Support Centre

I. OVERVIEW OF PROTEGO EDUCATIONAL FRAMEWORK

I.1. Background

The ProTego project will provide a toolkit for health care organizations to better assess and reduce cybersecurity risks related to remote devices access to Electronic Health Record data, including risks assessment and risks mitigation tools as well as methodologies and protocols for prevention and reaction. In addition, the toolkit will provide tools to raise awareness and educate stakeholders in how they can reduce or prevent risks.

This stakeholder education is crucial, especially if we consider non IT personnel, mostly clinical but also administrative. After all, it has been demonstrated that people are the weakest link of an organization's security and they are the most exploited vulnerability by attackers.

Although it is feasible to compose and distribute protocols and work instructions explaining the correct use of the tools and systems from the cybersecurity perspective, the reality is that all those protocols are perceived by health staff as technical material treating technical issues that are, hence, responsibility of the IT department. Furthermore, any protocol or work instructions set cannot cover all existing risks in a changing environment that offers new functionalities every day, such as Bring Your Own Device (BYOD), Internet Of Medical Things (IO(m)T), telemedicine and remote patient care through cloud services. And all under the mandatory requirement of interoperability that on the one hand allows the existence of a unified EMR whose benefits are out of the scope of this document, but instead offers attack vectors to reach many interconnected systems.

Therefore, the educational framework defined in ProTego has as fundamentals the following objectives for each target audience:

- healthcare industry / regulators: to describe the adherence to the cybersecurity standards of the ProTego toolkit. Choosing the NIST CSF [7] as reference the document elicits which items are facilitated by the toolkit (Section II).

- healthcare staff and patients: to improve situational awareness of healthcare staff and patients, increasing correct behaviours regarding cybersecurity and making them more receptive to future recommendations or protocols (Section IV and V).

- external providers: to explain how to create ProTego compliant applications and services, to take advantage of the features offered by ProTego. (Section VII).

- healthcare IT: to understand the basics of the ProTego toolkit, allowing to assess the ProTego adoption in the healthcare organization, provide the required infrastructure and overview the deployment and management of the toolkit. (Section V1).

These recipients are described in more detail in section I.2.

I.2. Stakeholders

The stakeholders of the educational framework must correspond to the stakeholders of the ProTego toolkit. This is the ProTego toolkit stakeholder map resulted from the analysis performed in Deliverable 2.2:

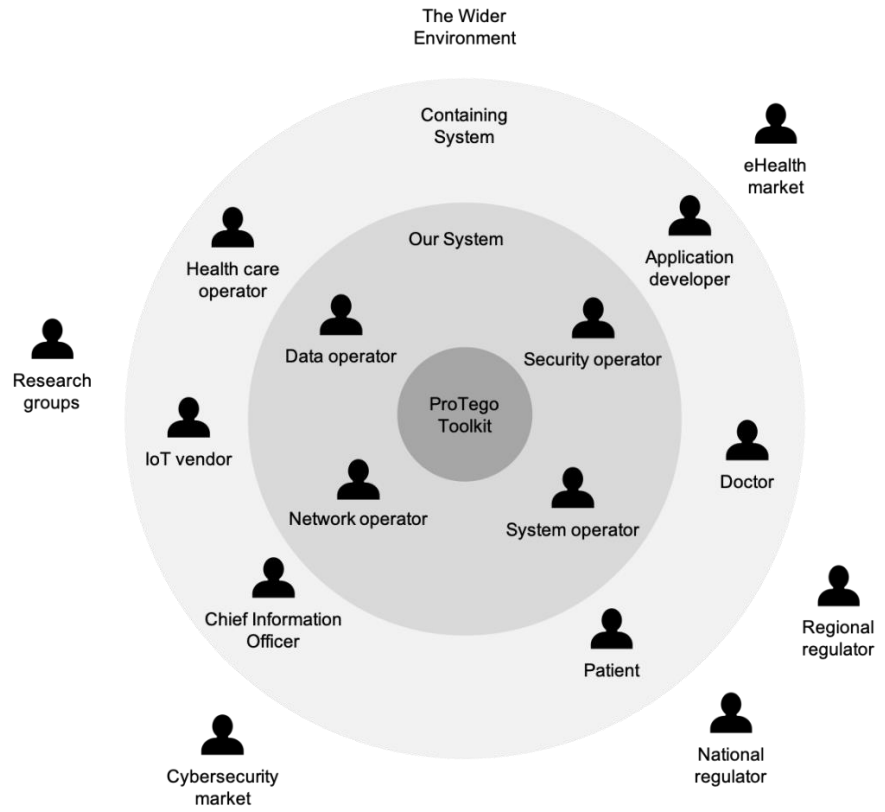


Figure 1: Stakeholder map of the ProTego toolkit

Attending to the interests, objectives and therefore type of educational material developed, this stakeholder map has been classified in five groups that conform the final stakeholder map of the educational framework.

ProTego toolkit stakeholders	Educational framework stakeholders	Description
Research groups	Health staff	Physicians, researchers, nurses, ancillary clinical personnel.
Doctors		
Patients	Patients	Patients
App developers	IT staff	Technical staff with responsibilities in the management (design, development, deployment, configuration, monitoring) of corporate applications
Healthcare operators		
CIO		
Network operators		
System operators		
Security operators		
Data operators		
eHealth market	External HW/SW providers	External HW/SW providers that need to know how to develop ProTego compliant products
IoT vendors		
Cybersecurity market	Regulators	External stakeholders interested in the compliance of ProTego toolkit with the information security standards
National Regulators		
Regional regulators		

Table 1: Educational framework stakeholders

This classification makes the list more general because although the segregation of duties and functions is a common recommendation in Information security standards, for example in control A.6.1.2 from ISO 27001:2013 [1], it is not widely applied, usually depending on the size of the organization.

I.3. Scope

The general scope of the educational framework is to provide tools to each stakeholder that contribute to reduce risks and to improve the overall security. It is necessary to define the main objectives to reach for each component of the stakeholder's map.

Health staff

Description: This group includes the most of the final users of the corporate applications and devices. They systematically treat sensitive data of patients from interconnected systems. They make use of BYOD strategies introducing risks to the working environment that were caused by behaviours in the private sphere. They don't know all the types of attacks in which they act as potential victims.

Objectives: Let them know the consequences of incorrect behaviours, even from private context and with their own devices. Increase a collaborative environment with cybersecurity operators, promoting the notification of incidences and risky situations.

Patients

Description: Final users of applications offered from healthcare organizations. Lower impact in the overall security due to restricting permissions, but very low level of cybersecurity awareness. Difficult to make training reach them.

Objectives: Increase situational awareness by reaching them with concrete messages through the limited communication channels.

IT staff

Description: Technical staff with responsibilities in the management of corporate applications and the design and management of the technological infrastructure.

Objectives: Provide enough information to make possible to assess the adoption of the ProTego toolkit. Describe the features and requirements of each component and which would be the tasks they would have to perform to deploy and manage the toolkit.

External providers

Description: External hardware and software providers of healthcare applications and IO(M)T devices that have historically focused on clinical functionality but less in information security.

Objectives: Describe the requirements for those hw/sw elements to be ProTego compliant, that is, to be able to integrate with ProTego taking advantage of the functionalities that the toolkit offers in fields as authentication, authorization, encryption or real time monitoring.

Regulators

Description: Regulators that may have interest or responsibility derived of the fact that the healthcare organizations accomplish with international cybersecurity standards.

Objectives: Explain to what extent the toolkit is compliant with the standards, helping to perform the controls that those standards recommend.

I.4. Structure

The following figure illustrates the structure of the educational framework:

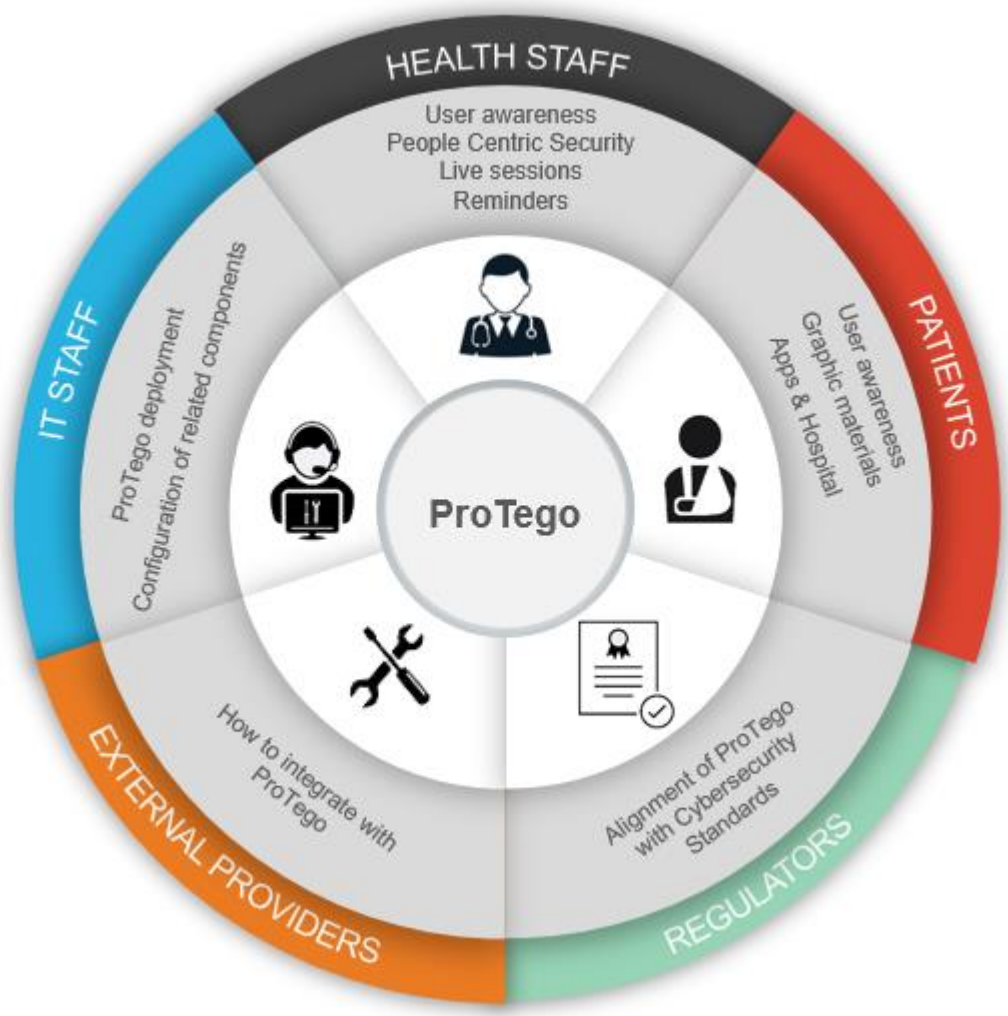


Figure 2: Structure of educational framework

The table below shows in which section of the document is included the content for each stakeholder:

STAKEHOLDER	SECTION OF THE DOCUMENT
REGULATORS	II.- Adherence to standards and regulations
HEALTH STAFF	IV-Educational material for health staff
PATIENTS	V-Educational material for patients
IT STAFF	VI-Educational material for IT staff
EXTERNAL PROVIDERS	VII-Educational material for external providers

Table 2: Stakeholders and document sections

I.5. Relation to the survey in D3.1

In Deliverable 3.1 of ProTego, a survey based on the Health Belief Model was executed to extract conclusions regarding the factors that lead users to adopt correct cybersecurity behaviours. Those conclusions have been observed for the design of the educational framework presented in this document.

The conclusions of the survey are summarised by the table below showing the hypothesis tested and the result in a binary categorical format of "SUPPORTED" / "NOT SUPPORTED":

ID	HYPHOTESIS	CONCLUSION
H1	Perceived Susceptibility (SUS) would be positively related to Cybersecurity Behaviour	NOT SUPPORTED
H2	Perceived Severity (SEV) would be positively related to Cybersecurity Behaviour	SUPPORTED
H3	Perceived Benefits (BEN) would be positively related to Cybersecurity Behaviour	NOT SUPPORTED
H4	Perceived Barriers (BAR) would be negatively related to Cybersecurity Behaviour	SUPPORTED
H5	Self-Efficacy (SEF) would be positively related to Cybersecurity Behaviour	SUPPORTED
H6	Cues to Action (CUES) would be positively related to Cybersecurity Behaviour	SUPPORTED

Table 3: Conclusions of the Health Belief Model survey in D3.1

Those conclusions have been used to focus on that factors that have been demonstrated to elicit better results in terms of good cyber security behaviours. The fact, for example, that H1 have not been supported does not mean that we don't need users to feel identified as potential victims of cyberattacks. It means that, once covered that basic objective, the more effort wasted on that subject will not be rewarded as increased levels of good behaviours.

That said, this is how each of the previous factors have been covered by the educational framework:

H1 - Perceived Susceptibility (SUS): Especially for the awareness program designed for health staff, daily situations are presented and it is explained the risk they can represent. It is mandatory that users understand that they can be used as attack vector just by performing normal behaviours.

H2 – Perceived Severity (SEV): The first block of the awareness training includes an explanation of the three main components (dimensions) of information security and which kind of impact may have a potential breach in each of them. By this, it is reinforced the concept of *perceived severity*: health staff can exactly map the potential consequences of unappropriated cybersecurity behaviours over the patient's safety. The goal behind that is to keep user's attention from the first beginning by letting them map impacts over patient's safety.

H3 – Perceived benefits (BEN): No special reference to this factor has been made. The benefits will be derived from avoiding risks.

H4 – Perceived Barriers (BAR): Mainly when speaking of non IT users (health staff) it has been an objective that the good behaviours to perform don't be perceived as complex technical matters. Almost all the recommendations are about paying attention and perform actions in feasible ways that avoid risks, so the perceived barriers have been set very low.

H5 – Self-Efficacy (SEF): Linked to the BAR factor, the objective has been that users understand how to perform correct behaviours by themselves even in their private scope.

H6 – Cues to Action (CUES): The Health Belief Model on which the survey was based posits that a cue, or trigger, is necessary for prompting engagement in health-promoting behaviours. In this framework "Reminders" have been designed to reinforce training and to improve correct behaviours among the Health Staff. These reminders come in the shape of graphic material in both paper and digital format, placed in strategic locations where can be consumed while performing other tasks and with short messages that will make the training concepts persistent in time.

In D3.1 it was also presented the *Risk Awareness Profile*, a tool that allows benchmarking of the cybersecurity awareness between different organizations or the same organization in different times. It will be used to measure in an objective way the result of the awareness training over the health staff by a second execution of the survey after that training will be performed.

The results will be explained in section IV.3 Assessment of the training program.

II. ADHERENCE TO STANDARDS AND REGULATIONS

As explained further in this section the normative and regulation that healthcare organizations must follow in terms of cybersecurity is different among countries in the EU, but all those regulations have a shared aim and, thus, share concrete items and controls as well.

In addition, GDPR's recital 81 states: "*The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller*" [2], and those approved codes of conduct and certification mechanisms include international recognized standards as ISO/IEC 27000 family, NIST ST-800, COBIT, etc.

From this point of view, it is relevant to know how the ProTego toolkit is aligned with the standards and facilitates to perform the controls included.

II.1. ISMS: Incorporating information security

Every organization is a target for cyber attackers, and that's particularly true in healthcare because healthcare manages the most sensitive data and with the higher value (and price) in black market. That high value is due to its business potential as healthcare services are expensive and being able to identify potential customers would be a high valued item for companies. In addition, any other information about individuals has or may have caducity: credit card numbers, addresses, even names or passport numbers can be changed. But biometrical and medical information is stored as part of the citizen personality and accompany them forever.

In addition, healthcare information has the higher potential to cause detriments or even physically harm individuals if its security is compromised in any of its dimensions:

- **confidentiality**: the unauthorized access or diffusion of healthcare information may cause social detriments as denegation of insurances, barriers to access jobs or social discriminations.

- **availability**: the unavailability of healthcare information may preclude the adequate provision of healthcare services. This risk is higher as the organization is more IT dependent, what use to come with the process integration and efficiency. It may make impossible the provision of services or obligate to take decisions without all the required information which may lead to errors.

- **integrity**: most of the clinical decisions are taken based on antecedents and the falsification of that information may lead to wrong decision as inadequate drug prescription, wrong diagnosis, etc. That risk is getting higher with the inclusion of automated or semi-automated CDSS.

This reality explains why the cyber security is a mandatory concern in healthcare industry. But robust cyber security requires an Information Security Management System (ISMS) built on three pillars: people, processes and technology.

An ISMS can be defined as "*a set of policies and procedures for systematically managing an organization's sensitive data. The goal of an ISMS is to minimize risk and ensure business continuity by pro-actively limiting the impact of a security breach. An ISMS typically addresses employee behaviour and processes as well as data and technology. It can be implemented in a comprehensive way that becomes part of the company's culture.*"[3]

By implementing an ISMS, organizations can secure information, increase resilience to cyber-attacks, and reduce the costs associated with information security

An ISMS brings these benefits to an organization:

- Secure information in all its forms: An ISMS helps protect all forms of information, whether digital, paper-based or in the Cloud.

- Increase organization's attack resilience: Implementing and maintaining an ISMS will significantly increase organization's resilience to cyber-attacks.

- Manage all information in one place: An ISMS provides a central framework for keeping organization's information safe and managing it all in one place.

- Respond to evolving security threats: Constantly adapting to changes both in the environment and inside the organization, an ISMS reduces the threat of continually evolving risks.

- Reduce costs associated with information security: Thanks to the risk assessment and analysis approach of an ISMS, organizations can reduce costs spent on indiscriminately adding layers of defensive technology that might not work.

To implement an ISMS, each organization has to choose a standard specification that serves as guide, and the most spread is the ISO 27001. Neither the concept of ISMS nor the ISO27001 are healthcare exclusives, but it is an accepted evidence that healthcare sector needs special consideration due to its particularities regarding criticism and risk level.

To address these peculiarities, specific branches of the standards are being created specific to this sector. That's the case of ISO that has branched ISO 27002 (Best practices in cyber security) into ISO 27799 (Best practices in cyber security in healthcare).

But healthcare has another significant difference: in the EU it is a business sector that in most cases is considered a public service and as consequence it is directly dependent on the public administration of each state. That has impact on the cyber security as well because in some countries the government states the standards and regulations they must follow. Those specific regulations are aligned with the International standards but have different structure and content. In other words, they are not contradictory to the standards.

As an example, in Spain any public administration, including healthcare organizations, is required to accomplish the ENS (Spanish National Security Framework). In France any chosen regulation needs to be aligned with the FDPA (French Data Protection Act). While, in other countries there is no need to follow additional regulations added to the selected standard framework, but there is still to choose one framework among all the possibilities: ISO / IEC 27001, COBIT, COSO guidelines, or NIST SP 800-53, just to name a few.

Resuming, although all the regulations are aligned and share objectives, recommendations and controls, there is not any standard that can serve as unique reference to implement an ISMS in all the EU healthcare organizations.

When an Information Security Officer plans the strategy for managing the risks associated with the information assets of his organization, he is faced with a decisive question that will define the course of protection actions in the future: What framework of reference should be used to ensure the coordinated management of security controls in an optimal, scalable and integrable way?

However, if one wanted to take advantage of the best of each of these frameworks, the best practices and methodologies in the industry and the experience of hundreds of volunteers in order to establish a consistent and practical line of work to address the risks of current cybersecurity, most likely the choice would be the NIST Cybersecurity Framework (hereinafter CSF).

II.2. NIST CSF

II.2.1. Background

As a result of the increasing number of computer attacks on critical infrastructure systems and the impact that such attacks could have in the context of United States national security, on February 12, 2013 President Barack Obama drafted the Executive Order (EO) of Critical Infrastructure Cybersecurity Improvement [4] where the NIST was delegated the development of

a framework for the reduction of risks associated with this type of environments, with the support of the Government, industry and users.

The result of this work - after the publication of multiple preliminary versions and receipt of contributions from volunteers through the Request for Information (RFI) model - was the first version of the document "Framework for Improving Critical Infrastructure Cybersecurity", known as "NIST Cybersecurity Framework" which was released on February 12, 2014.

At the same time (2013) in the European Commission, ENISA first introduced the Network and Information Security (NIS) Directive [5] but it required to align 28 different sets of national cybersecurity agendas, and of securing a common view from the European Parliament that has somewhere between four and six major party groups, took considerably longer than the gestation of the Framework.

That's because the NIS directive started the implementation phase in 2017, and as of April 2020 it is still not possible to find any concrete content that can serves as a guide to implement any ISMS in an organization. The European directive entered in force in August 2016 and it has been transposed into each's EU member, but those transpositions are enumerations and brief descriptions of lines of action at high country levels, that are more oriented to national cyber security as global than to offer resources that a single company or organization can use. Some examples can be found following the links in the above table [6]:

EU MEMBER	LINK TO NIS TRANSPOSITION
Spain	https://www.dsn.gob.es/es/file/932/download?token=9-T_SSTE
Italy	https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf
France	https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf

Table 4: Examples of EU NIS transpositions

Meanwhile, the NIST CSF was undergoing its first major revision in 5 years based on changes in threat and experiences of global adopters.

In this situation, NIST CSF is the chosen framework to base the adherence to standards of the ProTego project.

II.2.2. Structure and implementation

The bases of the NIST CSF were established as the following:

1. Identify security standards and guidelines applicable across the board to all critical infrastructure sectors
2. Establish a common language to manage cybersecurity risks
3. Provide a prioritized, flexible, repeatable, neutral, performance-based and cost-effective approach based on business needs
4. Help managers and operators of critical infrastructure to identify, inventory and manage computer risks
5. Establish criteria for defining metrics to monitor performance in implementation
6. Establish controls to protect intellectual property, the privacy of individuals and civil liberties when cybersecurity activities are carried out
7. Identify areas for improvement that can be managed through future collaborations with particular sectors and organizations oriented to the development of standards

8. Do not introduce new standards when there are already developed initiatives that cover the objectives of the executive order.

And is the 8th point which promotes the link between other standards, as the subcategories (lower-level elements) point to controls to be performed, that can be conducted with the preferred standard (ISO, COBIT, NIST 800). Therefore, an organization does not need to adhere fully and only to one standard using all its defined controls, but it is allowed to choose the most suitable standard to perform each control, among the following:

- Control Objectives for Information and Related Technology (COBIT)
- Council on Cyber Security (CCS) Top 20 Critical Security Controls (CSC)
- ANSI / ISA-62443-2-1 (99.02.01) -2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program
- ANSI / ISA-62443-3-3 (99.03.03) -2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels
- ISO / IEC 27001: 2013, Information technology --Security techniques --Information security management systems --Requirements
- NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations

To better understand how it works:

Framework Core

It is a set of cybersecurity activities, expected results and applicable references that are common to critical infrastructure sectors, in terms of industry standards, guidelines and practices that allow the communication of cybersecurity activities and their results throughout the organization, from the executive level to the implementation / operation level.

To do this, it uses five fundamental functions:

Identify: Identify the organization's systems, assets, data and competencies, its business context, the resources that support critical functions and cybersecurity risks that affect this environment.

Protect: Protects and implements the necessary countermeasures and safeguards to limit or contain the impact of a potential cybersecurity event.

Detect: Allows to develop and implement the appropriate activities to identify the occurrence of a cybersecurity event through continuous monitoring.

Respond: Allows the definition and deployment of activities to react to an identified cybersecurity event and mitigate its impact.

Recover: Allows the deployment of activities for resilience management and the return to normal operation after an incident.



Figure 3: NIST CSF Functions

In turn, each of these functions is divided into categories as shown in the above figure:

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Procedures
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

Figure 4: NIST CSF Categories

And these categories divide themselves in subcategories that finally guide to the implementation of controls referred in international standards.

As NIST is a guideline it can be tailored to each organization, this is, organization is free to select those items (subcategories and referenced controls in the selected standard) that best fits its objectives.

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	· **CCS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	· **CCS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	· **CCS CSC** 1 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	· **COBIT 5** APO02.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	· **COBIT 5** APO03.03, APO03.04, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· **COBIT 5** APO01.02, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

Figure 5: NIST CSF Subcategories and informative references

Framework Implementation Tiers

Implementation tiers enable the organization to rank at a predefined threshold based on current risk management practices, the threat environment, legal and regulatory requirements, business objectives and mission, and the constraints of the company itself.

The ranges of the implementation levels are as follows:

- **Level 1 – Partial**: At this level, cybersecurity risk management practices are not formalized (ad-hoc) and generally act reactively. The prioritization of activities is not aligned with the organizational risk objectives, the threat environment or with business requirements. There is minimal external participation in terms of collaboration and information sharing.
- **Level 2 - Risk Informed**: At this level, risk management practices are approved by Management, but may not be established as a global policy. There are defined and implemented procedures and processes and qualified personnel. External participation is done informally.
- **Level 3 - Repeatable**: At this level, formal risk management practices are regularly updated as part of the application of analysis of changes in business requirements, threats or technologies. A formal collaboration framework with third parties has been established.
- **Level 4 - Adaptive**: Cybersecurity practices are based on lessons learned and predictive indicators derived from previous and current cybersecurity activities, through a process of continuous improvement to adapt to changes. These tasks are part of the organizational culture. It collaborates actively with third parties, sharing information on cybersecurity events.

Framework Profiles

Profiles are used to describe the current status and current profile of certain cybersecurity activities. The differential analysis between profiles allows the identification of gaps that should be managed to meet the risk management objectives.

For this, the definition of an action plan is required that includes a prioritization of activities depending on the business needs and risk management processes of the organization. This risk-based approach allows the organization to estimate the resources necessary (for example, personnel and funding) to achieve the established cybersecurity goals in a prioritized and cost-effective manner.

According to the previous descriptions, the global architecture of the cybersecurity framework would be as follows:

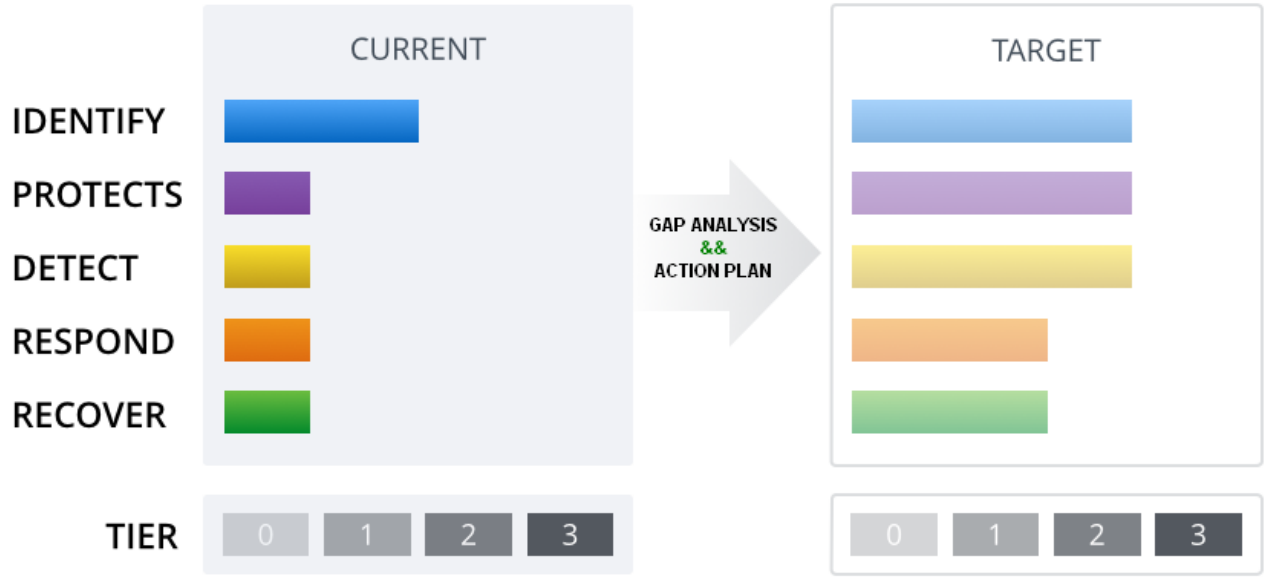


Figure 6: NIST CSF Profiles

How is CSF implemented?

The implementation of a CSF-based cybersecurity program consists of the following iterative steps:

Step 1 - Prioritization and scope definition: By identifying the business objectives and mission and high-level priorities in organizational terms, the control applicability environment is strategically decided. This environment can be the entire organization, a particular line of business or a process, bearing in mind that each of these elements may have different levels of risk tolerance.

Step 2 - Orientation: The systems, assets, regulatory requirements, threats and vulnerabilities related to the defined applicability environment are identified.

Step 3 - Create a current profile: Through the functions of the basic framework and using the categories and subcategories, the results of implementing controls in the environment are obtained.

Step 4 - Run a risk analysis: A risk analysis is carried out to determine the probability and impact of cybersecurity events in the analysed environment.

Step 5 - Create an objective profile: The objectives that the organization intends to cover in terms of cybersecurity are established.

Step 6 - Determine, analyse and prioritize the detected gaps: Through the differential analysis between the current profile and the objective profile, an action plan prioritized in terms

of cost / benefit is defined, which allows the determination of resources and improvement actions.

Step 7 - Implement the action plan: Proceed with the alignment of controls and deployment of improvements gradually and monitored.

All these actions must be implemented within a continuous improvement environment, allowing the organization to continuously optimize its security controls and scale to higher levels within the framework.

II.3. NIST CSF in ProTego

Within the NIST CSF, the subcategories and informative references are the elements that need to be measured and evaluated to define the current profile of the organization, and also it is needed to take decisions about the objective profile, in order to make possible to measure the gap and build the action plan.

Both the evaluation of the current profile of the healthcare organization and the definition of the objective profile are out of the scope of the ProTego project. In the first case because ProTego is providing a set of technical tools (toolkit) that are going to be incorporated to the organization's IT infrastructure, but it is the whole IT infrastructure that need to be analysed in the NIST CSF. In the second case because the definition of the objective profile has to be defined based on the resources and possibilities of the organization, and has to be defined by those who can provide the means to perform the emerging action plan. For this reason, it is highly recommended that before starting any strategy, the CISO takes as a fundamental goal the appropriate awareness of the organization managers, because they are who must provide the resources needed and, thus, will implicitly decide the scope of the ISMS.

Nevertheless, the aim of the ProTego project is to develop data-protection toolkit reducing risks in hospitals and care centers and because of that the toolkit and educational framework will be of utility to improve a subset of the NIST CSF items. The following table identifies the NIST CSF items that will be impacted in an organization that incorporates the ProTego toolkit and educational framework to its IT map, or in other words, the items that the ProTego project will help to improve by facilitating to accomplish the related controls:

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1**: Asset vulnerabilities are identified and documented	**ISO/IEC 27001**:2013 A.12.6.1, A.18.2.3
		ID.RA-3: Threats, both internal and external, are identified and documented	**NIST SP 800-53** Rev. 4 RA-3, SI-5, PM-12, PM-16
	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1**: Identities and credentials are managed for authorized devices and users	**ISO/IEC 27001**:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3
		PR.AC-3: PR.AC-3: Remote access is managed	**ISO/IEC 27001**:2013 A.6.2.2, A.13.1.1, A.13.2.1

PROTECT (PR)		**PR.AC-4**: Access permissions are managed, incorporating the principles of least privilege and separation of duties	**ISO/IEC 27001**:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4
		PR.AC-5: Network integrity is protected, incorporating network	**ISO/IEC 27001**:2013 A.13.1.1, A.13.1.3, A.13.2.1
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1**: All users are informed and trained	**ISO/IEC 27001**:2013 A.7.2.2
	Data Security (PR.DS): Information and records (data) are managed	**PR.DS-1**: Data-at-rest is protected	**NIST SP 800-53** Rev. 4 SC-28
		PR.DS-2: Data-in-transit is protected	**ISO/IEC 27001**:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
		PR.DS-5: Protections against data leaks are implemented	**ISO/IEC 270**01:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1**: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	**ISO/IEC 27001**:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	**ISO/IEC 27001**:2013 A.9.1.2

DETECT (DE)	**Anomalies and Events (DE.AE)**: Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-2**: Detected events are analyzed to understand attack targets and methods	**ISO/IEC 27001**:2013 A.16.1.1, A.16.1.4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	**NIST SP 800-53** Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-4**: Event detection information is communicated to appropriate	**ISO/IEC 2700**1:2013 A.16.1.2
RESPOND (RS)	**Improvements (RS.RP)**: Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.RP-1**: Response plan is executed during or after an event	**ISO/IEC 27001**:2013 A.16.1.5
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1**: Response plans incorporate lessons learned	**ISO/IEC 27001**:2013 A.16.1.6
RECOVERY (RC)	**Recovery Planning (RC.RP)**: Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1**: Recovery plan is executed during or after an event	**ISO/IEC 2700**1:2013 A.16.1.5

Table 5: ProTego-related items within the NIST CSF

For each subcategory, the NIST CSF provides various informative references to choose among them. In this document, the ISO/IEC 27001 has been chosen whenever possible as the preferred option.

The previous table has identified the NIST CSF items that are included in the scope of ProTego. The description of the controls regarding each item (subcategory) and the feature that ProTego toolkit makes possible to perform such controls are described below.

ID: 1

Subcategory: ID.RA-1: Asset vulnerabilities are identified and documented

Controls: ISO/IEC 27001:2013 A.12.6.1

Description: Management of systems audit controls - Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

ProTego Feature: ProTego includes the System Security Modeller (SSM) where the assets and the processes of a given IT system are identified generating a System Model of that. SSM provides the means to automatically identify cyber security and compliance threats and get help on how to address those threats by suggesting potential preventative controls. The domain model of SSM is subject to constant refinement to incorporate new system modelling requirements and new threats and can be updated in an SSM installation by its administrator. ProTego toolkit is able to retrieve information on software vulnerabilities and revaluate risks at runtime.

ID: 2

Subcategory code: ID.RA-3: Threats, both internal and external, are identified and documented

Controls: NIST SP 800-53 Rev. 4 RA-3, PM-12

Description: RA-3: Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

PM-12: To establish insider threat programs. The standards and guidelines that apply to insider threat programs that include security controls to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns

ProTego Feature: SSM allows to conduct risk assessments, including the likelihood as a parameter to determine the magnitude of harm. The System Model acts as centralized point of analysis. It will take as entry the technical information gathered by the SIEM that will detect information that needs to be analysed based on the policies defined by the organization.

ID: 3

Subcategory: PR.AC-1: Identities and credentials are managed for authorized devices and users

Controls: ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3

Description: A.9.2.1 User registration and de-registration - A formal user registration and de-registration process shall be implemented to enable assignment of access rights.

A.9.2.2 User access provisioning - A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.

A.9.2.4 Management of secret authentication information of users - The allocation of secret authentication information shall be controlled through a formal management process.

A.9.3.1 User responsibilities - To make users accountable for safeguarding their authentication information

A.9.4.2 Secure log-on procedures - Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure

ProTego Feature: In ProTego this is done via the Identity & Access Management (IAM) system of the hospital. The design of the access control and key management system enforces that the

identities and credentials of all authorized devices and users are registered and managed by these IAM systems. The reason for this is that the access control system requires a valid authorization token for each data access. These tokens will be issued by the IAM systems in place. By not introducing new IAM and being able to integrate with the already existing one, ProTego collaborates towards the centralization of the credentials management and access policies.

ID: 4

Subcategory: PR.AC-3: Remote access is managed

Controls: ISO/IEC 27001:2013 A.13.2.1

Description: A.13.2.1 Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities

ProTego Feature: Data stored in external storage is encrypted. In order to decrypt the data, one needs to get the decryption key from the KMS. The KMS will only send the decryption key to the data gateway via a secure channel, and will only do this if a valid authorization token is presented to the access control system, and when the remote data access is granted by the access control system (based on the content of the token and the security policies in place).

ID: 5

Subcategory: PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties

Controls: ISO/IEC 27001:2013 A.6.1.2

Description: A.6.1.2 Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets

ProTego Feature: The goal of the access control system is exactly to manage and enforce the access permissions to data assets.

ID: 6

Subcategory: PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate

Controls: ISO/IEC 27001:2013 A.13.1.1, A.13.1.3

Description: A.13.1.1 Network controls - Networks shall be managed and controlled to protect information in systems and applications

A.13.1.3 Segregation in networks - Groups of information services, users and information systems shall be segregated on networks.

ProTego Feature: Network Slicing technology allows the definition of segregated slices within a communication channel, providing isolation and ensuring the allocation of resources needed.

ID: 7

Subcategory: PR.AT-1: All users are informed and trained

Controls: ISO/IEC 27001:2013 A.7.2.2

Description: A.7.2.2 Information security awareness, education and training- All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

ProTego Feature: Educational Framework developed in ProTego covers the required training to different categories of users, addressing different needs. For health staff it focuses on cybersecurity awareness, while IT staff will be trained on more technical details to allow a proper deployment of the toolkit and the included security features.

ID: 8

Subcategory: PR.DS-1: Data-at-rest is protected

Controls: NIST SP 800-53 Rev. 4 SC-28

Description: SC-28: The information system protects the confidentiality and integrity of the information at rest. The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of information on information system components.

ProTego Feature: Apache Parquet based encryption system ensures the confidentiality and integrity of the data at rest. To prevent unauthorized accessions, accesses will only be performed with the grant of the KMS. To ensure integrity, any file tampering will be detected and raise alerts to advice of such situation.

ID: 9

Subcategory: PR.DS-2: Data-in-transit is protected

Controls: ISO/IEC 27001:2013 A.13.1.2

Description: A13.1.2 Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced

ProTego Feature: The definition of slices supported by Network Slicing provides isolation in terms of both confidentiality and performance. It allows the definition of service levels according to the needs of each slice.

ID: 10

Subcategory: PR.DS-5: Protections against data leaks are implemented

Controls: ISO/IEC 27001:2013 A.9.1.2, A.9.2.3, A.9.4.1, A13.2.3

Description: A.9.1.2 Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

A.9.2.3 The allocation and use of privileged access rights shall be restricted and controlled

A.9.4.1 Access to information and application system functions shall be restricted in accordance with the access control policy

A13.2.3 Information involved in electronic messaging shall be appropriately protected

ProTego Feature: The combined features of ProTego toolkit minimizes the possibility of a data leak due to:

- the protection of data in transit provided by the network slices
- the protection of data at rest provided by the parquet data encryption
- the protection against not allowed access to data, provided by the access control system
- the client device control provided by the continuous authentication
- the threats detection mechanisms provided by the SIEM

ID: 11

Subcategory: PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

Controls: ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3

Description: A.12.4.1 Event logging - Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

A.12.4.2 Protection of log information - Logging facilities and log information shall be protected against tampering and unauthorized access

A.12.4.3 Administrator and operator logs - System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

ProTego Feature: ProTego SIEM provides a centralized point for systems, services, and application logging. So even if a host is somehow compromised and the logs tampered, they will still be available in the SIEM. The communications between the hosts producing the logs and the SIEM are encrypted to prevent to maintain the Integrity and Confidentiality needed. The regularity of the review process has to be defined by each organization.

ID: 12

Subcategory: PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality

Controls: ISO/IEC 27001:2013 A.9.1.2

Description: A.9.1.2 Access of networks and network services - Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

ProTego Feature: Data stored in external storage is encrypted. In order to decrypt the data, one needs to get the decryption key from the KMS. The KMS will only send the decryption key to the data gateway via a secure channel, and will only do this if a valid authorization token is presented to the access control system, and when the remote data access is granted by the A.C. (based on the content of the token and the security policies in place). Without a valid token, one cannot access the data.

ID: 13

Subcategory code: DE.AE-2: Detected events are analyzed to understand attack targets and methods

Control: ISO/IEC 27001:2013 A.16.1.1, A.16.1.4

Description: A.16.1.1 Responsibilities and procedures - Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.

A.16.1.4 Assessment of and decision on information security events - Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

ProTego Feature: Security incidents and management has to be defined in the security policy of each organization. To define security policies, it's recommended that both, IT department and the other administration and management departments of the hospital, participate. Rules extracted from the security policies can be applied as rules in the ProTego SIEM to detect those compromising situations.

ID: 14

Subcategory: DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors

Controls: NIST SP 800-53 Rev. 4 AU-6, CA-7, SI-4

Description: AU6: Reviews and analyses information system audit records for indications of inappropriate or unusual activity and reports findings to appropriate personnel or roles. The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. The organization analyses and correlates audit records across different repositories to gain organization-wide situational awareness. The information system provides the capability to centrally review and analyse audit records from multiple components within the system.

CA7: The organization develops a continuous monitoring strategy and implements a continuous monitoring program.

SI-4: The organization monitors the information system to detect attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives and unauthorized local, network, and remote connections.

ProTego Feature: ProTego SIEM provides the mechanisms to collect, store, correlate, and analyse in a centralized location. Metrics and frequencies can be defined by the organization.

ID: 15

Subcategory: DE.DP-4: Event detection information is communicated to appropriate parties

Controls: ISO/IEC 27001:2013 A.16.1.2

Description: A.16.1.2 Reporting information security events - Information security events shall be reported through appropriate management channels as quickly as possible.

ProTego Feature: ProTego SIEM provides the means to report alerts. These alerts will be defined by each organization and may be shown in a dashboard as well.

ID: 16

Subcategory: RS.RP-1: Response plan is executed during or after an event

Controls: ISO/IEC 27001:2013 A.16.1.5

Description: A.16.1.5 Response to information security incidents - Information security incidents shall be responded to in accordance with the documented procedures.

ProTego Feature: By the integration of the SSM and the SIEM, the ProTego toolkit will also provide decision support information at run-time for the security operators. The information will help them better understand the current risk level and how to respond to an attack suggesting some reactive control strategy, e.g., disablement of an asset.

ID: 17

Subcategory: RS.IM-1: Response plans incorporate lessons learned

Controls: ISO/IEC 27001:2013 A.16.1.6

Description: A.16.1.6 Learning from information security incidents - Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.

ProTego Feature: The Domain Model can be refined by adding new information and knowledge gathered from previous incidents.

ID: 18

Subcategory: RC.RP-1: Recovery plan is executed during or after an event

Controls: ISO/IEC 27001:2013 A.16.1.5

Description: A.16.1.5 Information security incidents shall be responded to in accordance with the documented procedures.

ProTego Feature: Despite the recovery must be defined by each organization, the ProTego toolkit has intrinsic features that may improve its success. First of all, it helps to maintain an inventory of digital assets, which is a basic must. Then, the integration platform based on kubernetes cluster allows an easy and fast recovery of the infrastructure (via ansible scripts) applications (via helm chart deployments) and the data, as the parquet encrypted files can be used as a centralized medical data repository thus minimizing the recovery tasks.

III. PEOPLE-CENTRIC SECURITY MODEL

There is a gap between attitudes and actual behaviour about data privacy and, thus, information security, and the People-Centric security model has been chosen in ProTego as base framework for the training program to reduce that gap and increase its effectiveness.

To better explain the previous mentioned gap: most individuals, when asked or surveyed, affirm that data privacy is a primary concern, but their behaviour is not coherent with that idea: they reveal personal information for small rewards, like discounts on purchases, access to websites or small gifts. This dichotomy of information privacy attitude and actual behaviour has been coined the term “privacy paradox” (Brown, 2001; Norberg et al., 2007) [8] or, to be more accurate, “information privacy paradox”.

This situation that has been documented through different empirical experiments as "*Privacy Choices Behavioural Economics Review*" conducted by Sören Preibusch in 2015 [9], or "*Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon*" by Spyros Kokolakis in 2017 [10].

This reality is materialized in more customary practices that have implications on cybersecurity as well: users from healthcare staff are aware about the password policies regarding length and strength and in the survey executed in ProTego Deliverable 3.1, it was concluded that the most of the MS staff that responded to the survey were able to find and remember strong passwords. But if those good practices are not applied outside of the work environment, it would be risk due to the BYOD trend, that causes private and working environments interlace each other.

This reveals the necessity of reduce that divergence between attitude and behaviour and that is only possible through a change of mentality.

To explain how we get to this point it is needed to look at the evolution of Information Security.

III.1. Evolution of information security

First wave: when it first appeared, IS was "Technology-centric", meaning that in that time the main points were algorithms, systems and protocols. The main contributors to this were STEM (Science, Technology, Engineering and Mathematics) that tried to come up with **technical artifacts**. This was the first wave. And how they were used takes us to the second wave.

The **second wave** was "Economic-Centric": once those technical artifacts were available, **cost and benefit parameters** were attached to it, to maximize payoffs and minimize cost. In this phase optimum policies were developed. The main contributors were classic economists and science management science experts. And in this phase, it was developed optimum security incentive mechanisms, **policies and regulations**.

But obviously from the earlier examples showing real cases regarding the privacy paradox, something was lacking. Technology and optimum design of policies were still not sufficient. What is lacking? To explain this, it is needed to observe this matter from a different angle, from the angle of people that attack systems.

Kevin Mitnick was one of the most famous hackers and he currently works as a security consultant. He stated that "*Companies spend millions of on firewalls and secure access devices, and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer and operate computer systems*" [11].

People that have a direct relation with the systems have to perform decision making in the real world. They can follow or not the recommendations stated in the policies. And that's de main focus of this **third wave**: **design and offer technology and policies that regular people** not only understand and agree with, but also **be able, capable and willing to use**.

The main contributors to this third wave are phycology, neuroscience, behavioural economics and sociology, that is, all the fields that will affect decision making. And the goal of this new wave of Information Security will be developing technical artifacts and protocols that will be actually used.

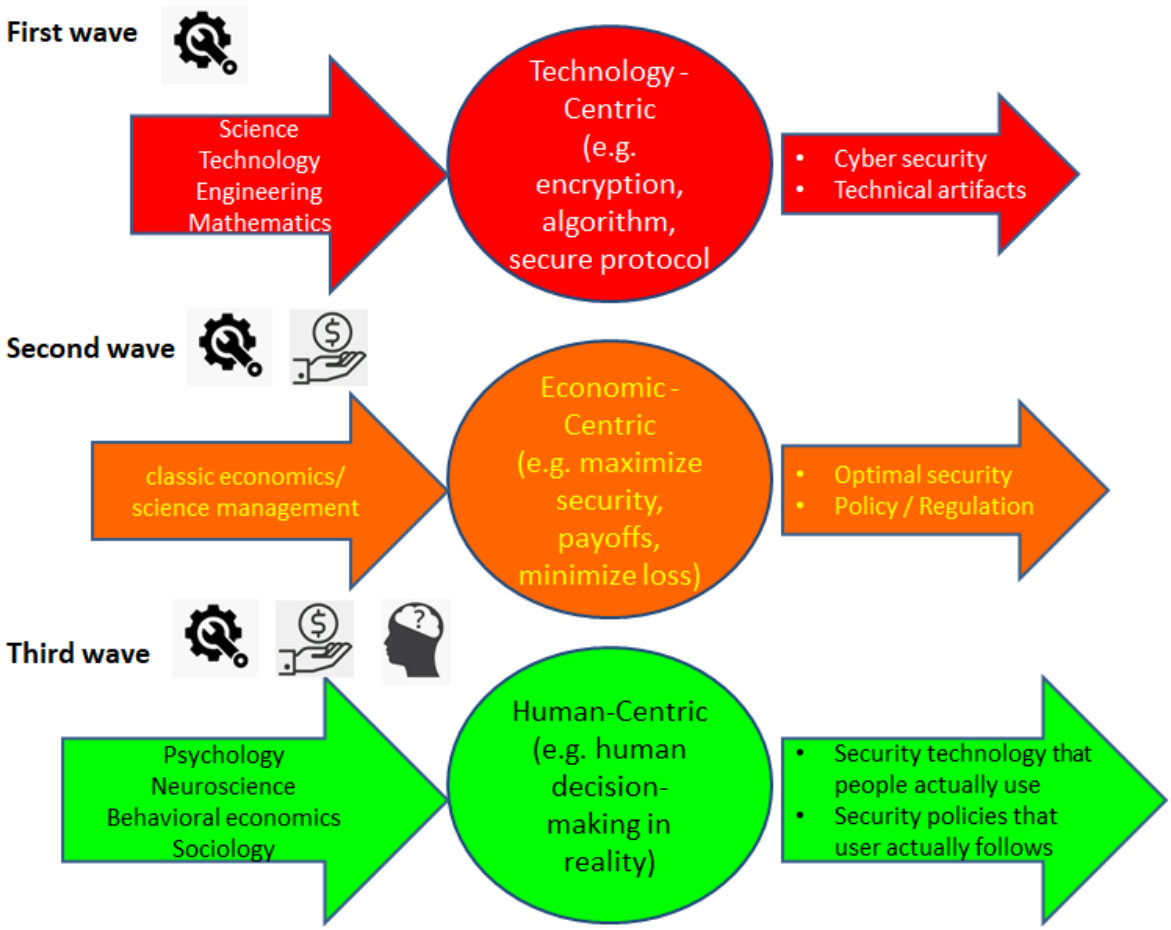


Figure 7: Three waves of Information security

III.2. Cybersecurity in the organization

From the psychological approach suggested by the third wave of Information Security we can extract some basis that will surround the design of the ProTego educational framework. The main objective is to actually engage people and probably the main challenge is to achieve that in the healthcare sector, which is a particular sector in terms of its final users because the most of them are health staff and they have been historically focused in patient safety and right care [12], deep-seated concepts that have never included cybersecurity concerns. Technology, applications and cybersecurity are considered tools that hospital's support services (as IT department) must provide and that are completely out of physician's scope: physicians, nurses and health staff in general must care about "*material safety*" and IT department about "*virtual safety*".

Cybersecurity is about people

First concept is that cybersecurity is about people because it is created as a result of the interactions between people and technology. Without technology, cybersecurity would not have anything to protect. And without people nobody would try to attack IT systems. Is this intersection that creates and necessitates security.



Figure 8: Cybersecurity scope

If each side of that equation is forgotten, it likely ends up without a good security solution in the organization. If we only have the security to technology but we don't address the people element, people would try to circumvent defined policies because they don't understand whether important, and on the contrary if technology is not addressed even the best policies can't protect unsecure systems by design.

Culture as a system

Culture is a fundamental portion of keeping an organization secure. It defines a complex social system, encompassing the behaviours, traditions, values, and interpersonal dynamics of a group. Its major inputs are shared norms, values, routines, and what the business reward or punishes. And its major outputs are user behaviours, employee retention and organizational health.

The goal is to create those unseen incentives and disincentives that promote the desired cybersecurity behaviours.

We can use drives or incentives towards the goal of getting staff to do certain things, in these three lines:

- Economic: we can introduce monetary bonus incentives if and only if, we can define measurable indicators that allow to objectively evaluate the achievement ratio. For example, if they attend to cybersecurity awareness trainings, the response to phishing simulation campaigns, the result of information security internal audits to different sections, etc.
- Social: this is about how the cybersecurity is perceived in the organization. Is it a roadblock or an enabler? A good example for this is when early on IT people started to talk about cloud. Many organizations decided it was not a possibility at all because of information security. This is an example of "*culture of no*". But instead of it, other companies decided to "*create a culture of yes*". They decided to open themselves to this new technology and create policies to address risks.
- Moral: this concept treats of mutual trust with users. Are users incentivized to report things that they think are relative to security violations? Or do they fear to be punished or shamed if they report that? We obviously want users that report because one of the main problems is that attacks remain undiscovered for a long time or even they are never discovered.

All these drivers work together and have unforeseen effects that can make that the same worded policy would be accepted completely different in an organization.

Communication in the organization

It is also important how we communicate about information security in the organization. This communication can be explicit but also implicit in the actions and decisions taken.

It is not about power: If any cybersecurity initiative is taken into an organization, it is very important that it would be applied from the top level of the organization. It is a usual error that just before a system is going live one of the terms discussed is whether or not the managers (e.g., CEO and directors) will consent on being applied by the security concerns, rules and protocols. And that is an error because if we have leaders talking about security but make themselves exceptions to the rules, it launches a message that security is about power: if you have power enough you are out of the scope of cyber security. And it is easy to imagine how different it is if the CEO not only talks about security but is also subjected to the same rules than the rest of the organization: that launches the message that cybersecurity is so important that nobody is about it.

It is not a lost cause: cybersecurity initiatives must not be approached with the objective of being completely safe. As many experts affirm, it is inevitable to fall victim of a cyberattack. There is no phishing simulation campaign where at least one people clicks the malicious link. There is no way to be out of it, but what can make the difference is how we deal with that, how do we respond to that vulnerability. If staff feels worried about being punished rather than encouraged to report breaches, it is a dangerous situation because security can be compromised and nobody is taking actions because the breach would not be detected. But if that is not assumed as a lost cause and a culture is created in the organization where nobody fears about punishment for a potential breach but rather staff feel incentivized to report immediately, the exposition time is minimized and the problem can be fixed with a minimized impact.

How cybersecurity often makes users feel can be illustrated with a phrase from the film WarGames (1983, John Badham) [13]: "*A strange game. The only winning move is not to play.*", and that is what should be avoided.

Make it easy: The easiest the cybersecurity mechanisms are, the higher adoption they will have into an organization. And taking it to the extremes, if users ran into a problem using a process, they will probably just ignore it. This idea can be illustrated with the example of the lock screen systems in phones. Several studies [14] demonstrated that the ratio of users that lock their device if it is equipped with biometric systems (fingerprint, face id) is higher than the same on devices that don't have these capabilities. Here the important point is not if those biometric systems have vulnerabilities or not (as it has been proved they have) but it is always better locking the screen that keeping it unlocked. That is, the best security mechanisms are those that are adopted by users. Here the message is that don't let perfect security obstructs good security.

Make cybersecurity team visible: In most organizations, cybersecurity team is an abstract person or team that users receive emails from, often to punish regarding some incorrect behaviour, or to give instructions perceived as obstacles to the job. To change that situation, it is a good idea that those people (cybersecurity team) will be known by the rest of the organization, that users can put face to that person or team, and understand that their job is to keep them safe. It is a psychological factor, human have a cognitive bias towards people we trust or people that we don't.

Teach differently: like in traditional education the difference between having a passionate teacher that explains why you should care about what you are learning and not only pay attention to what you are learning makes the complete difference. And for people whose job is not so related to cybersecurity (like health staff) repetition is very important. As it is not feasible to repeat the training sessions quite often, this repetition can be achieved by making cybersecurity more present, by creating visual material as posters, digital banners, etc. with key concepts that refers to the main subjects of the training sessions, and place it in physician work places, corporate intranet, etc.

III.3. People-Centric Security model

The cybersecurity awareness strategy for final users designed by ProTego is based on the People-Centric Security (PCS) model. Within the following sections the model will be presented and its concrete adaptation to ProTego.

This model aims to achieve an effective cybersecurity culture within the healthcare organization, increasing the global level of cybersecurity and reducing the risk of incidents directly related to one of the key components in this matter: people.

It is framed within a cybersecurity management strategy in which people play an active and relevant role, acquiring responsibilities in the management of the information they handle. To define this new cybersecurity management model Gartner has coined the term "*People-Centric Security*" [15].

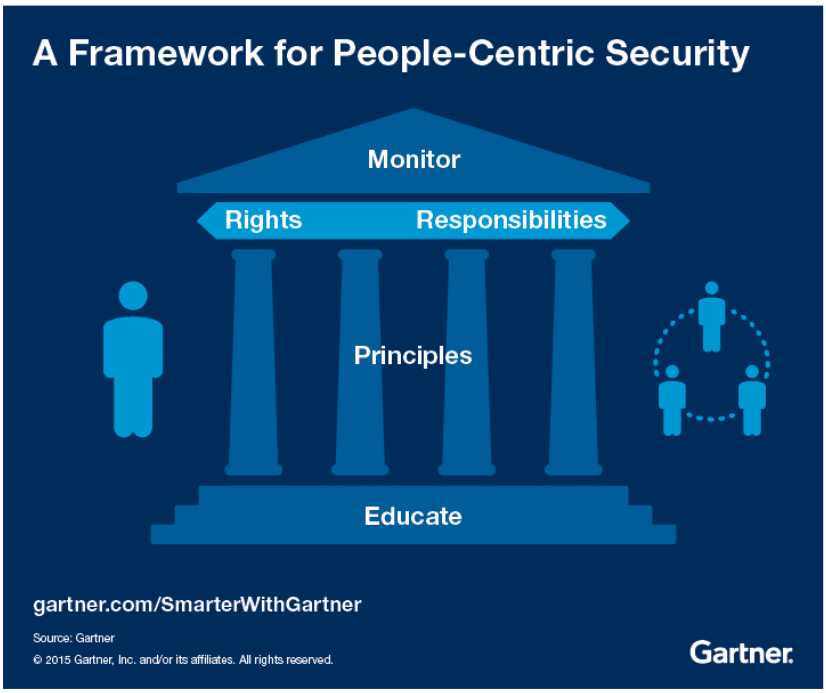


Figure 9: Concept of Gartner's People-Centric Security

In keeping with this name, PCS is a strategy in which the person has rights and responsibilities in the cybersecurity management of the technologies they use and the information they manage through them, and must manage the associated risks.

PCS aims to make the people who work in an organization part of its line of cyber defence: "human firewall". To achieve this objective the framework defines three main lines of work:

- **Training**: Provide the person with the attitudes and skills necessary to carry out adequate risk management.
- **Personal risk management**: Definition of an appropriate methodology that allows people to carry out practical and effective risk management.
- **Monitoring**: Continuous review of risk management carried out by each person who works in the organization.

Training is the most essential part of this strategy: it is necessary to approach the training of people so that they can adequately manage the risks that affect them through continuous awareness-raising and training. In the PCS model training splits in three sections:

- Awareness: Through awareness it is about involving the person in the protection of the technologies and information it manages. To do this, it shows people the threats they face and their possible impact, making them understand why they must properly manage cybersecurity.

- Training: Through training, the necessary knowledge is transferred to people to put into practice adequate cybersecurity management. They are trained in how to do it.
- Simulation: By executing training actions, people are helped to keep their knowledge up to date in order to effectively manage risk

In ProTego, an awareness program has been designed to improve correct behaviours in cybersecurity (see Section IV). Training and simulation are not suitable in the most of healthcare organizations because clinical resources are precious and limited, and increase awareness is the basic element that should be performed, as a synonym of “understand why”. From this point other objectives can be examined, as more specific trainings with a deeper technological component.

IV. EDUCATIONAL MATERIAL FOR HEALTH STAFF

It is a globally accepted fact that the contents in education need to be adapted to those they are addressed to. In this case the objective people are health staff that has its own particularities. In this concrete scope, to impart a right awareness training is about:

- designing the right content: every possible item that can be included in a cybersecurity training can't be covered so it is needed to select and cover those contents considered more relevant and that keep attenders connected and interested.
- demanding the right effort: it is known that health staff perceive any issue outside of healthcare as an extra content that should probably not be addressed to clinical personnel. Therefore, any training program should mind the time required to be attended. In the case of ProTego, it is about 90 minutes, including the consumption of the main material (videos and printable tips) and the response to the survey to assess the quality of the material.
- communicating through the right channel: for clinicians in general and physicians in particular it is a proven fact that their perception and understanding of any matter get better if it is transmitted from a colleague, this is, from another physician. This strategy has been followed in many healthcare organizations by involving clinical key users in relevant IT committees, where they are the receptors of the change requests, prioritize them and communicates to the rest of the health staff. This strategy is going to be followed in ProTego, involving the heads of clinical services in the communication strategy, so the final users perceive this awareness program more related to their clinical responsibilities. Besides that, the main topics have been spread in the shape of short educational videos in an educational website, which will be later explained and makes it more easy to be attended/consumed.
- making messages persistent in time: cybersecurity awareness program should not be a sort of technical training where you are teaching someone about how to do a concrete task to reach a touchable or a least countable objective. This is about impress the necessity of perform correct behaviours that are not mandatory to reach the objective, and that is the point: users don't necessarily need to apply the right behaviours to reach their goals, but even so we need them to feel the necessity to act correctly. And for this objective is important that the messages transferred become persistent. And this has been addressed by the creation of reminders with visual and direct messages that make users remember the concepts treated in the training.

IV.1. ProTego educational website

In addition to the previous concerns, one of the major concerns to be observed and which is vital for the success of the rising awareness program is the number of people that get the messages, that is, that consumes the training material. To maximize this indicator the educational material has been developed in the shape of an on-line educational website placed at https://protego-project.eu/cybersecurity/. This alternative improves accessibility compared with regular training sessions scheduled at fixed times because:

- The material is fully available and anyone can access it at the preferred time
- The users can review it during different sessions, dedicating just a few minutes each time
- The material can be used as many times as the user needs
- As users that consumed it would recommend it to new users, they can also use it by their own and at their preferred time
- As it is a public website, it is not limited to the health staff of a concrete hospital, and the training material can be consumed by patients and general public.

The educational material created addresses the four main topics to cover:

1. The good employee
2. Safe passwords
3. Social engineering
4. Mobile devices

The contents of each section will be later described. For each section it includes:

a) A short and easy-to-consult video, as the main item, specifically designed to make it easy to understand for non-technical attenders, and adjusted to three minutes of duration. The videos make use of '*personas'* archietipical users from various groups so not only health staff but any of the employees can feel identified. The following figure illustrates the videos look and feel:

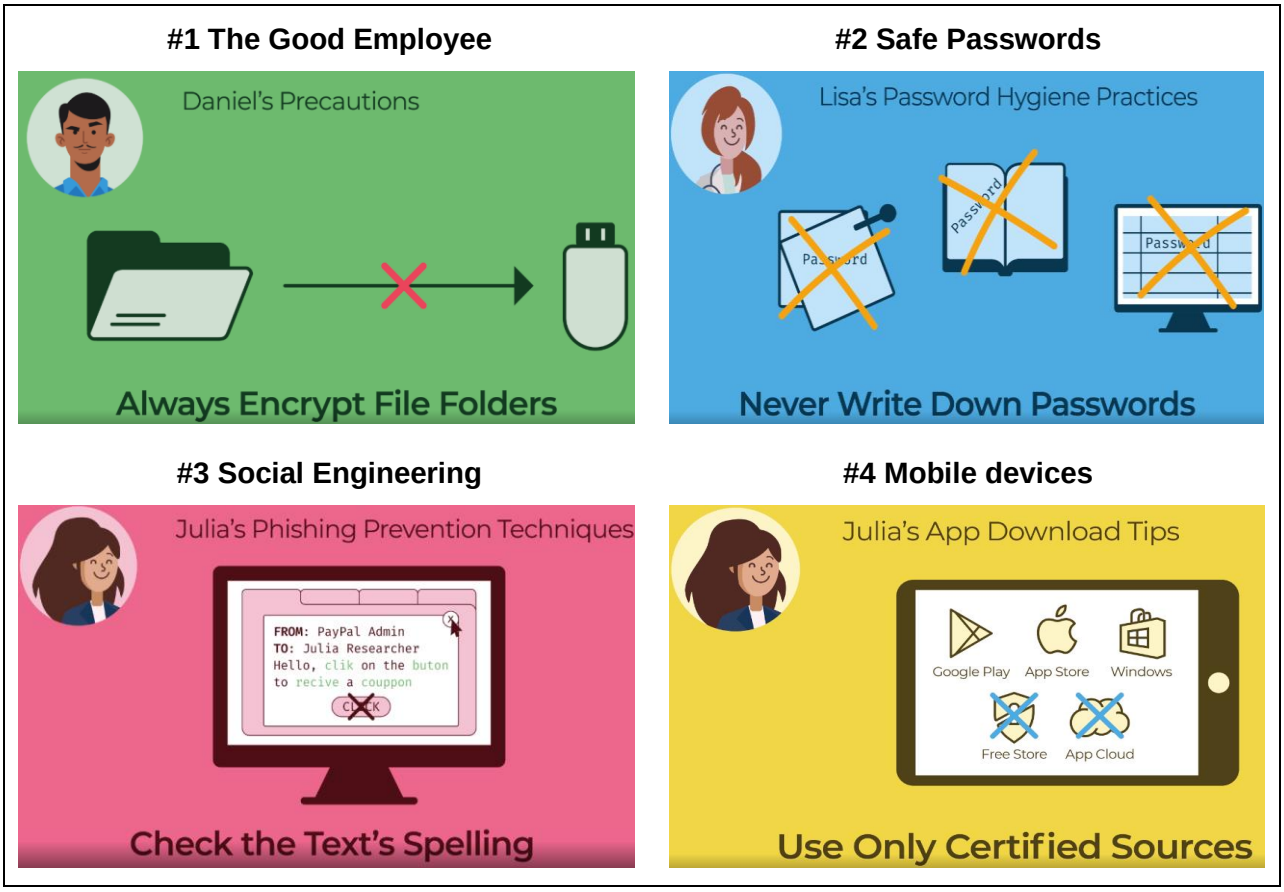


Figure 10: Screenshots of the educational videos

b) A printable PDF containing the main tips explained on each video, that can be physically printed and placed as remainder at the workplace.

#1 The Good Employee



#2 Safe Passwords



#3 Social Engineering



#4 Mobile devices



Figure 11: Printable tips

c) Links to external internet sites where the attender can go deeper on those concepts introduced in the videos. The following table explains the topics covered in links provided for each section:

#1 Links for "The Good Employee"	#2 Links for "Safe Passwords"
➢ Intranet of the hospital where the internal policies are explained ➢ How to remove metadata from files (Windows and Mac) ➢ How to encrypt files (Windows and Mac)	➢ How to choose strong passwords ➢ Password managers ➢ Enable two factor authentication (Windows and Mac)
#3 Links for "Social Engineering"	**#4 Links for "Mobile devices"**
➢ Keep safe during teleworking ➢ Deepen the knowledge on social engineering attacks ➢ Spot phishing emails	➢ How to control apps permissions (Android and IOS) ➢ Best antivirus for mobile devices (Android and IOS)

Table 6: Educational external links

Finally, a link to a survey has been included. The content of the survey is addressed to two different objectives:

- Elicit the opinion of the attender about the material provided, in terms of easiness of consumption and understanding.
- Allow to obtain the Risk Awareness Profile to assess the impact of the training over the health staff behaviours

As part of the material provided, printable posters have been designed as well, used to disseminate the educational website. The posters, included in the following figure, include a QR code that can be read with a bar-code scanner of a mobile device and takes the user to the educational website. The posters have been spread across the two hospitals (MS and OSR), placed at physical places commonly used by health staff.



Figure 12: Dissemination posters

IV.2. Execution of the training program

The correct execution of the training program implies a top-down communication process to ensure required resources and engage participants. The following table resumes the plan:

STEP ID	NAME	PARTICIPANTS TO ENGAGE	OBJECTIVES
1	Kick-off meeting	Organization managers	Communicate the awareness training plan. Ensure material and personal resources.
2	Engage clinical managers	Managers of clinical services	Prepare first communication for final recipients by clinical managers

3	Present training to users	Health staff	Present cybersecurity training as a clinical subject
4	Use the training material	Health staff	Explain risks derived from user's normal behaviour. Teach how to act to avoid those risks.

Table 7: Phases of awareness program for health staff

This is the explanation of each step:

- Communicate to organization managers: First of all, it is important to advice organization managers to ensure the clinical resources needed will be available, mainly those referring to clinical managers as head of medical services.
- Engage clinical managers: Then it is needed to engage heads of medical services. The first talk to the final receptors of the training will be given during a clinical session, so the final recipients understand it as a clinical concern.
- Present training to users: Clinical managers will introduce the training program to the final recipients (health staff). They have to explain the importance of cybersecurity, highlighting:
    - Healthcare as a main target for cyber criminals due to the increasing price of the health related data in the black market.
    - Dimensions of information security (Integrity, Availability, confidentiality) and explain examples of risks associated to each of them.
    - Cybersecurity is not only a technical matter, it is also part of health staff responsibilities

  Section Block 0: Introduction will describe this more in depth and can be used as a guide for the introductory speech.
- Use of the training material: Once the educational program has been introduced, the health staff can access the ProTego educational website. To facilitate this, they can access it by scanning the QR code in the posters, and in addition an email communication campaign has been spread to all the employees with a link to the website.

IV.3. Contents of the training program

IV.3.1. Block 0: Introduction

This section will be used during the introduction made by the clinical managers to the health staff to put this training in context. It is important to understand why the information security is essential in healthcare, and it is closely linked to interest of cyber criminals on healthcare information and the severity of the impact that security breaches may have.

Healthcare organizations are special targets for cyber criminals due to the high value of healthcare information on the black market. Healthcare services are expensive and being able to identify potential customers would be a high valued item for companies. In addition, any other information about individuals has or may have caducity: credit card numbers, addresses, even names or passport numbers can be changed. But biometrical and medical information is stored as part of the citizen personality and accompany them forever.

The previous is the most immediate reason we can think of when trying to imagine why somebody would perform a cyber-attack against a hospital. But technology has evolved and each time its presence, and thus impact, is greater in every single healthcare workflow.

To better explain this idea, we're going to introduce the concept of dimensions of information security and the impact that a breach on each of them can have on the patient's safety.

The three main components (also called dimensions) of information security are confidentiality, integrity and availability. These three components put together conform the CIA triad [16] which is a security model created to guide information security policies within an organization.

- **Confidentiality:** Confidentiality is the security principle that controls access to information. It is designed to ensure the wrong people cannot gain access to sensitive information while ensuring the right people can access it.

Access to information must be restricted only to those who are authorized to view the required data. Data can be categorized according to the type and severity of damage that could happen to it should it fall into unauthorized hands. According to these categories, strict measures can then be implemented.

Protecting confidentiality may also include special training for those who share sensitive data.

Strong passwords and password-related best practices must be used as well as information about social engineering attacks to prevent them from unwittingly avoiding proper data-handling rules and potentially causing disastrous results.

An example of a method used to ensure confidentiality is the use of data encryption. Two-factor authentication is now becoming the norm for authenticating users to access sensitive data, while user IDs and passwords should be considered standard practice.

Users should also be cautious to reduce the number of places where the information appears and where sensitive data is transmitted in order to complete a transaction.

Healthcare information has the highest level of sensibility because the unauthorized access or diffusion of healthcare information may cause serious social detriments as denegation of insurances, barriers to access jobs or social discriminations.

- **Integrity**: The second component of the triad, integrity assures the sensitive data is trustworthy and accurate. Consistency, accuracy, and trustworthiness of data should be maintained over its life cycle. Sensitive data should not be altered in transit, and security measures, such as file permissions and user access controls, should be taken to make sure that it cannot be modified by unauthorized users. To ensure this dimension of information security, there are other technical strategies to put in place as cryptographic checksums for verification of integrity and backups or redundancy plans to be able to restore any affected data in case of integrity failure or security breach in order to restore data back to its correct state.

To understand the impact that a breach on the integrity dimension may have it is important to be aware of that the most of the clinical decisions are taken based on antecedents and the falsification of that information may lead to wrong decision as inadequate drug prescription, wrong diagnosis, etc. That risk is getting higher with the inclusion of automated or semi-automated CDSS

- **Availability**: Availability is the guarantee of reliable and constant access to sensitive data by authorized people. It is best guaranteed by properly maintaining all hardware and software necessary to ensure the availability of sensitive data. In addition, organizations should provide disaster recovery plans with safeguards against interruptions in connections and data loss, considering unpredictable events such as a fire or a natural disaster.

The unavailability of healthcare information may preclude the adequate provision of healthcare services. This risk is higher as the organization is more IT dependent, what use to come with the process integration and efficiency. It might make impossible the provision of services or obligate to take decisions without all the required information, which may lead to errors in the provision of appropriate cares and health services in general.

The APENDIX_A includes the slides that could be used to help explain these concepts with visual support.

IV.3.2. Block 1: The good employee

This is the first block of content included in the ProTego educational website. It covers general topics that hospital employees could face during their normal job activities.

The topics covered the following:

1. Users should not access sensitive data through public networks, since the traffic could be spoofed.
2. Users must beware of listeners when speaking about sensitive data, as it may produce a data leak even if the information is not printed or digitally sent.
3. Users must beware also of the information written or printed on paper, observing if it includes any sensitive data.
4. Users must respect protocols to destroy or archive paper-format data, which is aligned with the confidentiality principle.
5. Users must encrypt files containing sensitive data before sending or uploading them anywhere, to preserve information confidentiality.
6. Users should never plug in USB devices from unknown sources, as it may contain malware.
7. Users must only use authorized cloud services, and of reading terms & conditions, what could determine further uses of the data being transferred.
8. Users should remove metadata from files before sending them, as it may give clues on how a malicious action could be performed.

Below the video there is a printable pdf including tips covering all the topics explained, so the user can download and/or print it to have them more accessible.

The section also offers links explaining the more technical topics that can help the user to perform the actions needed, precisely:

a) Intranet of the hospital where the internal policies are explained

b) How to remove metadata from files (Windows and Mac)

c) How to encrypt files (Windows and Mac)

IV.3.3. Block 2: Safe passwords

This is the second block of content included in the ProTego educational website. It deserves a specific block as incorrect password management supposes an exploitable thread that could invalidate many cybersecurity measures in place.

Good password policies put in place by the IT staff (for example, requirement of strong passwords that should be monthly changed) often leads to incorrect password management performed by users, as writing them down in paper or plain digital files to have them accessible. Users must know how a good password management should be performed, and this is the objective of this block.

The concrete topics covered are the following:

1. Users must never write down passwords on paper or electronic sheets, since this practice may make easy for an unauthorized person to access the hospital systems and sensitive data.

2. Users should avoid to always using the same password for every system, so a security breach in one system does not compromise the rest of systems where the user has an account or credentials to log in.
3. Users must never share their passwords with anyone. It is never allowed no matter of the reason to do that.
4. Users have to choose strong, unintuitive and non-guessable passwords, avoiding the formation of a password by unsecure techniques as starting from a dictionary word and capitalizing or tailoring it with numbers or special characters until they reach the requested length.
5. User must use password managers as proper software to create and manage strong passwords.
6. Users should enable two-factor authentication whenever it is possible. The two-factor authentication (something you know/something you have) is explained, and it is also introduced the three factor authentication based on the "something you are" concept which supposes an extra biometric validation.
7. In case of the existence of recovery questions, users should choose non-true answers, making more difficult for an attacker to impersonate the user and retrieve his password.
8. Users must change all their passwords whenever a data breach occurs because their passwords may have been exposed.

The printable tips document included in this section cover all these concepts to serve as a remainder.

In the links section, users can access more in depth information regarding the following topics:

a) How to choose strong passwords
b) Password managers
c) Enable two factor authentication (Windows and Mac)

IV.3.4. Block 3: Social engineering

The third block of content included in the ProTego educational website is devoted to the social engineering. Jointly with an incorrect management of passwords it may suppose a way to overcome the cybersecurity measures set up by the IT staff, and depends almost exclusively on the adherence of the final users to the existing recommendations and policies.

Social engineering is a broad term used to describe a range of techniques to trick people into giving fraudsters what they want. Phishing is a specific technique within social engineering, designed to gain personal information.

Phishing rude techniques have evolved to become more sophisticated and malicious emails can now come from well-known senders and are less easy to identify. Because of that, user awareness in fundamental to protect the organization from this source of risk.

The topics covered in this block are the following:

1. Users should check if text messages contain grammar or spelling errors, since it may spot a phishing email, originated in a certain language and then translated to different ones. This is most frequent on less elaborated phishing campaigns but still it is a factor to observe
2. Users must check the email address of the sender, not the explicit name. For example, *USC<cxv@cybyx.ru>* could be an example of someone trying to impersonate our *USC*.
3. Users should know that by moving the mouse over a link, they can check the associated URLs. As in the case of the email of the sender, what is shown to the user may not correspond with the real destination the link points to.

4. Users should be aware of that social engineering techniques can be extremely personalised. The rough phishing emails from years ago have evolved to a more fine-grained methodology where hook emails are prepared specifically to its recipient. That is known as spare phishing and is much more difficult to detect.
5. Users must never open unexpected attached contents in emails. By doing that it may allow the installation of malware in the PC or device they are operating from, overcoming the security measures in place to prevent attackers reach the hospital IT infrastructure.
6. Users should not click on links provided by email, and directly type the website URL instead. Legit organizations will seldom include links in the notifications, and will ask the user to directly access the website instead.
7. Urgent requests should always lead to be suspicious since one of the objectives of the attacker is to lead the victim take some action without taking time to observe, think and decide if such action is legit (expected, aligned with the work protocols and frequently asked).
8. Users must contact the IT security whenever unsure about any message, since the experts in the IT department could more easily detect a phishing email and take the appropriate measures, as rules in the email server or advice the employees via corporate communication channels if it may suppose a risk.

The tips are included in a printable guide in the website below the corresponding video.

In the links section, users can get more in depth information regarding the following topics:

a) best practices to keep safe during teleworking
b) deepen the knowledge on social engineering attacks
c) learn how to spot phishing emails

IV.3.5. Block 4: Mobile devices

The fourth and last training block of the ProTego educational website covers mobile devices. It is mandatory to make a specific reference to mobile devices because they have acquired capabilities like those of personal computers, and business users are granted high-level access from personal mobile devices (smartphones and tablets). In fact they are effectively replacing desktops for many business tasks. However, personal mobile devices don't offer the same level of built-in security or control as the organization-owned desktop computers they are replacing.

This trend is known as BYOD (Bring Your Own Device) and it is getting even more common in healthcare because of the necessity to allow physicians to monitor patients even not being physically near.

That is causing that a high percentage of workers now routinely access corporate data from smartphones, and that means keeping sensitive data out of the wrong hands is an important concern.

Many, if not all, the hacking techniques related with social engineering may be performed through a mobile device, and the general recommendations of not clicking links from emails, SMS, check websites URL, etc. are relevant on smartphones as well. But there are, moreover, some specific comments to be made in reference to them.

The concrete topics covered in this section are the following:

1. Users should download apps from certified websites/app stores only. When new Apps are developed, they need to be certified in terms of security, performance, resource needs, etc. This certification is made before allowing the apps to be uploaded to the certified sites (Play Store for Android and App Store for iPhone's IOS) so if the apps are downloaded from these sites, users can be sure those controls have been performed and the apps are safe, among other features.

2. Users must control the permissions given to each app on the device. By downloading Apps from the official sites users can be sure that they are not fake apps or apps that have been reported for security issues. But there is something else that user must take care of. Each app will need permissions to some functionalities or contents into the phone and users are asked to allow access to them during the app installation
3. Users must be aware of that cyber attacks can also target operating systems for mobiles. Most of them have the incorrect impression that viruses and malware can only affect to PCs, what leads to a lack of control of this issue on their mobile devices.
4. Due to the previous, users must install antiviruses and protection systems on the mobile devices owned to keep them safe from that threat.
5. Users must keep the operating system and the apps updated, since official updates released add protection to known cyber security threats.
6. Users must not click on links or contents attached to unexpected messages, in a similar way to what has been explained on the training block devoted to social engineering.
7. Users must understand that cyber security passes by private life and personal devices. The BYOD trend act as a communicating vessel between those two environments that were formerly separated.
8. Users must keep in mind that also voice calls can be spoofed. It is form of social engineering known as *vishing* (voice phishing) that apply to voice calls.

As in the previous training blocks, the tips are included in a printable guide in the website below the corresponding video.

In the links section, users can get more in depth information regarding the following topics:

a) how to control app permissions – (Android and IOS)

b) more about best antivirus apps – (Android and IOS)

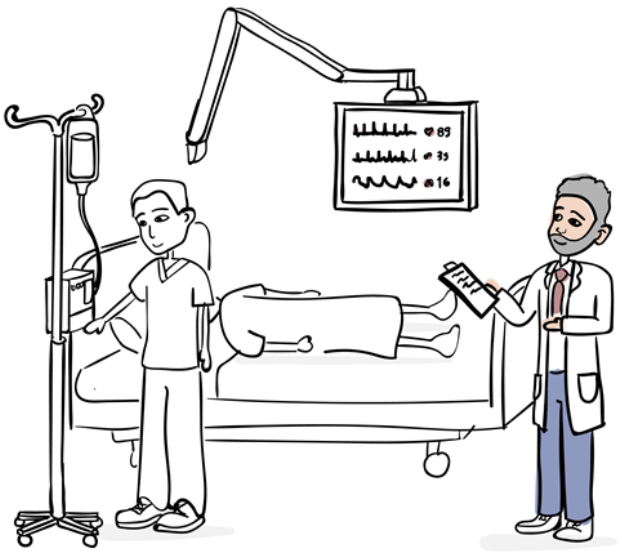
IV.4. Storyboard

With illustrative purposes in this section a storyboard is included, showing the use case of consumption of the educational material by a member of the health staff.

#1

Mark, is a 50-year-old cardiologist working at the “Central Hospital”.

Over the years Mark’s work has evolved enormously: when he started, the exchange of information happened almost completely on paper



#2

Today he uses various devices through which he can consult and exchange information concerning patients and therapies.

However, having the information written on paper is a habit that he has kept to this day



#3

Recently, Mark happened to receive suspicious emails asking him to enter personal information; it was hard for him to say if they really came from the hospital.



#4

During a break with his colleagues, Mark notices a poster form ProTego's "Cyber Security Awareness Program", explaining the cyber risks within the hospital.

He knows what it is since the responsible of the Cardiology area introduced during a clinical meeting.



#5

The poster invites the reader to deepen the knowledge on cyber security.

Thanks to the QR code on the poster, Mark can access to the online Cyber Security Awareness Program



#6

He lands on the welcome page where he can discover more about the aim of the program



#7

Moreover, he finds the educational section divided by topics.

Each topic is described with a set of tips, a video, and printable suggestions



#8

Thanks to the educational awareness material consulted, Mark is now better aware about the principal cyber security risks; he removes the password on paper, and he can now recognize a phishing email



#9

Moreover, to be sure to remember all the advices he got on cyber security risks, he prints the posters provided on the website



#10

Finally, Mark can evaluate the material with a questionnaire he finds on the website



IV.5. Assessment of the training program

At the time of writing this document the training program has been executed in both ProTego testbed hospitals (OSR and MS). In this section the conclussions of that execution will be

explained by analizing the answers to the survey included as part of the training material. The mentioned survey is divided in two secions:

- One included questions that allow to compare the Risk Awareness Profile of the organizations after and before the educations program. This tool was presented in D3.1 as a mean of assessing some key indicators regarding cybersecurity.
- The other included questions to gather the opinnion of the users about the educational program itself, including the contents included, the channels used and the easyness or difficulty to consume and understant the material.

The complete survey used has been included in the APENDIX D. As it can be viewed, the column labeled as *"Section"* indicates to which finality each question is related to.

IV.5.1. Impact on the Risk Awareness Profile

IV.5.1.a. MS results

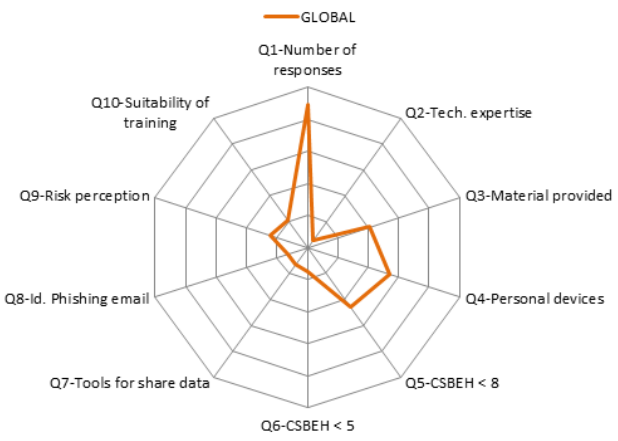
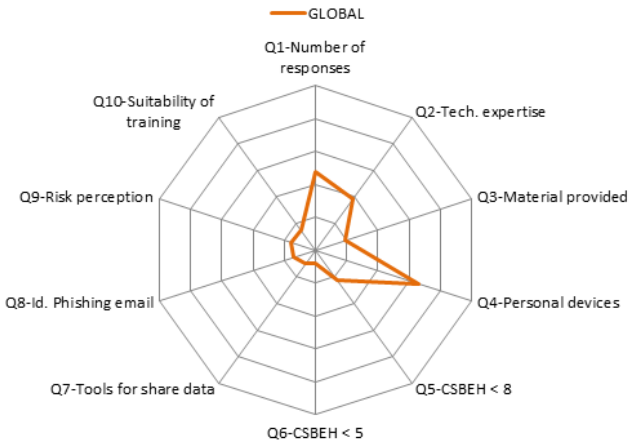
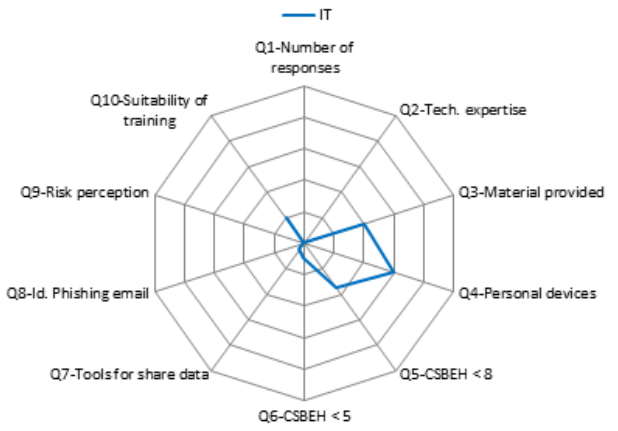
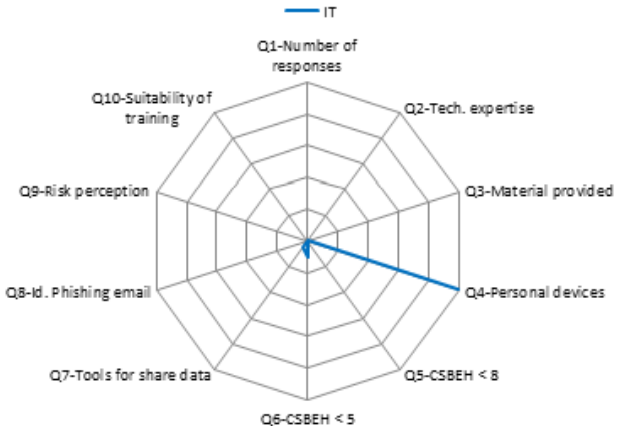
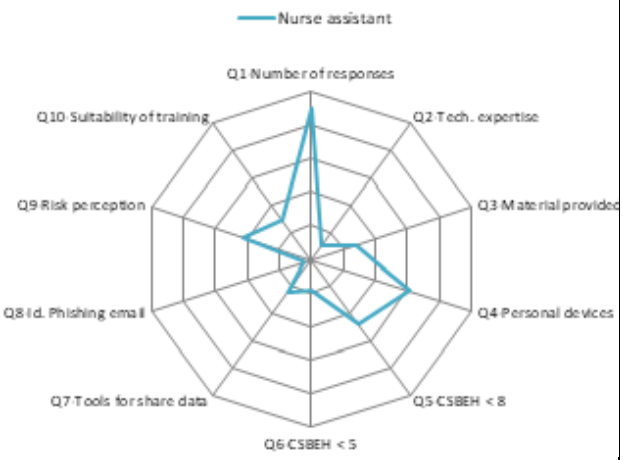
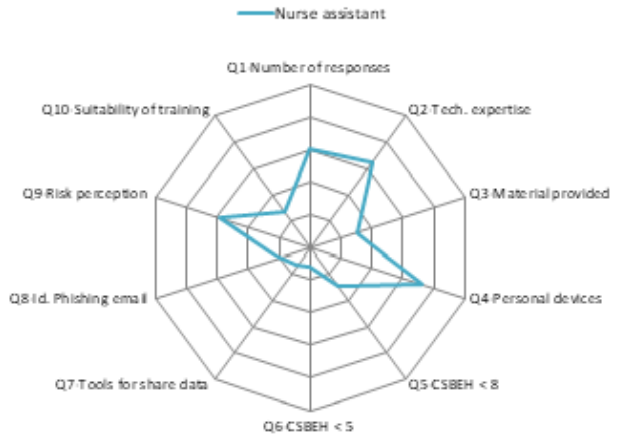
To help understand the conclusions extracted, it is required to present the following table, including the responses for each of the 10 items included both before and after the educational program has been executed:

	BEFORE TRAINING						AFTER TRAINING					
QUESTION	IT (%)	Support (%)	Physician (%)	Nurse (%)	Nurse ass. (%)	GLOBAL (%)	IT (%)	Support (%)	Physician (%)	Nurse (%)	Nurse ass. (%)	GLOBAL (%)
Q1-Number of responses	0,0	90,4	91,3	91,7	90,2	89,6	0,0	55,4	38,1	47,2	61,2	48
Q2-Tech. expertise	0,0	0,0	10,0	7,9	9,5	5,9	0,0	51,2	21,5	41,3	64,7	38,3
Q3-Material provided	40,0	48,1	50,0	36,8	28,6	41,2	0,0	15,4	8,5	28,3	30,6	18,9
Q4-Personal devices	60,0	25,9	50,0	68,4	61,9	53,7	100,0	53,7	54,7	77,8	72,9	65,9
Q5-CSBEH < 8	35,0	59,3	26,7	34,2	47,6	45,45	0,0	22,8	19,7	24,8	29,4	22,6
Q6-CSBEH < 5	0,0	25,9	20,0	5,3	19,0	15,4	0,0	9,8	7,6	6,1	11,8	7,8
Q7-Tools for share data	0,0	7,4	23,3	7,9	23,8	13,2	0,0	10,6	13,9	6,1	14,1	10,3
Q8-Id. Phishing email	0,0	33,3	13,3	10,5	4,8	13,2	0,0	20,3	9,4	13,9	20,0	14,0
Q9-Risk perception	0,0	22,2	53,3	5,3	42,9	24,3	0,0	13,8	8,1	9,1	58,8	15,6
Q10-Suitability of training	20,0	22,2	20,0	15,8	28,6	20,6	0,0	13,0	10,3	17,8	27,1	15,1

Starting from the previous table, we will describe the conclusions obtained, for each item of the R.A.P. and diving into each user group when necessary. It is worth to remember that the values should be read as negative values, that is, the higher the result, the more risk it represents. Reader can find the R.A.P. description on D3.1.

As an example of that we can take the value for the Physician user group to the Q1. The value 38,1 means that the survey has been answered by the 61,9% (100 – 38,1) of the Physicians. In this case the risk situation comes from not having responded the survey, what indicates low engagement about cybersecurity concerns.

Graphically, this is the representation of the "GLOBAL" columns, representing the average results of the observed user groups:

BEFORE TRAINING	AFTER TRAINING
MS GLOBAL RISK AWARENESS PROFILE	**MS GLOBAL RISK AWARENESS PROFILE**
	
MS RISK AWARENESS PROFILE - IT	**MS RISK AWARENESS PROFILE - IT**
	
MS RISK AWARENESS PROFILE - NURSE ASSISTANT	**MS RISK AWARENESS PROFILE - NURSE ASSISTANT**
	

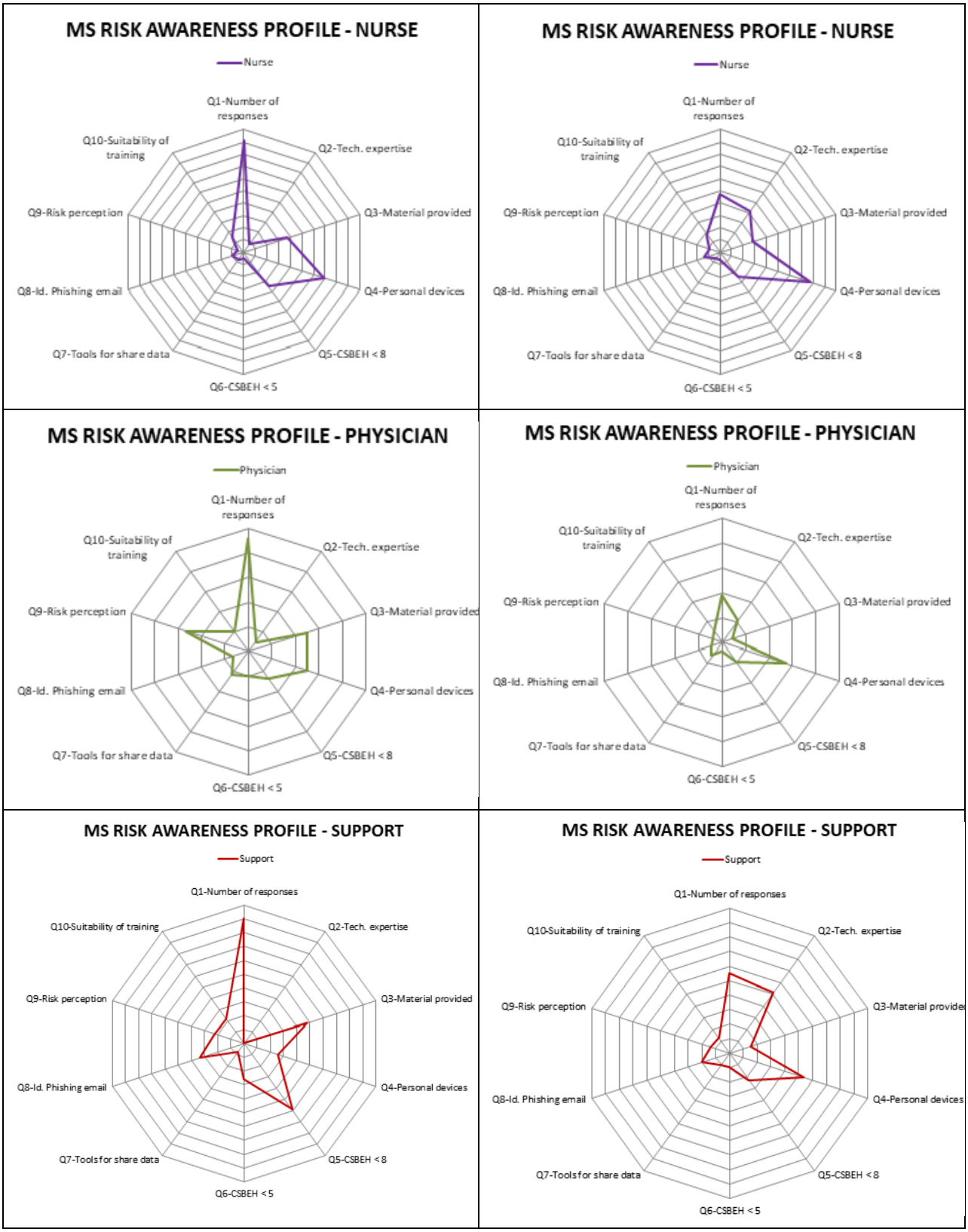


Figure 13: Risk Awareness Profile - MS

Q1.-Number of responses

The following table shows how the amount of users responding the survey has been increased compared form the first survey launched before the execution of the educational program:

		BEFORE TRAINING		AFTER TRAINING	
User type	**Total staff**	**Responses obtained**	**Percentage (%)**	**Responses obtained**	**Percentage (%)**
IT	20	20	100	20	100
Support	276	27	9,78	123	44,56
Physician	360	30	8,33	223	61,94
Nurses	436	38	8,72	230	52,75
Nurse assistants	219	21	9,59	85	38,81
TOTAL	1311	136	10,37	681	51,95

In the first execution (D3.1) we obtained a 10,37% of potential responses. In this second execution we obtained 51,95%. That means:

- The health staff is more engaged. The perception of cybersecurity as an important subject has been increased. With this, the first objective succeeded.
- The representativeness of the sample is higher and so the conclusion more robust. That may cause some indicators seem to deteriorate, but it is not actually true. The reason is that with this higher participation these results show a more valid picture of the reality.
- We can observe significantly more engagement in physicians (61,9%) and nurses (52,8%) than in nurse assistants and support personnel, being their participation around 40%. It shows that the groups of users that treat more health data are more concerned. The IT staff has provided 100% of potential responses, not varying from the first execution.

Q2.-Tech expertise

The interpretation of this item needs to be done jointly with the previous question. Attending solely to the results obtained it leads to think that the expertise level informed by the users has become worst (lower). But if we attend to it mixed with the number of total responses, we can extract some interesting conclusions:

- The value of the tech expertise reported by the staff is more real because it has been observed over a more representative sample (51,95% of the total staff).
- The results from the first execution showed more skilled users. But the fact is that only the most skilled users, that is, those users that were more interested in IT in general, did respond the survey. A lecture of this is that the mechanism used to spread the educational program had the expected impact and the material has been consumed even by a significant part of those users with lower IT skills, that is, less interested in IT and cybersecurity.
- Leaving apart the IT staff, the tech expertise is significantly higher in physician and nurse user groups, in comparison to the nurse assistant and support user groups.

Q3.-Material provided

The interpretation of this item is quite clear. Previous to this educational program, the material regarding cybersecurity was included in internal policies that, despite being published and accessible to the staff, did not got their attention and when asked, they did not could remember it or associate it as educational material.

The material provided has been clearly identifiable as cybersecurity training material and, ths, more probably consumed.

Q4.-Personal devices

Depending on the organization policies and rules, the use of personal devices may or not be considered as a bad behaviour, but anyway it shows a relevant point to focus when designing security policies. It the staff reports to be using personal devices to access sensitive and/or health data, access corporate applications, etc., both educational material and security policies need to be enabled to protect from the risks associated to that behaviour.

In the case of MS, and increased by the pandemic, the percentage of staff members that use personal devices is about 65%.

Q5.-CSBEH < 8

This item from the R.A.P. measures the percentage of the users that confirmed to apply less than 8 good cybersecurity behaviours, within a list of 17, covering most of the concerns an average user has to deal with. It includes topics from every training bock: password management, social engineering, mobile devices.

Its interpretation may have two different uses: attending to the results for each user group under study, it is possible identify gaps that discover higher risks on certain user groups and so focus on the training of them.

It is also possible to make an interpretation focusing on those bad behaviours reported, that is, those good behaviours that have less adherence from final users, and intensify the training regarding those specific topics.

In the case of MS it can be observed the same tendency of previous questions, where physicians and nurses (around 20%) report more maturity if compared with nurse assistants and support staff (near 30%). Comparing the results from the first execution, the risk indicator has been reduced by 50%. That's because of the user's recognition of the bad behaviours explained in the videos, what caused they to respond the survey as a "will do", instead of merely describing what they actually have been doing.

Q6.-CSBEH < 5

This question is quite similar to the previous one, but it would reveal a more risky situation if the indicator is more than 15%, since it shows the percentage of users that admit to perform more than 12 bad behaviours from a list of 17.

The same analysis as in Q5 could be performed. In this case we observe values around 10%, with a reduction of 50% respect the first execution. The lecture is the same that in the previous question.

Q7.-Tools for sharing/processing data

This question shows the percentage of users that share sensitive data through untrusted tools (Personal e-mail, External Cloud, External USB/HD key, Skype, WhatsApp).

The total values obtained (10,3%) remains similar to those obtained in the first execution (13,2%). This has more to do with the measures set in place in each organization and we can see it by attending to the incorrect behaviours reported in the responses. At a first glance one may think that these values would be higher, and that the use of USB devices should be one of the most reported bad behaviours. But in the case of Marina Salud it is almost negligible because the most of the users behave to a user profile that has the usb ports disabled, and so, no data can be stored and shared by the use of that kind of devices. That has impact in the total value as well, keeping it around 10% which is a very low value, which can be interpreted as this is not a high risk for the organization.

Q8.- Identify phishing email

On this question, and despite the increased number of responses, we can observe the same tendency with a 13 to 14% of incorrect responses, that is, the 14% of the responders could not identify the phishing email. But this indicator is now more robust and it should be considered that by a more challenging example of phishing email these results and the level of risk associated may be increased.

Q9.-Risk perception

In this question the results obtained show a decrease in the risk indicator, that is, a higher percentage of users answered they think they can fall victim to a malicious attack. The total result decreased from a 24,3% to a 15,3%. By roles, physicians are by far who reported more conscience about this risk, swapping from a previous 53,3% to a current 8,1%. This result can be explained as a direct consequence of the educational material provided and the effect on the physicians, that are who make a more intense use of the IT tools during their work routines, and so can feel more identified with the situations depicted in the videos.

Q10.- Suitability of training

The value obtained shows that the 85% of the staff consider as a good initiative to participate in cybersecurity training. That has been improved by a 5% from the previous results, but with a higher number of responses.

Part of the success in this concrete topic has been the shape of the educational material, with short and easy-to-understand videos, that anyone could attend on their preferred time and with no necessity to be physically present, what may be a handicap especially for health staff.

IV.5.1.b. OSR results

The following table contains the responses for each of the 10 items included both before and after the educational program has been executed in OSR.

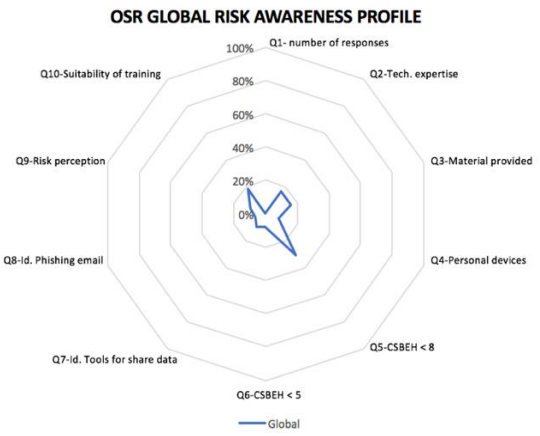
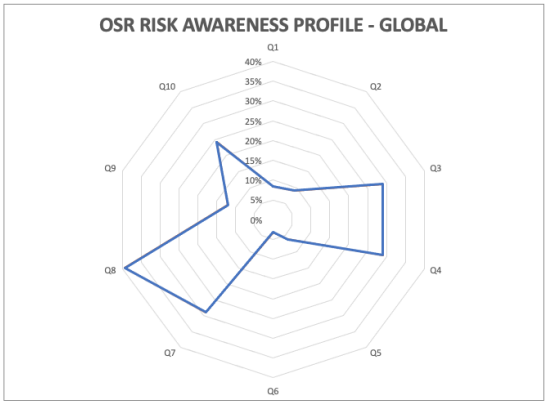
	BEFORE TRAINING					AFTER TRAINING				
QUESTION	Clinical (%)	Research (%)	Staff (%)	Technical (%)	GLOBAL (%)	Clinical (%)	Research (%)	Staff (%)	Technical (%)	GLOBAL (%)
Q1-Number of responses	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	n.d.	8,0
Q2-Tech. Expertise	30,6	5,2	0,0	10	16,1	13,0	0,0	33,3	n.d.	9,1
Q3-Informative material provided by the Hospital	15,3	20,7	14,3	0,0	16,1	20,0	38,0	33,3	n.d.	29,3
Q4-Devices used during work activity	4,2	15,5	4,8	0,0	8,1	27,0	38,0	0,0	n.d.	29,3
Q5-Awareness Health Belief Model (Less than 8)	41,7	27,6	19	0,0	31,1	13,0	0,0	0,0	n.d.	6,1
Q6-Awareness Health Belief Model (Less than 5)	9,7	6,9	9,5	0,0	8,1	7,0	0,0	0,0	n.d.	3,2

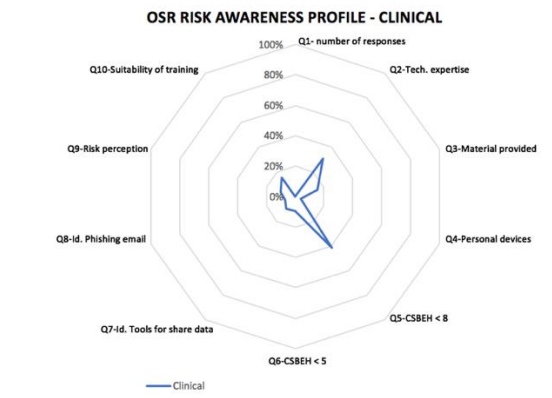
Q7-Tools used to share sensitive data	9,7	8,6	19	0,0	9,9	27,0	38,5	0,0	n.d.	29,3
Q8-Identify phishing email	7	5,1	4,8	10	6,2	53,0	31,0	33,3	n.d.	39,4
Q9-Perception of risk	9,7	8,6	14,3	10	9,9	13,0	15,0	0,0	n.d.	12,1
Q10-Suitability to spend time in training	15,3	22,4	19	20	18,6	27,0	31,0	0,0	n.d.	24,4

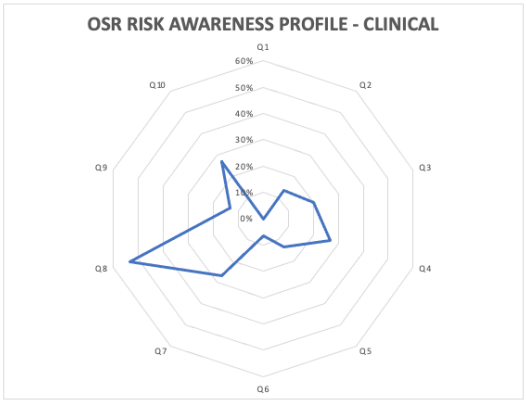
Starting from the previous table, we will describe the conclusions obtained, for each item of the R.A.P. and diving into each user group when necessary. It is worth to remember that the values should be read as negative values, that is, the higher the result, the more risk it represents.

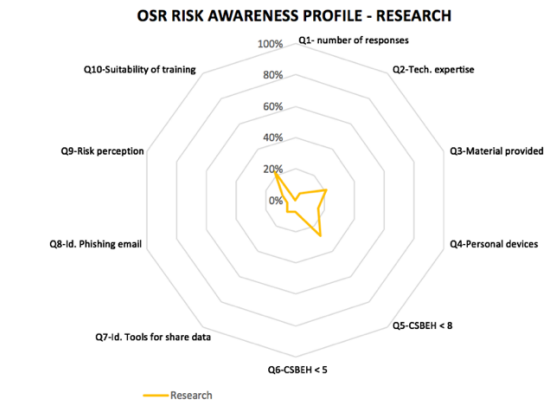
As an example of that we can take the value for the Clinical user group to the Q2. The value 13,0 means that the 87% of respondents have said they're not technological beginners (100 – 13,0) of the Clinical employees. In this case the risk situation comes from being a beginner, what indicates low knowledge about cybersecurity concerns.

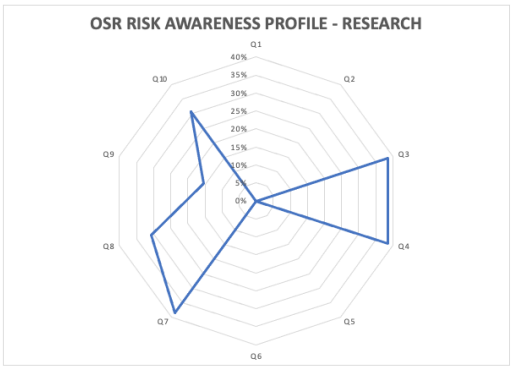
Graphically, this is the representation of the "GLOBAL" columns, representing the average results of the observed user groups:

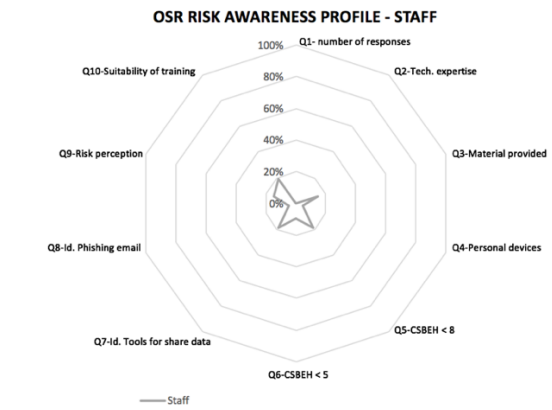
BEFORE TRAINING	AFTER TRAINING
	

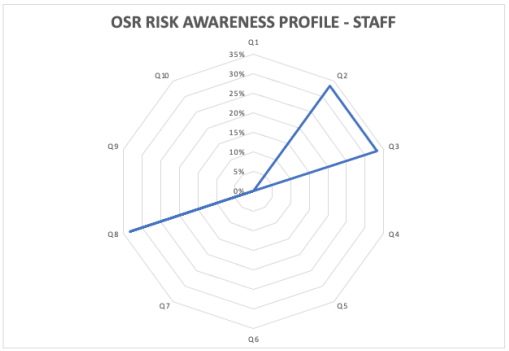

OSR RISK AWARENESS PROFILE - CLINICAL
Q1- number of responses
Q2-Tech. expertise
Q3-Material provided
Q4-Personal devices
Q5-CSBEH < 8
Q6-CSBEH < 5
Q7-Id. Tools for share data
Q8-Id. Phishing email
Q9-Risk perception
Q10-Suitability of training
100%
80%
60%
40%
20%
0%
Clinical

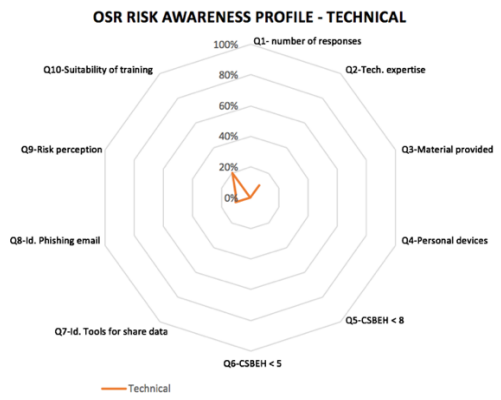

OSR RISK AWARENESS PROFILE - CLINICAL
Q1
Q2
Q3
Q4
Q5
Q6
Q7
Q8
Q9
Q10
60%
50%
40%
30%
20%
10%
0%


OSR RISK AWARENESS PROFILE - RESEARCH
Q1- number of responses
Q2-Tech. expertise
Q3-Material provided
Q4-Personal devices
Q5-CSBEH < 8
Q6-CSBEH < 5
Q7-Id. Tools for share data
Q8-Id. Phishing email
Q9-Risk perception
Q10-Suitability of training
100%
80%
60%
40%
20%
0%
Research


OSR RISK AWARENESS PROFILE - RESEARCH
Q1
Q2
Q3
Q4
Q5
Q6
Q7
Q8
Q9
Q10
40%
35%
30%
25%
20%
15%
10%
5%
0%


OSR RISK AWARENESS PROFILE - STAFF
Q1- number of responses
Q2-Tech. expertise
Q3-Material provided
Q4-Personal devices
Q5-CSBEH < 8
Q6-CSBEH < 5
Q7-Id. Tools for share data
Q8-Id. Phishing email
Q9-Risk perception
Q10-Suitability of training
100%
80%
60%
40%
20%
0%
Staff


OSR RISK AWARENESS PROFILE - STAFF
Q1
Q2
Q3
Q4
Q5
Q6
Q7
Q8
Q9
Q10
35%
30%
25%
20%
15%
10%
5%
0%



<NO DATA>

Figure 14: Risk Awareness Profile - OSR

Q1.-Number of responses

A total number of 47 people replied to the survey. Among them, 14 respondents did not complete the survey and therefore were excluded from the sample. The remaining 33 respondents (15 clinicians, 13 researchers, 3 staff employees and 2 OSR visitors) fill out entirely the questionnaire and thus represent the OSR sample size. It is important to notice that the samples of the two runs are not represented by the same participants and therefore only a relative comparison of the collected data can be made.

Q2.-Tech expertise

The percentage of people who have declared themselves beginners is quite low in this second execution compared to the first. In particular, clinicians and researchers who responded that they were beginners halved. On the other hand, Staff employees who declared themselves as beginners in this second execution increased by 33,3%.

Q3.-Material provided

Most of OSR respondents are aware of the material provided to them by the hospital. However, there are still about 29% of respondents who have had difficulty defining the educational resources available to them in the hospital. Specifically, some respondents declare that the Hospital doesn't provide them any material, arguing that the ProTego material is the first educational material on cyber security topic that they got.

Q4.-Personal devices

In general, the percentage of respondents who use personal devices to carry out work activities is around 29%. By looking at the researchers, the percentage rises to 38% of people using personal devices. Staff reported using only corporate devices.

Q5.-CSBEH < 8

Comparing the results of the first run, the risk indicator has significantly decreased, by around 25%. This is probably due to the educational content explained in the videos that allowed users to improve their awareness of what behaviors should not be adopted.

Q6.-CSBEH < 5

In this case we observe values around 3%, with a reduction of 5% with respect to the first execution. The lecture is the same that in the previous question, the educational content

explained in the videos allowed users to improve their awareness of what behaviors should not be adopted.

Q7.-Tools for sharing/processing data

In OSR, researchers appear to be the largest proportion of respondents (38%) to use unofficial tools to exchange data. Staff members declared they only uses business-related tools.

Q8.-Identify phishing email

About 40% of respondents were unable to identify the phishing email presented in the survey.

Q9.-Perception of risk

In general, it can be said that the perception of risk by OSR employees is quite high; only 12% of them obtained a score indicative of low-risk perception.

Q10.-Suitability to spend time in training

Most of OSR employees are inclined to attend training courses. However, 24% of respondents perceived inconvenient to spend time on cybersecurity training courses

IV.5.1.c. Conclussions

The Risk Awareness Profile has been designed in ProTego as a tool to measure the impact of a training plan, or the current situation in terms of cybersecurity awareness in a healthcare organization. It is an analytic tool and thus it is based on a set of indicators, and the validity of the conclusions has a directly dependence on the representativeness of the sample, that is, the number of responses respect the total of potential responses.

So, to maximize the number of responses is a main objective to extract valid conclusions. But not only that: more responses would indicate more engagement and higher awareness levels.

By analysing the results we can see an increase of good behaviors since questions 5 and 6 show improved results after the health staff of both hospitals consumed the educational material.

But the main conclusion that can be extracted is about the way to achieve that clinical staff perceive cyber security as part of their responsibility and not as a (exclusively) technical concern.

The dissemination of the material and the survey has been done in different ways in the two testbed hospitals: while in OSR it has been performed by an email campaign, in MS it has been done with the collaboration of the clinical managers, following the procedure described in the section IV.2. So we can compare the results between both: in a context of pandemic where it is certainly difficult to reach clinical staff with concerns not purely clinical, the results in OSR have worked as expected, with a lowered level of participation. Concretely 47 responses were obtained, while in the pre pandemic survey executed in the context of D3.1 we obtained 217 answers.

In the meantime, in MS we have obtained 617 responses, where in the D3.1 pre-pandemic survey we obtained 136 responses with a classic email campaign as a dissemination method.

This numbers shows the importance of engaging the clinical managers in the training program, mainly to introduce it to the final recipients, give the appropriate “not-only-technical” approach.

IV.5.2. Assessment of the material provided

The survey did also include a set of questions to assess the opinion of the users about the provided material and its effectiveness.

The questions aimed to this objective can be found in the table included in APENDIX D, labelled as “Effectiveness / Opinion” in the column “*Section”* of the table.

To perform this assessment the analysis will go through the following topics:

- Effectiveness
- Perceived usefulness
- Perceived Clarity
- Perceived motivation
- Perceived efficiency
- Satisfaction
- Most liked aspects
- What to improve

The analysis will compare the values obtained in both testbed hospitals (MS and OSR) to determine if there are major differences between them.

IV.5.2.a. Effectiveness

The ISO 9241-11:2018[22] define the effectiveness as the “accuracy and completeness with which users achieve specified goals”. The main goal of the educational material is to increase the awareness of employees on the principal cybersecurity topics. In order to measure how effective the material was, it has been calculated the percentage of correct answers over the total number of answers received for the questions related to each section of the material: The good employee, Safe password, Social engineering and Mobile devices

The results obtained in the two hospitals are shown in the figure below:

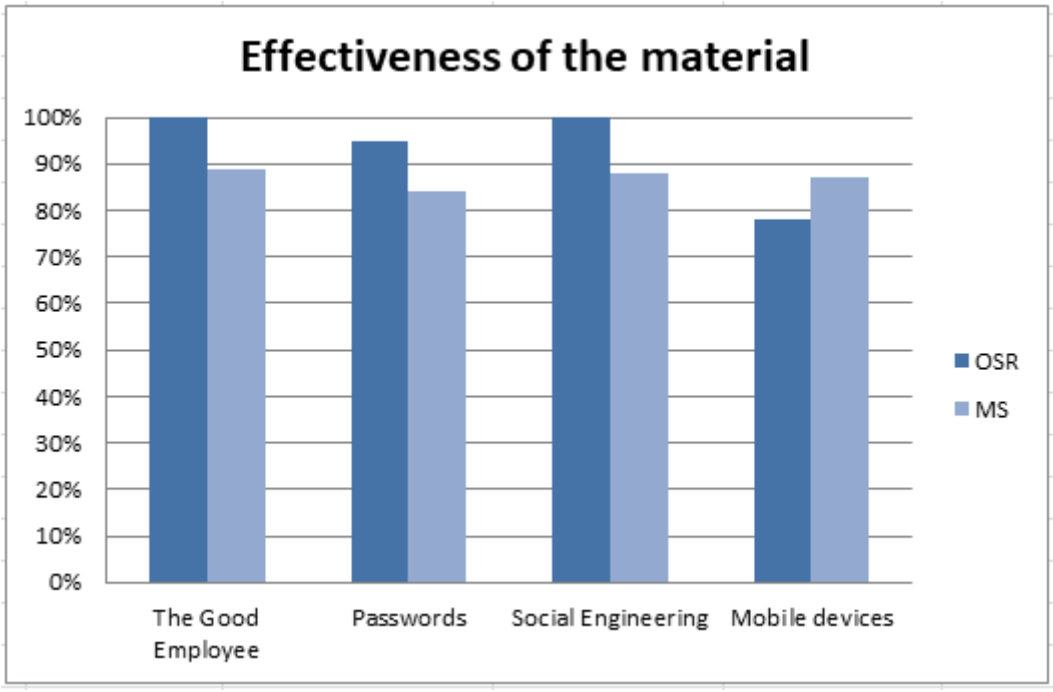


Figure 15: Effectiveness of the material

With this question it can be observed that the most of the users (nearly 90%) could understand the messages informed in the videos, and so the material has been effective. This is aligned with the results observed in the questions Q5 and Q6 of the Risk Awareness Profile, where we can observe that the bad behaviors reported by the users have been lowered.

IV.5.2.b. Perceived usefulness

To measure the material usefulness, it has been asked to the users to indicate (on a Likert scale ranging from “Strongly Disagree” to “Strongly Agree”) to which extent they believed the material was useful to improve they awareness on cybersecurity.

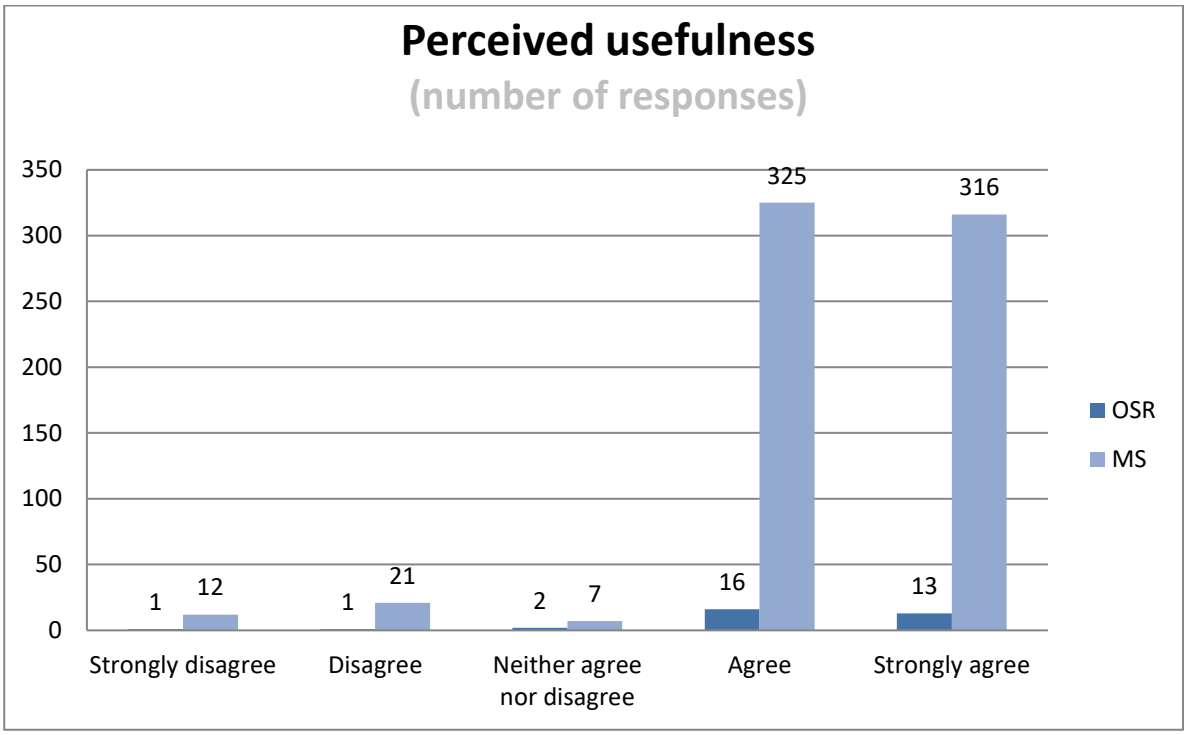


Figure 16: Perceived usefulness

The material has been perceived as very useful, as it can be deduced form the results. 93.8% of the respondents agree or strongly agree that the proposed educational material has been useful to improve their awareness on the proposed topics. And the results remain similar in both hospitals.

IV.5.2.c. Perceived clarity

To measure the material clarity, it has been asked to the users to indicate (on a Likert scale ranging from “Strongly Disagree” to “Strongly Agree”) to which extent they believed the material was clear to describe cybersecurity topics.

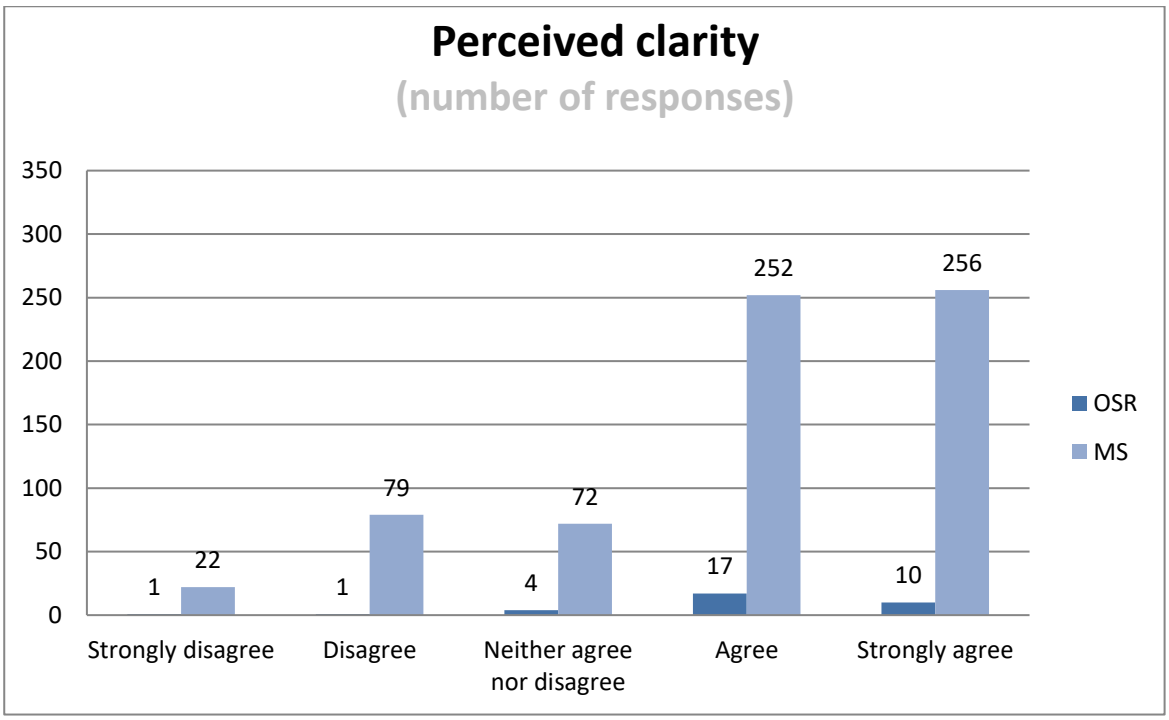


Figure 17: Perceived clarity

The results show that the majority of the responders opinined that the material is clear, with a 75% in the range of ”Agree” or ”Strongly Agree”. But there is a 25% that think the material is not clear enough. If we study these results jointly with the ”what to improve” question (later in this document) we can deduce that those who didn’t agree with the clarity of the material is because of the language, as the material has been provided fully in English and there are still users with low skills to fluently understand English.

That being stated, we can conclude the material is clear enough for the majority of users.

IV.5.2.d. Perceived motivation

To measure the material motivation, it has been asked to the users to indicate (on a Likert scale ranging from “Strongly Disagree” to “Strongly Agree”) to which extent they believed the material was motivating.

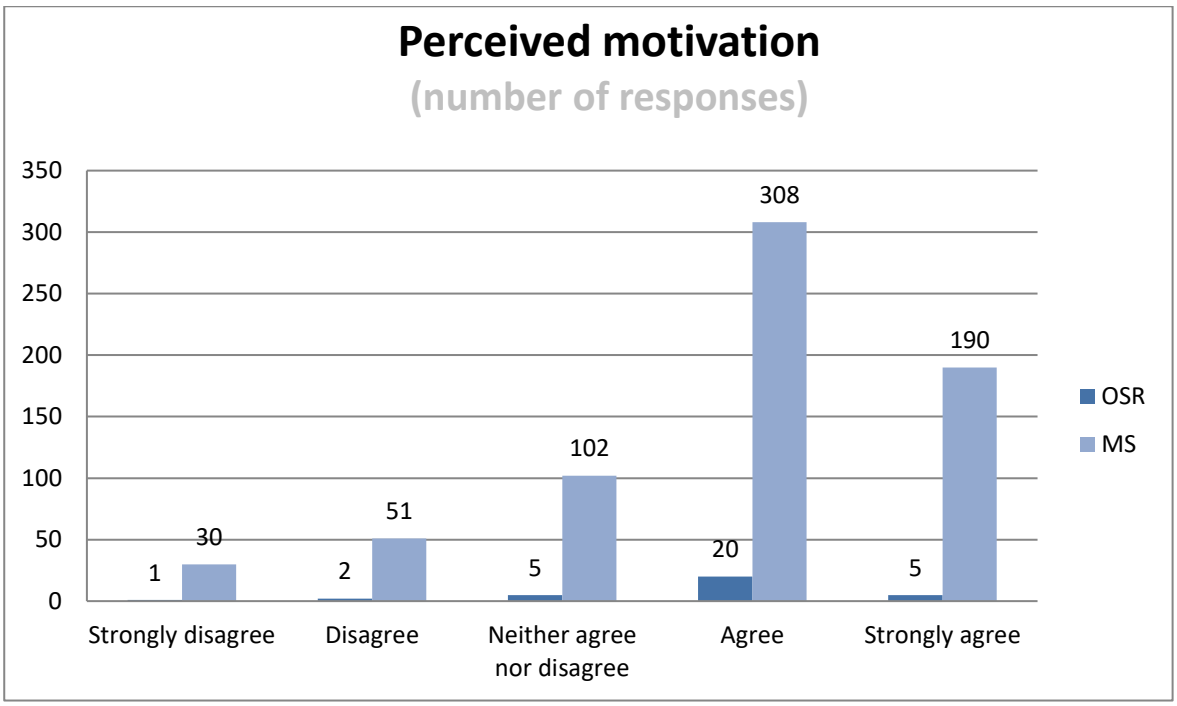


Figure 18: Perceived motivation

The results show that 73.3% of users agree or strongly agree in stating that the proposed educational material has been perceived as motivating in explaining the topics related to cyber security. And 15% neither agree nor disagree. The result is that only 11.7% of users think that the material is not motivating.

IV.5.2.e. Perceived efficiency

The ISO 9241-11:2018 [22] define the efficiency as the "resources used in relation to the results achieved". In order to measure how efficient the material was, it has been asked to the users to indicate (on a Likert scale ranging from "Strongly Disagree" to "Strongly Agree") to which extent they believed the time spent to consult the material was appropriate.

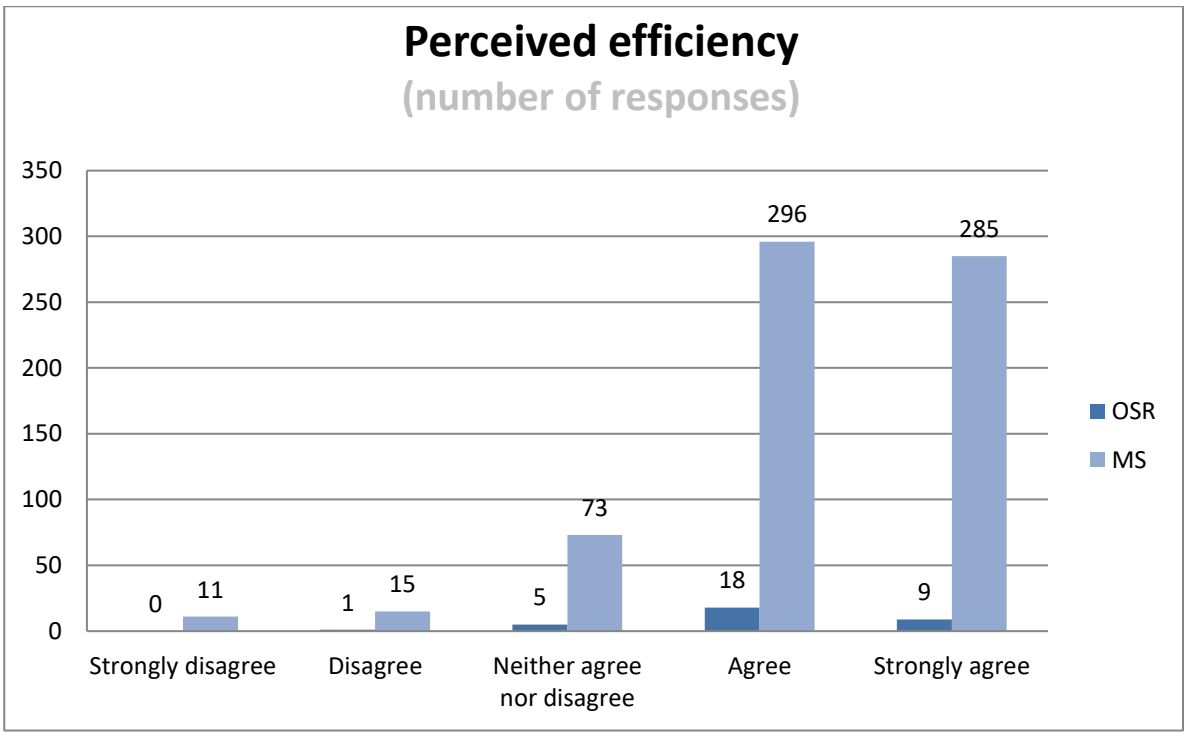


Figure 19: Perceived efficiency

It was one of the main issues addressed in the design of the training material, as we considered that if we demand a small portion of time to consume the material, the overall opinion would be improved. And by the results obtained it seems clear that the objective was achieved, since 85.15% of the users both agree or strongly agree with the assumption that the required time was appropriate.

IV.5.2.f. Satisfaction

The ISO 9241-11:2018 [22] define the satisfaction as the “extent to which the user's physical, cognitive and emotional responses that result from the use of a system, product or service meet the user’s needs and expectations”. To measure how satisfactory, the material was, it has been adopted the *Net Promote Score (NPS)* question. In this question, the users had to indicate (on a scale ranging from 1 to 10) to which extent they were likely to recommend the educational material to a friend or colleague. The scores ranging from 0 to 6 describe the detractors, that are those users that were not likely to recommend the material. The scores ranging from 7 to 8 describe the neutrals, that are those users that were neither not likely nor likely to recommend the material. The scores ranging from 9 to 10 describe the promotors, that are those users that were likely to recommend the material.

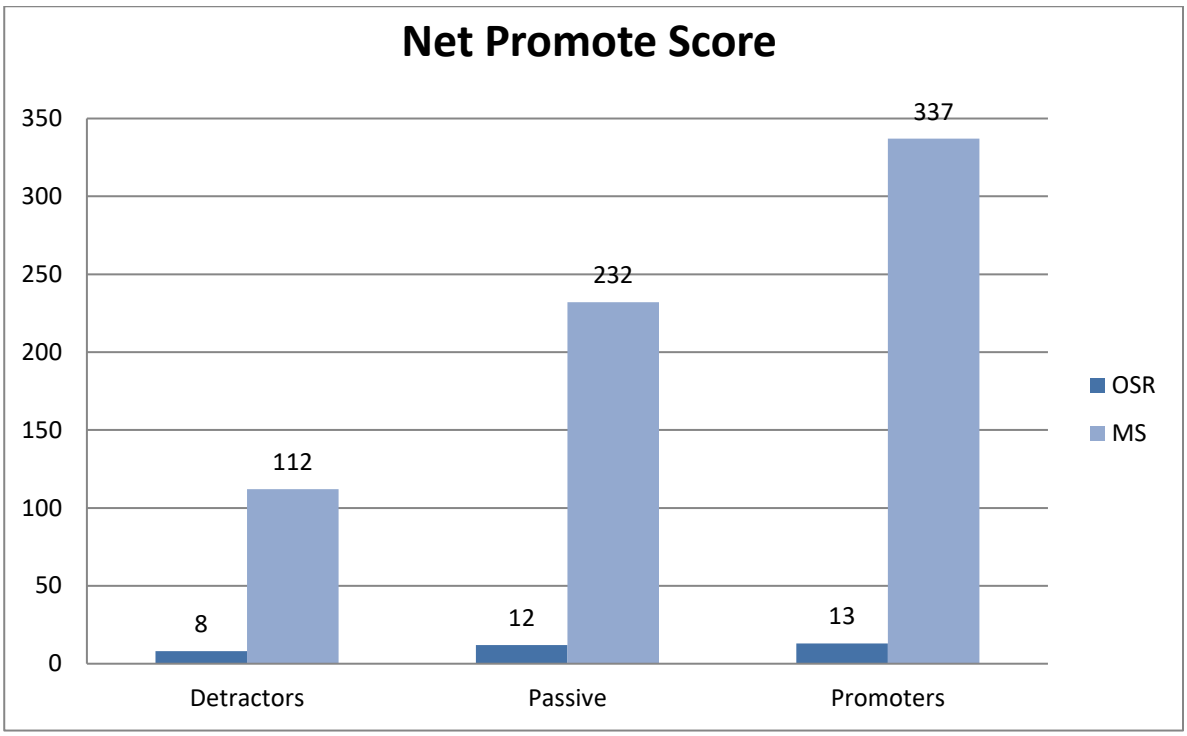


Figure 20: Satisfaction

Attending to the results, 50% of users could be defined as promoters, 34% as passives and 16% as detractors.

IV.5.2.g. Most liked aspects

Users were asked through an open question to describe the most appreciated aspects of the educational material.

There was coincidence in the items more mentioned in both hospitals that were mostly related with the user experience, concretely:

- ***CREATIVITY OF METHODS***, that have been perceived as creative and attractive.
- ***VISUAL LANGUAGE.*** Users defined the illustrations and graphical elements as immediate and captivating.
- ***CONTENT CLARITY***, stating that they liked the structure of the educational website and found it clear and that allowed them to consult it without problems.
- ***CONCISION***, since users defined the material as brief and concise.

IV.5.2.h. What to improve

At the end of the survey, users were asked through an open question what aspects of the educational material should be improved.

The most commented issue in both hospitals has been the recommendation to create the material also in Spanish / Italian language.

Apart of this main concern, users did also suggest some other ideas to improve the material:

- ***ADD CONCRETE EXAMPLES,*** arguing that the use of more concrete could be helpful and raise awareness of concepts that otherwise always seem abstract and “distant”.
- ***IMPROVE MATERIAL WITH WEBINAR,*** expressing that despite the material is useful, adding that an interactive webinar with the contents of ProTego educational material could be useful and effective.
- ***ADD MORE TOPICS*** to increase their skill on cybersecurity.

V. EDUCATIONAL MATERIAL FOR PATIENTS

Patients act as final users of healthcare applications. Their role in cybersecurity is similar to the role of health staff but with some key differences:

1. Their access is limited to consult their own health data, that is managed by the hospital or healthcare organization
2. The interaction with that data is mainly done through web or mobile apps.
3. The educational material offered must be easy to understand, as no expertise can be assumed for 'patient' architype since it refers to the general population.
4. The educational material should focus on the improvement of specific cybersecurity behaviours that may overcome technical measures put in place.
5. It is difficult to reach them, as there is no defined space for cybersecurity in the relation between patients and healthcare organizations.

The contents of the ProTego educational website have been designed to fulfil the needs of patients as well. The main sources of threats are related to the password management, social engineering and use of mobile devices, and these topics have specific sections in the educational website.

But the main handicap about extending cybersecurity awareness education to patients is to find the appropriate ways to reach them.

In the case of the health staff, and as it has been explained in the SECTION IV.2, the educational program has been introduced by clinical managers. But in the case of patients most of them have fleeting contacts with the healthcare organization and the time is used to give the requested cares and services, with no possibility to place any extra activity.

In this context the way to reach patients should be to introduce them in parallel with the ”normal” healthcare activity and allow them to deepen into it by easily accessible contents.

Following this strategy, the following channels have been used in the two testbed hospitals and are suggested to be used to spread the educational content to the patients in any healthcare organizations:

- Clinical apps: ProTego toolkit will be used by two apps, Pocket EHR and FoodCoach. These apps can act as vehicle to broadcast the educational material to the general population. By including a section in the apps that takes the user (patient) to the educational website the user will have it accessible from a tool that is of interest for him. Future apps that aim to be ProTego-ready will be required to accept the same behaviour, this is, to have a dedicated cybersecurity section that links to the ProTego educational Website.
- As mentioned before, posters in paper format will be placed in different places, some of them reachable by patients as nursery controls on wards. The posters include QR codes that patients can use to access the educational content.
- Calling monitors: it is common that hospitals use automatic procedures for calling patients to external consultancies. Those monitors, except when the call is made, are showing TV signal or any other content of interest for the hospital, like remembering flu vaccination, or health campaigns in place. Those monitors can be used to show the posters in digital format, letting patients to access the educational website.

Summarizing, the contents of the educational website address the needs of the patients so they can obtain easy-to-understand recommendations regarding the three areas that represent the major source of risk for their role in the management of health data: password management, social engineering and management of mobile devices.

The dissemination mechanisms used introduce cybersecurity in the relationship between the patients and the hospital or healthcare organization. They cover both the virtual side by

introducing a dedicated section in the apps provided, and the physical side by making present cybersecurity messages while patients are on site at the hospital.

VI. EDUCATIONAL MATERIAL FOR IT STAFF

VI.1. Introduction

It is important to put in context the role of the IT staff in the ProTego project. As mentioned above, ProTego is a toolkit that offers tools for risk assessment and risk reduction. The following figure illustrates the location of ProTego in terms of interaction with users and applications:

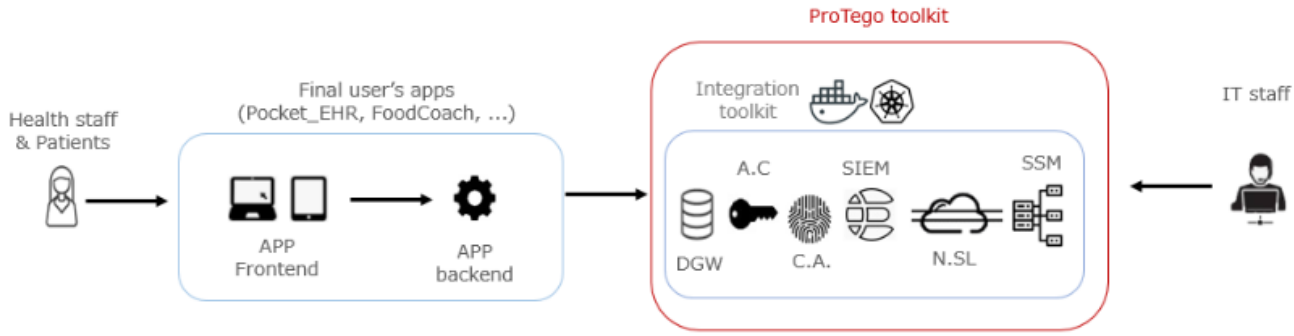


Figure 21: User interaction with the ProTego toolkit

Health staff and patients will interact with front-end user applications that will interact with its own backend, and that backend is which will interact with the ProTego toolkit. From this point of view there is no direct interaction between end-users and the ProTego toolkit, and the IT staff could be considered as the end user of the ProTego toolkit since it is the user group that will have direct interaction with it.

IT staff will be the responsible of:

1. Assess ProTego adoption: understand the functionality of the ProTego toolkit and its containing components to assess the suitability of including the ProTego toolkit in the Hospital IT map
2. Provision of requirements: provide the required infrastructure to deploy the ProTego toolkit
3. Deployment of ProTego: deploy and configure the ProTego toolkit
4. Use o ProTego: Manage and use the ProTego toolkit, reacting to the threats raised by the system

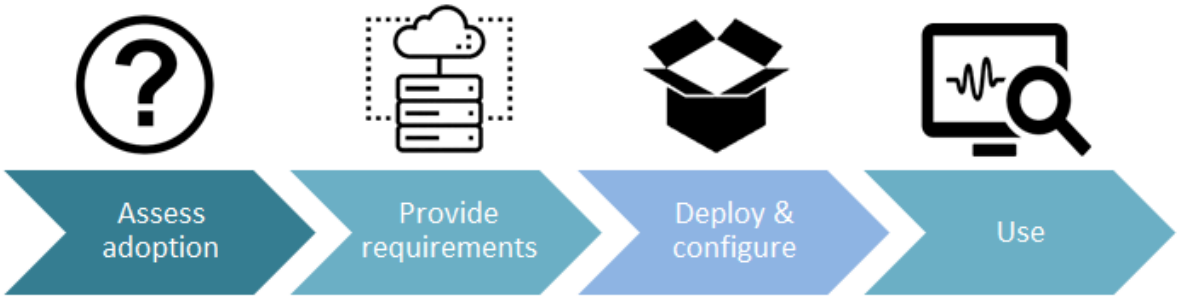


Figure 22: Phases for ProTego adoption

VI.1.1. Personas

The following sections will dive into the previous four points, addressing the information needed to the two archetypical user "Personas" defined in deliverable D2.3 (Network Operator and IT Infrastructure Manager) as they represent the most common division of roles in the structure of IT departments in current healthcare organizations.

	*"I guarantee the availability of the hospital infrastructure"*
User role	Network operator
Description	Carlo, 38 years old. He works as a network operator in the IT department of the hospital. He is in charge of installing configuring and maintaining the network components within the hospital infrastructure. His primary duty is to monitor and analyze the network, eventually resolving network issues in order to maximize uptime. As part of his job, Carlo performs technical research on network upgrades to address short-, mid- and long-term necessities.
Goals	His goal is to collaborate with the other technical staff to ensure connectivity, compatibility and availability of the system.
Needs & opportunity	• He needs to uphold confidentiality when it comes to information regarding the networks

Table 8: Carlo, the "Network operator" persona

	*"I manage the functioning and security of the hospital's IT infrastructure"*
User role	IT infrastructure manager
Description	Andrew, 45 years old. He works as an IT infrastructure manager in the hospital IT department. He is responsible for planning, managing and designing the IT infrastructure and coordinating the team responsible for maintaining this infrastructure. Given the nature of his work,

	he is able to effortlessly assume a technical or managerial role. Indeed, almost every task in which the IT department team is involved, from performing routine system updates to the installation of new components, is executed under his supervision. In parallel, he collaborates with colleagues and heads of other departments in order to develop strategies that will help his team better align with the company's overall strategy. Passionate about his work, in his spare time he devotes himself to writing technical guides on system automation and the Linux operating system.
Goals	His goal is to ensure the functioning and security of the entire IT infrastructure. By doing that, he guarantees that all data in the infrastructure are used, transmitted and stored appropriately and securely.
Needs & opportunity	• He wants to integrate new applications in the hospital infrastructure • He wants to secure data in use, in transit and at rest • He wants to assess the cybersecurity associated with the infrastructure

Table 9: Andrew, the “IT Infrastructure Manager” persona

VI.2. Assess ProTego adoption

This section is addressed to both ”Network Operator” and ”IT Infrastructure Manager” personas, since both will be in charge of deciding if the toolkit can be adopted in the healthcare organization. With such objective, it will be presented an overview of its components and describe the modularity and versatility the toolkit offers, what can lead to easy adoption.

It is worth to mention that ProTego adoption means its integration with the applications already present in the IT map of the healthcare organization, and with those that will come in the future. In the section VII – Educational Material for external providers it will be detailed how the applications should integrate with each component of the toolkit from the application provider’s perspective.

That section is also of interest by the IT staff since they act as application providers for those self-developed applications, and also must have an overview of the compatibility of those provided externally with the ProTego toolkit.

VI.2.1. Overview of the ProTego toolkit

ProTego provides a toolkit, the ProTego toolkit, for healthcare organizations to better assess and reduce cyberrisks related to access to Health Data, including risk assessment and risk mitigation tools.

As stated in the previous definition, the ProTego toolkit is composed of set of tools divided in two categories: risk assessment and risk mitigation. Below there is a short description of such elements and more fine grained description could be found in the deriverable D4.3 for the risk assessment tools and D5.3 for the risk mitigation tools.

Risk assessmment tools:

System Security Modeller (SSM): SSM is a web-based graphical tool which allows a system designer or analyst to perform a design-time risk assessment of a system. It is primarily a tool

for “design time” analysis. That is, it assists the user in describing a socio-technical system, letting them specify the impact of different threat consequences (“misbehaviours”) and lets them understand which controls are necessary and sufficient to reduce the risk level to an acceptable level. Ideally, this is all done at the point of designing the system so that when the system is implemented it is sufficiently secure with the controls already in place. Of course, the tool can also be used to model existing systems and assess the risks as they are or after proposed changes.

But beyond this, it can be integrated with runtime monitoring systems (SIEM) to make the model consistent with the real-time status of the system and provide a decision support system for determining what to do to control emerging threats.

To perform the model of the system it is needed that the IT staff will be trained in the use of the tool. In the APENDIX C it has been included a tutorial that explains the basics of the tool and the main concepts regarding cybersecurity risks that need to be assimilated.

Security Information and Event Management (SIEM)

The SIEM is the ProTego tool that monitors security during run-time. That is accomplished by collecting information from various sources, enriching data, correlating different pieces of information, and analysing all the set.

It is composed by a set of different independent Open Source tools already available, integrated and working together, that carry out the different tasks that are necessary to be performed by the SIEM.

In the basics, it collects logs from different sources (data lakes) that are then correlated by a correlation engine to raise alerts when threads are detected, based on rules defined into the engine.

It is integrated with the rest of the components of the toolkit:

- SSM: the SIEM will send to the SSM information about vulnerabilities discovered so that risk can be automatically recalculated. This is a very important aspect of the ProTego toolkit since as far as we know there is no other solution that accomplishes that, since all existing risk assessment tools perform risk recalculation based on manual procedures. This very aspect is where the tools developed in WP4 go beyond the State of the Art.
- Data Gateway: the SIEM receives and notifies alerts detected by the Data Gateway such as, for example, possible data tampering or illegal authorization attempts.
- Access Control Framework: the SIEM receives and notifies alerts detected by the Access Control Framework since it is tightly integrated with the Data Gateway.
- Continuous Authentication: the SIEM receives and notifies alerts detected by the Continuous Authentication backend, such as, for example, unusual behaviour of a user.

Risk mitigation tools:

Data Gateway (DGW)

The DGW acts as the persistence layer inside the ProTego toolkit. The DGW stores FHIR (Fast Healthcare Interoperability Resources) in encrypted Parquet format, and allows for powerful SQL queries of the stored data.

Conceptually, the Data Gateway consists of two subcomponents:

a) A FHIR server which receives FHIR requests over REST to store FHIR resources as encrypted Parquet files,

b) A Query Gateway which implements a REST end point to receive SQL queries and execute them against the encrypted Parquet files.

The data can only be accessed if the Control Access Framework (see below) does validate the credentials sent in the request and, thu, provides the DGW a valid criptographic key to decrypt the data.

Access Control Framework (A.C.)

The main application of the A.C. component is to enhance the security of the Data Gateway (DGW) by ensuring that only authorized users can have access to FHIR data that is stored within the parquet encrypted files . It consists of the following two sub-components:

a) Key Management Service (KMS): This component is used to protect the Key Encryption Keys (KEK) that are needed by the Data Gateway to access FHIR data. The KEKs are not stored directly in the KMS, but are encrypted/decrypted with a master key that is stored internally in the KMS. Therefore, when access to FHIR data is needed, the DG will make encryption/decryption queries to the KMS to get access to the corresponding KEK.

b) Access Control (AC): This component is used to manage the encryption/decryption queries made to the KMS, and decide whether the KEK should be sent to the DG or not. This decision depends on whether the data access request – which triggered the DGW to query for the KEK – should be granted or not.

The KMS and AC jointly realize the access control framework functionality. However, besides interacting with the DG, it is indirectly also linked to an **external IAM**. The latter is not one of the components developed by ProTego, but is needed to make access control decisions. The main goal of the IAM is to manage all the users in the system and their respective roles and/or attributes (e.g., being a doctor in hospital x). Users authenticate to the IAM, and receive a JSON Web Token (JWT) upon successful authentication. These tokens are digitally signed by the IAM.

Network slicing (NSL)

NSL covers the protection of data in transit by partitioning the network into logical networks. That can not only improve the resource management among different services, but also the security of each service. Logical isolation adds an extra layer of security, avoiding interaction between different network overlays. It has two main functions:

a) Data channel confidentiality: multiple slices can be created over the underlying network infrastructure, having each of them its own properties and requirements and isolating the traffic from the rest, meaning data from one slice cannot move to another. That brings out relevant enhancements regarding cybersecurity:

- Security protocols - Support for security protocols within each slice.
- Communication isolation - No support for communication between slices or supported communication between slices under strict rules.
- Cybersecurity assurance - If one slice is compromised, this should not influence the other slice

b) Data channel bandwidth allocation: The second function of network slicing is to provide data channel bandwidth allocation. Network slices are created on top of the physical network infrastructure. Therefore, one needs to specify which resources are used by each network slice. This allows us to create different resource allocations for each slice. In the context of ProTego, this means that we can create slices with more allocated resources, such as bandwidth

Continuous Authentication (C.A.)

The continuous authentication (CA) system is the main component centred in mobile device security. CA is a method of verification that continuously monitors and authenticates users

based on collected data. Through this component ProTego is capable to identify the authorized users and unauthorized users of mobile devices.

The continuous authentication system is composed by the following main components:

1. **C.A. Agent:** This component is a mobile agent that retrieves behavioural metrics and sends them to the API. The CA agent performs as an Endpoint Detection and Response (EDR). The main task of this component is to retrieve information to continuously authenticate the user, but it also has response capabilities. For example, CA agent can raise a security alert to inform other components like the SIEM.
2. **C.A. API:** This component is a backend that centralizes the logs and associates each of them with the users' identity. Periodically, this API generates machine learning models based on the logs stored and evaluates the new incoming logs against these models.

These two components are responsible of the correct performing of the CA system. A typical behaviour for checking the device user authorization will be the following: the CA agent periodically asks for the trust of a user; the backend checks all the logs stored since the creation of the model and returns a value between 0 and 1 (a trustworthiness percentage).

Integration toolkit

All these components are integrated together by an Integration Toolkit which provides a packaging, provision, orchestration toolkit. It provides a platform to deploy, manage and orchestrate them by means of a multi-node kubernetes cluster plus a Rancher UI that provides user-friendly interface.

The components of the ProTego toolkit are provided as dockerized applications, packaged in Helm charts. From the Rancher UI the administrator can easily find the components catalogue to deploy new components or update the already deployed to latest versions. It is also possible to monitor the status of the cluster's worker nodes and the applications running into the cluster.

The Integration toolkit also takes care of the integration of the elements within the ProTego toolkit in a way that it is transparent for the administrator how these elements communicate as everything happens internal to the cluster and the requirements to perform the integration are built inside the cluster.

The Integration Toolkit is provided as an installation bundle, packaged as a Docker container, containing all necessary software and links to deploy and configure the Kubernetes clusters, deploy Rancher, other software like Istio, and deploy the ProTego components.

This installation bundle also provides an installation UI for a more user friendly installation process with detailed instructions on what's being performed in each step and possible manual steps that need to be performed by the user.

More detail of this element can be found in D6.3.

The following table resumes the elements of the ProTego toolkit:

ELEMENT	DESCRIPTION
SSM	Risk assessment in design time for both new or already existing systems. Dynamic re-assessment if combined with the SIEM
SIEM	Monitoring security during run-time. Logs correlation to detect threads.
DGW	Persistence layer. Interface to store/retrieve data. Encrypts FHIR formated data through advanced encryption. And stores it in parquet encrypted files. Allow SQL for retrievals. Dependence on A.C. as authorization system.

A.C.	Uthorization system. Assess the requests to allow/deny the access to the data. Keeps the Key encryption Key required by the DGW to access it. Requires a JWT token that should be provided by the client once obtained from an external authorization system.
C.A.	Provides verification of the users interacting with the applications through mobile devices. Keeps a 'trust level' indicator that let applications from both inside or outside the Protego toolkit to detect and react if the identity of a user has been compromised.
NSL	Allows the creation of SDNs to isolate the traffic based on certain communication parameters. Provides confidentiality and specific resource allocation to each slice. Prevents that problems in one slice impacts on other's minimizing the risks of loose of integrity or availability of critical systems/services.

Table 10: Resumed functionality of the ProTego toolkit components

VI.2.2. Modularity and versatility for easy adoption

IT staff have within their main roles to assess the suitability of adopting new systems into the organization. They should understand if there is any overlap or incompatibility between the assessed system and the current IT map of the organization. To facilitate adoption, ProTego toolkit offers modularity and versatility.

VI.2.2.a. Modularity

The ProTego toolkit can be adopted in a modular way, that is, the elements don't have dependences that obligate potential adopters to make an "all or none" decission. The only dependences are:

- A.C. and DGW that should work together since the A.C. is needed to provide acces to the data controlled by the DGW
- Integration toolkit that should act as platform for the ProTego toolkit, whichever the toolkit elements selected would be.

With the described dependence between A.C. and DGW, we can make a Karnagh map with 5 variables to show all the possibilities. The Integration toolkit is left over because it is required for any combination of the elements since it provides the basic platform over which all the elements are deployed and used:

#Combination	RISK ASSESSMENT		RISK MITIGATION		
	SSM	SIEM	DGW/ + A.C.	C.A.	NSL
1	YES	YES	YES	YES	YES
2	YES	YES	YES	YES	NO
3	YES	YES	YES	NO	YES
4	YES	YES	YES	NO	NO
5	YES	YES	NO	YES	YES
6	YES	YES	NO	YES	NO
7	YES	YES	NO	NO	YES
8	YES	YES	NO	NO	NO
9	YES	NO	YES	YES	YES
10	YES	NO	YES	YES	NO

11	YES	NO	YES	NO	YES
12	YES	NO	YES	NO	NO
13	YES	NO	NO	YES	YES
14	YES	NO	NO	YES	NO
15	YES	NO	NO	NO	YES
16	YES	NO	NO	NO	NO
17	NO	YES	YES	YES	YES
18	NO	YES	YES	YES	NO
19	NO	YES	YES	NO	YES
20	NO	YES	YES	NO	NO
21	NO	YES	NO	YES	YES
22	NO	YES	NO	YES	NO
23	NO	YES	NO	NO	YES
24	NO	YES	NO	NO	NO
25	NO	NO	YES	YES	YES
26	NO	NO	YES	YES	NO
27	NO	NO	YES	NO	YES
28	NO	NO	YES	NO	NO
29	NO	NO	NO	YES	YES
30	NO	NO	NO	YES	NO
31	NO	NO	NO	NO	YES

Table 11: Catalogue of possible configurations of the toolkit

That allows the adoption on the toolkit selecting which elements the organization wants to include if, for example, there are restrictions that makes unsuitable some elements to be deployed in the organization. And also allows to perform a progressive deployment if, for example, there is a restrition with any element in a moment of time, and this restriction gets later overcomed and the ”banned” element is allowed be added to the toolkit.

With clarifiction purposes, we describe some examples which ilustrate possible reasons for not selecting each of the toolkit elements:

- SSM: the organization is pplanning to make significative changes to the network infrastructure in the short term. As it may have such a big impact on the model of the system to be entered into the SSM, the adoption of this element will be hold over those changes will be applied.
- SIEM: the organization already has a SIEM tool, connected to the current systems. Instead of moving right now to a new SIEM, they decide to connect the ProTego toolkit elements with the current one, and hold over the decission of swaping it.
- DGW / A.C.: The organization decides to not change the way the data is stored and retrieved because it would imply many changes to the applications currently running.
- C.A.: The organization has not any mobile device app, all the applications are operated via PC.
- NSL: the organization is pplanning to make significative changes to the network infrastructure in the short term. That will change the catalogue of networks available over which the slices would be created. Because of that they decide to hold over the adoption of this component.

Without this modularity, any of the described situations would lead to discard the adption of ProTego, but wit the modularity described, it only implies the concerned element to be delayed so it can be assessed and adopted at the most suitable time.

VI.2.2.b. Versatility

The versatility of the ProTego toolkit is to be assessed in regards of which “kind” of environment does it need to be deployed, and which ways of integration it provides to integrate with external elements. That is important because the ProTego toolkit will be part of an already existing ecosystem with running applications it will surely must interact with.

The versatility of the ProTego toolkit relies mainly on the Integration toolkit it uses. All the components are provided as Helm charts wrapping docker images of the toolkit components. And those components are then deployed into a Kubernetes cluster, which is the underlying platform, from a functional perspective.

This Kubernetes cluster can be provided and hosted in many different environments, as it has been demonstrated by the two different use cases: from the hospital premises version illustrated in the FoodCoach scenario, to the cloud premises one used in the Pocket EHR scenario.

The only element of the ProTego toolkit that has higher dependence on the underlying infrastructure is the Network Slicing and a subset has to be deployed in the hospital premises. That’s because the slices that will be created within the hospital network infrastructure and the software elements governing the slices should be close to it to reduce the latency. More detail in D5.3.

Besides this, the interfaces provided by the toolkit are REST services, which is a broadly used standard for communication between applications. There are a few exceptions to this:

- SIEM: the SIEM needs to use log sources. For that purpose if offers a set of different possibilities (agents) that allow from the consumption of logs in text format, to the connection to AWS cloud S3 buckets as event sources. It also exposes kafka topics, so the applications can push the data, instead of just offering it.
- C.A.: while the Continuous Authentication backend does offer a REST service for integration, there is also a frontend layer that should integrate with the end user app (FoodCoach, Pocket HER) to communicate. If offers a native “java” integration for those apps built in java, as FoodCoach. But for applications built in different languages, it also offers integration via “intents” at the O.S. level of the mobile device, as it has been implemented in Pocket EHR.
- A.C.: The access control needs an external authentication system. The only requirement is that the external authentication system uses JWT. So any system supporting this standard would be able to integrate with ProTego.

VI.3. Provision of requirements

In order to successfully deploy the ProTego toolkit the organization has to provide the infrastructure needed, in terms of platform resources and comunications. As it has being said, the ProTego toolkit can be seen as a modular system so the requirements would vary depending on the selected components, but this section will assume a full deployment, that is, with all the components.

Deliverable D6.3 offers a detailed description of all the requirements, differentiating between integration, interoperability and resources, but mainly focused on the ProTego toolkit. In this deliverable we will offer a broader vision, considering the outsider elements as the applications that will integrate with ProTego.

As the information is to be addressed to different ”*personas”* it will be split on this basis:

PERSONA	REQUIREMENT TO BE PROVIDED
IT Infrastructure Manager 	Provide a Kubernetes cluster with two worker nodes with this minimum hardware capacity - 2 CPUs - 8 GB RAM - 128 GB disc space
	Define the log sources for the SIEM
	Provide an authentication system compatible with JWT
	Define the user roles that will serve as the base of the authorization mechanism to access the data
	Ensure that external aplications integrating with ProTego's Data Gateway are FHIR compliant

Table 12: Requirements - IT Infrastructure Manager

PERSONA	REQUIREMENT TO BE PROVIDED
Network Operator 	Provide a Wi-Fi network to create the network slices over it

Table 13: Requirements - Network Operator

VI.4. Deployment and configuration

The following tables contains the main actions that should be taken into account while deploying the ProTego toolkit, and are also divided into those addressed to the ”IT Infrastructure Manager” and to the ”Network Operator” persona.

PERSONA	ACTION TO BE PERFORMED
IT Infrastructure Manager	Deploy the ProTego toolkit components into the kubernetes cluster via the Rancher UI **a detailed guide on how to do this will be provided in 7.4 as the tool is going to offer improvements from its current version*
	Create the system model into the SSM (shared rask)
	Create SIEM agents (log consumers) according to the type of log sources that the SIEM will analyze

	Create SIEM rules to detect threats and raise alarms
	Ensure the users identity in the authentication system contains the role feature in order to be used by the A.C. to allow the appropriate access to the healthcare data
	Add the tag ”`custom:aud`” to the JWT used by the authentication system and set it to the endpoint where the agent intalled in the mobile device will request for continous authentication of the user.

Table 14: Deployment - IT Infrastructure Manager

PERSONA	ACTION TO BE PERFORMED
Network Operator 	Create the system model in the SSM (shared rask)
	Isolate the ProTego toolkit in a separate network
	Provide connectivity from the Protego toolkit to the external applications that will interact with it, by exposing only the ProTego REST endpoints to the networks they are going to be requested from.
	Create the network slices to isolate the traffic from different applications, or group of applications.

Table 15: Deployment - Network Operator

VI.5. Use of the ProTego toolkit

Once the ProTego toolkit has been deployed it is the time to start using it. As previously explained, the ProTego toolkit is formed by risk assessment and risk mitigation tools.The use of the toolkit is mainly related to the risk assessment tools, as the risk mitigation tools (DGW / A.C., C.A., NSL) are silent modules that introduces security to the data at rest and in transit but will not advise users for any situation that would require actions to take. However the risk assessment tools promote the interaction with the users (IT staff) to improve the overall security and to respond to threats detected.

The interaction with the ProTego toolkit, thus, will be made trhough the SSM and the SIEM.

SSM: during the deployment phase of ProTego a model of the system has been created, in a shared task between the Network Operator and the System Infrastructure Manager. The SSM offered the overall risk index of the system and suggestions to apply certin controls (configurations) to the components inside the model to reduce risks to an acceptable level, or even avoid them.

The task for both the IT Infrastructure Manager and the Network Operator is to explore the model, review those suggestions and decide which of them could be applied. By doing this they will reduce the risk level of the concrete components the controls would be applied to, and as a consequence for the whole system.

The previous is the ”static” part of the operation, but there is also a ”dynamic” part: the SSM is integrated with the SIEM and that allows that threads detected by the SIEM during real time operation could vary the trustworthyness of some components and increase the risk level. Because of that it is also needed to make periodic reviews to detect any increase in the risk level and react to it by assessing the recommendations triggered by the SSM and applying those that are suitable and have a higher impact in risk reduction.

Both for those static and dynamic actions, the SSM allow users to assess the result of any action under evaluation without changing the system, so those suitable controls that will have a higher impact can then be translated to the real system, making easier the process.

The review should be made first taking care of the most critical risks, because by solving or reducing them, some of the lower level risks will also be mitigated, due to a cascade effect.

Another taks that has to be performed is the maintenance of the system model, that is, the system model should be updated to reflect the current status of the real system. That implies that the changes on the real system should be reflected on the system model to ensure the SSM will offer the actual risk level and the actual impact of controls under evaluation.

SIEM: during the deployment and configuration phase of the SIEM, it has been decided wich elements of the IT infrastructure will become log producers for the SIEM, and wich risks are to be triggered by the design of rules inside the SIEM engine. It is worth to say that the previous is reffered to elements outside the ProTego toolkit because the toolkit comes with predefined integration between the SIEM and the rest of elements, and built-in rules to raise abnormal situation representing risks that should be attended. From this starting point, the operation of the SIEM consists of:

- Assess the scope of the SIEM, that is, if any new system or application should integrate with the SIEM. If so, the new element should become a log provider in wether a passive (by creating an instance of the SIEM agents according to the type of log produced by that system) or active way (by offering a Kafka endpoint via REST resvice so the system can send logs through it). Then it is needed to create rules to detect risks from the consumed logs, both isolated or correlated with the logs of other systems already conected to the SIEM.
- Passively react to alerts raised by the SIEM: Depending on the assessment performed and the corresponding configuration, the SIEM will raise alerts with different severity levels. The severity level indicates how serious or important the alert is. During the configuration phase it is decided what severity levels will be notified by special means, such as email, instant messaging applications such as Telegram or Microsoft Teams, or even other means. Operators especially review alerts notified by these special means to respond to possible threats.
- Actively access to the Kibana UI offered by the SIEM: Regardless of the severity level of each alert, all alerts are available to be checked at the UI. Therefore, once the most important alerts are taken care of, operators also review alerts with lower severity levels deciding whether any further action is necessary in response to the possible threat.

VI.6. Summary

This section is devoted to recap of the main points to be observed by each IT staff persona along the four stages in which the whole process has been divided. The aim is to offer an overview of the tasks under each persona's responsibility, so they can find a guide to successfully use the ProTego toolkit.

PERSONA	STAGE	ITEM
IT Infrastructure Manager	Assess ProTego adoption	Understand the ProTego toolkit in terms of functionality and requierements and assess if/how it can be adopted in teh Organzation
	Provision of requirements	Provide a Kubernetes cluster with two worker nodes with this minimum hardware capacity

		- 2 CPUs - 8 GB RAM - 128 GB disc space
	Provision of requirements	Define the log sources for the SIEM
	Provision of requirements	Provide an authentication system compatible with JWT
	Provision of requirements	Define the user roles that will serve as the base of the authorization mechanism to access the data
	Provision of requirements	Ensure that external aplications integrating with ProTego's Data Gateway are FHIR compliant
	Deployment and configuration	Deploy the ProTego toolkit components into the kubernetes cluster via the Rancher UI **a detailed guide on how to do this will be provided in 7.4 as the tool is going to offer improvements from its current version*
	Deployment and configuration	Create the system model into the SSM (shared rask)
	Deployment and configuration	Create SIEM agents (log consumers) according to the type of log sources that the SIEM will analyze
	Deployment and configuration	Create SIEM rules to detect threats and raise alarms
	Deployment and configuration	Ensure the users identity in the authentication system contains the role feature in order to be used by the A.C. to allow the appropriate access to the healthcare data
	Deployment and configuration	Add the tag ”`custom:aud`” to the JWT used by the authentication system and set it to the endpoint offered to allow the C.A. agent request for continous authentication of the user.
	Use of the toolkit	Keep the system model updated by reflecting changes in the real system
	Use of the toolkit	Review risks revealed by the SSM from more to less criticity and assess their application to the real system. Repeat the task until the overall level of risk of the system is set to a level accepted by the organization.
	Use of the toolkit	Integrate applications external to the ProTego toolkit with the SIEM
	Use of the toolkit	React to the alerts raised by the SIEM, regarding IT infrastructure
	Use of the toolkit	Proactively review the SIEM’s Kibana UI

Table 16: Summary - IT Infrastructure Manager

PERSONA	STAGE	ITEM
Network operator 	Assess ProTego adoption	Understand the ProTego toolkit in terms of functionality and requierements and assess if/how it can be adopted in teh Organzation
	Provision of requirements	Provide a Wi-Fi network to create the network slices over it
	Deployment and configuration	Create the system model in the SSM (shared rask)
	Deployment and configuration	Isolate the ProTego toolkit in a separate network
	Deployment and configuration	Provide connectivity from the Protego toolkit to the external applications that will interact with it, by exposing only the ProTego REST endpoints to the networks they are going to be requested from.
	Deployment and configuration	Create the network slices to isolate the traffic from different applications, or group of applications.
	Use of the toolkit	Keep the system model updated by reflecting changes in the real network infrastructure
	Use of the toolkit	Review risks revealed by the SSM from more to less criticity and assess their application to the real system. Repeat the task until the overall level of risk of the system is set to a level accepted by the organization.
	Use of the toolkit	React to the alerts raised by the SIEM, regarding the network infrastructure
	Use of the toolkit	Proactively review the SIEM's Kibana UI

Table 17: Summary - Network operator

VI.7. Oppinion about the ProTego toolkit

The ProTego toolkit has been presented in a way that its primarly users, represented by the IT Infrastructure Manager" and the "Network Operator" personas, can undesrstand its components, functionality, scope and the required actions to adopt it.

Now it is time to assess their oppinion about the toolkit itself. That has been made by means of an interview with the IT staff representing both archetypical roles in both Marina Salud and OSR hospitals.

The interview has been selected, over the survey, as the vehicle to gather such opinion because it allowed the ProTego team to structure it in a way that covers all the main subjects to be observed while allowing the interviewees to express themselves freely about what they consider relevant.

The interview has been designed to cover these main subjects:

<table>
<tr><th>ID</th><th>Subject</th></tr>
<tr><td>#1</td><td>Does the scope covered by ProTego match areas in which there is a lack of cybersecurity controls within your organization? Explain which ones.</td></tr>
<tr><td>#2</td><td>Do you think ProTego would help to reduce cyber-risks in your organization? Explain why.</td></tr>
<tr><td>#3</td><td>Do you think ProTego would increase situational awareness under an attack and improve the response time?</td></tr>
<tr><td>#4</td><td>Can you identify features offered by ProTego that apply to each item on the following table? Short description.
<table>
<tr><th colspan="2" rowspan="2">ProTego toolkit</th><th colspan="3">STATES OF DATA</th></tr>
<tr><th>Data at rest</th><th>Data in transit</th><th>Data in use</th></tr>
<tr><td rowspan="3">CYBER-SECURITY DIMENSIONS (CIA TRIAD)</td><td>Confidentiality</td><td></td><td></td><td></td></tr>
<tr><td>Integrity</td><td></td><td></td><td></td></tr>
<tr><td>Availability</td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>#5</td><td>Can you identify any feature offered by ProTego that is not covered by applications already in the market, as far as you know? List them.</td></tr>
<tr><td>#6</td><td>Do you think the ProTego toolkit would be suitable to be adopted in your organization? Explain why.</td></tr>
<tr><td>#7</td><td>which contras can you see in the ProTego toolkit? Explain.</td></tr>
</table>

#8 Please summarize the opinion about the ProTego toolkit from the scope of each of the following roles you are in charge of:

User role	Description	Opinion about the ProTego solution
Network operator	Network operators manage the network capabilities of the hospital. They need to guarantee that the network meets the necessary quality of service attributes	
Data operator	Data operators are in charge of data flows and how they are stored within the hospital infrastructure. Data operators must guarantee that sensitive data are stored with an appropriate level of protection	
Security operator	Security operators take care of the security concerns of the hospital infrastructure. These include controlling access to the hospital services, assessing the risk associated with the infrastructure, and monitoring the data exchange for possible attacks and foreseeable risks	
System operator	System operators are responsible for installing, configuring and managing computer systems in the hospital infrastructure	
Administrator	Special role capable of making unrestricted, system-wide changes (e.g., registering accounts for other IT operators)	

Table 18: Interview for IT staff

The collection of the IT staff opinion will be gathered in further stages of the ProTego project and included in D7.4. The reason of this is that at the time of preparing the current D3.3 deliverable the toolkit has recently been completely deployed in both partner hospitals (MS and OSR) and by letting a time period to better test the toolkit it will be possible to get a more real opinion about it.

VI.8. Medical devices - IO(m)T

IoT devices suppose a point of high interest to be covered in any initiative regarding cybersecurity in healthcare. But in this project we will make a difference between small and personal wearable devices (IoT devices) and electro-medical devices commonly owned and used by healthcare organizations, also named as IO(m)T devices.

This section will cover the IO(m)T devices because the means of adding cyber-security has more implications for the IT staff, while the general wearable IOT devices will be covered within the section devoted to the external providers, concerning specifically to those (IoT devices).

VI.8.1. Diagnose of current situation

To make possible to understand which are the cyber-security problems that the current market situation of IO(m)T introduces it is necessary to describe it. Electro-medical devices are not usually isolated but instead they come within a sub-infrastructure provided by the manufacturer. The figure below illustrates this:

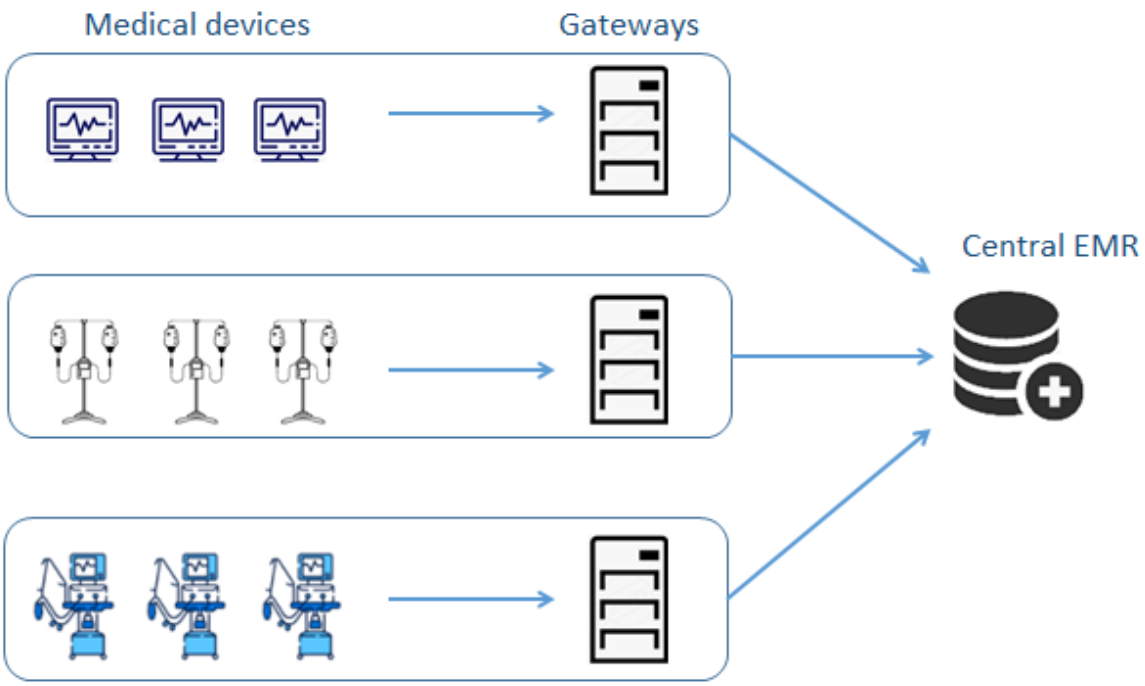


Figure 23: IO(m)T systems

There are three major asset types in this scheme:

- Medical devices: are the electro-medical devices that get connected to patients, performs a concrete action and collects data from him. Examples of these can be vital signs monitors, infusion pumps or ventilators, just to name some of the most frequently used. They perform very simple logic as the ”intelligence” is delegated to the gateway.
- Gateways: act as the central controlling and monitoring point of each ”subnet” of electro-medical devices. They are provided by the vendor as part of the turnkey system acquired. They keep the data persistent while the devices remove the data collected once it has been sent. The data is transferred from the devices to the gateway in non-standard formats and the gateway is in charge of translating that data into open standards like HL7 to send the data to the Central EMR, if the capability is enabled. Anyway, they will keep a copy of the data, making the integration with the EMR an extra added functionality. So they become a source of medical persistent data that should be appropriately managed.
- Central EMR: Is the central repository of medical data within the organization. As it contains all the data referring to patients that come from several origins, is where the intelligence and CDSS will take place, by combining vital signs, antecedents, medications, allergies, etc.

It is also common that each set of medical devices, jointly with the corresponding gateway, requires to be isolated in a private LAN and the communications between the elements are performed via broadcast. That way it is reduced the need of controls, and new elements connected to the private LAN will be automatically connected to the gateway, what often leads to a lack of filiation of what devices are in place at the hospital at each time, which is an evident risk.

But over than the technical details, it makes sense how the procurement of those kind of devices is performed. First of all it is the medical staff who decides which kind of devices they need, select the concrete models with only medical considerations, and arrange the purchase directly with the vendor. The IT staff, that is in charge of the cyber-security, does not take part on the procurement process and is only asked to provide the infrastructure and communication requirements so the devices can be deployed into the hospital. By the described communication

model, via private WLAN, the lack of control is almost total, since new devices could be included without any notice to the IT staff.

Following that apparently extreme but real instead scenario, the provider installs the devices and gateway letting gateway's password easy to remember to the health staff that has directly managed the procurement. As it has been the health staff, no requirements about the O.S., antivirus, etc. has been requested, and all it depends on the good or bad behaviors the provider has.

At this point, to make possible to identify which patient would be the medical device connected to (and consequently who belongs the data to), it will be necessary that the health staff operates the medical device to perform administrative actions, like register the patient. That operation can be avoided through *integration* as it will later be explained, and so the risks derived from it will be mitigated as well.

At the end of this process, the healthcare organization will have a situation which clearly has increased the risk level by many different factors:

- New hardware and software elements included in the IT infrastructure, with no obligation to have them all registered.
- No restrictions about the software components (O.S. antivirus)
- No updating policies have been ensured
- Communications performed by broadcast within the private WLAN created for each device group. By simply accessing that LAN anyone can have access to the data transmitted.
- Password management is not ensured, as it has been delivered to health staff.
- The link between each medical device and the corresponding patient is not ensured as it is performed by manual operation by the health staff.
- New health data sources will be introduced, in each gateway server, with no guaranties of appropriate management (backup, recover plans, encryption, etc.).
- The overall risks for the entire organization could not be assessed and the IT staff will not have the whole information about the system.

With the previous decription, it can be clearly seen that the objective of introducing security to the IO(m)T will not require only technical measures, but a complete redefinition of the whole process instead, including changes at organizational levels.

VI.8.2. Proposal

The strategy proposed is alligned with the "Procurement guidelines for cybersecurity in hospitals" report by ENISA [19]. But while this ENISA document is intended to cover all type of procurements in a hospital and includes remote care systems, mobile client devices, identification systems,building management systems, network equipments, medical devices, clinical information systems, industrial control systems, professional services and cloud services, this section is focused only on medical devices and will help to better understand the measures suggested.

ENISA remarks a set of good practices to be applied during the whole procurement process, that it divides in three main phases: Plan, Source and Management. The whole list of good practices suggested will be later depicted but it is worth to list those considered as general ones:

- Involve the IT department in procurement
- Vulnerability management
- Develop a policy for hardware and software updates

- Secure wireless communication
- Establish testing policies
- Establish Business Continuity plans
- Consider interoperability issues
- Allow auditing and logging
- Use encryption

It is needed to remark that all it starts with the "Involve the IT department in procurement", since without this we get the current situation described in the previous section, with no control of what is actually included in the IT map and so with less possibilities to set up the appropriate controls and measures. In other words, "you can't control what you don't know about".

The initiative to acquire any new medical device or equipment comes from the health staff, who detects the need. They must pre-select those in the market which satisfies their requirements in terms of medical consideration. After this pre-selection, the IT staff will be involved into the process. They should contact with the IT department of the device providers and gather the information to make an assessment of the candidates:

QUESTION	BEST RATED OPTION
Does the provider own a certification regarding cyber security concerns?	The provider is certified in any of the recognized standards, as ISO 27001
Do the devices require a gateway server?	Recent version with update policies allowed
O.S. versions of the devices and the gateway, and update policies	Recent version with update policies allowed
Antivirus version of the devices and the gateway, and update policies	Best antivirus with update policies allowed
Allow the devices and gateway to install the corporate antivirus?	Corporate antivirus allowed
Do the elements require a private WLAN?	Don't require a separate WLAN
Do they use broadcasting or communication point to point?	No broadcasting used
Data format for data sent between devices and gateway.	Descriptive. No preference
Are those communications encrypted (TLS)?	TLS enabled
Data formats allowed between the gateway and the hospital data sources.	Standard HL7 formats
Are those communication encrypted (TLS)?	TLS enabled
Does the gateway (and thus, the devices) allow reception of patient demographics and orders? Description of HL7 events allowed.	Gateway allows HL7 ingestion and act as a master for the devices
Does the gateway collect logs that allow detecting abnormal situations?	Gateway with log sources defined
SLA's to restore services if an downtime event takes place	Short time recovering ensured
Describe wireless and wired connections needed	Descriptive. No preference
Does the gateway or devices communication with the Internet?	No need to expose services or even accessing the internet

Do the devices or the gateway keep data collected inside?	No data is persisted
If so, can it be configured to send it out and avoid acting as a health data source?	Can be configured to send the data to a corporate repository
Can the data gateway be deployed as a virtual server in the hospital infrastructure or does it need a dedicated physical server?	Gateway inside the hospital IT infrastructure

Table 19: Assessment of medical devices

The point to which an alternative should be banned is up to the organization, but these are some items that must lead to discard them:

- Devices with no gateway server
- Devices with no update policies for the O.S. or antivirus
- Devices with no possibility to install antivirus
- Devices that can't avoid to keep medical data inside
- Devices that are nor capable to integrate via HL7 with external services
- Devices with no log source to check abnormal events
- Providers that don't offer an appropriate SLA to help restore from downtime events

We consider **integration** capabilities a decisive factor because it has big potential to reduce risks derived to the manual operation of the devices, and to reduce the data sources containing health data. Besides that, it also increases patient safety by ensuring the correct action will be performed over the correct patient.

Inbound integration

The MDS should act as a satellite of the centralized EMR of the hospital. It means that the patient information it requires (mainly for identification of the patient that it will be connected to) should be received via HL7 messages. To accomplish this goal, the EMR should trigger events in the shape of HL7 messages that will be then sent to the corresponding MDS.

Outbound integration

The MDS collects health data, and that data is stored (persisted) in the gateway as the devices use to have few capabilities (resources) to keep it. This causes that the organization will have one extra health data source for each MDS, that is usually unattended or at least with less controls than the centralized data repository. To avoid this, the MDS should be able to transmit the data via HL7 messages to the centralized EMR, avoiding to store it internally once it has the confirmation that has been received. By this means the gateway has not to be considered a health related data source.

To better explain this idea, we will describe the integration of the ICU vital signs monitors. We will refer to the medical device system (MDS) and not to a single medical device since, as it has been explained, the medical devices don't come alone but in conjunction with a gateway

Regarding the inbound integration, when a patient is transferred from any location to the ICU, the EMR triggers a HL7 ADT^A02 message and sends it to the gateway of the vital signs monitor. The gateway receives the messages, checks that an ingress in the UCI has been informed and stores the demographics of the patient in its patient list. When the patient arrives physically to the ICU and the health staff connects him to the monitor, they don't need to enter any data. The monitor connects to the gateway, reads the patient list and shows it to the health staff (only the list of patients that have been informed through HL7 events). They have only to select the patient from those in the list. When the patient will be discharged from the ICU, the EMR will inform with another ADT^A02 and the gateway will remove him from the patient list.

That way the interaction of the health staff due to administrative concerns is no longer needed and the device may have that part of logic disabled or at least not accessible.

Regarding the outbound integration, the monitors collect data and send it to the gateway, and the gateway should transform it and send it in HL7 format to the EMR. Once the EMR confirms the reception (delivery guarantee) the gateway should remove the data. As this should occur in real time, the data will not should be considered as data at rest, but in transit instead.

With an appropriate codification of the hospital zones and design of events triggered, it will be possible to prevent the manual interaction in any medical device, and with that the cyber risks related to the incorrect operation of the health staff will be lowered (or even suppressed).

The same behavior can be applied to any MDS, finding the events in the real world that may notify about the patient to the appropriate MDSs. Below are listed a set of the most commonly used MDS and the events over the patient management that should be notified:

MDS	EVENTS	HL7 message family
Medication dispensers	Demographics combined with pharmacy orders	ADT + RDE
Anaesthesia towers	Admission/discharge of the patient in the surgery area	ADT
Spirometers	Order for a spirometry study	ORM
Ultrasounds	Order for an ultrasound study	ORM
ECGs	Demographics (to cover unscheduled tests) and orders (to cover scheduled tests)	ADT / ORM

Table 20: Examples of Medical Device Systems

At this point, by having the IT staff involved in the procurement process and ensuring the integration capabilities of the MDS in study, the premises that make possible to apply most of the good behaviors recommended by ENISA can be achieved. Below they will be listed and a brief explanation on how to achieve them has been included.

- General practices:
  - Involve the IT department in procurement: The IT department has been fully involved, and selected the most cyber secure alternative among those which fulfilled the health operational requirements
  - Vulnerability management: By engaging the IT department, they will have a complete list and description of the elements, so an appropriate vulnerability management can be performed.
  - Develop a policy for hardware and software updates: It has been agreed with the MDS vendor during the evaluation phase.
  - Secure wireless communication: TLS capabilities have been a decision element.
  - Establish testing policies: Focus on integration as the basic functionality of the medical device is ensured by the vendor.
  - Establish Business Continuity plans: SLAs agreed with the MDS provider.
  - Consider interoperability issues: Interoperability, referenced as integration, is a basic point to select the MDS to acquire.
  - Allow auditing and logging: The MDS is required to provide a gateway that is the element which can provide a more advanced auditing and logging.
  - Use encryption: Instead of encrypting data at rest, the proposal makes unnecessary to maintain health data in the MDS that, if existed, should have been encrypted.

- Plan phase:
  - Conduct risk assessment: IT department will have all the information required to conduct a risk assessment.
  - Plan requirements in advance: During the evaluation phase, IT department has overseen the requirements the MDS has.
  - Identify threats: By having all the information of the MDS, the threats can be foreseen.
  - Segregate network: The IT department can perform appropriate network segregation according to the communication requirements informed.
  - Establish eligibility criteria for suppliers: The table 19 depicts the eligibility criteria, so the providers can know which are they are in advance and the evaluators have concrete guidelines to base their decisions.
  - Create dedicated RfP for cloud: Applicable to cloud services. Out of the scope of this document.

- Source phase
  - Require certification: Certification has been included in the eligibility criteria.
  - Conduct a Data Protection Impact Assessment (DPIA): IT staff will be able to perform the DPIA. The integration (interoperability) capabilities will have a significant impact on it, if the *outbound* integration is supported.
  - Address legacy systems: Legacy systems will be part of the DPIA since the interoperability makes them part of the system under study.
  - Provide cybersecurity training: By foreseen the threats and risks, an appropriate cybersecurity training can be designed, focusing on those elements that may suppose higher risks, based on the output of the risk assessment.
  - Develop incident response plans: An appropriate response plan could be designed by having all the information of the system acquired.
  - Involve supplier in incident management: For those actions required by the vendor, the SLAs have been agreed.
  - Organize maintenance operations: This item is also related with the *manage phase*. To let organize those maintenance operations, the form included in the APPENDIX A should be used.
  - Secure remote access: Remote access for the provider should be configured at personal level, and requiring digital certificates to both encrypt the communications and ensure the concrete person accessing.
  - Require patching: Observed in the update policies of the software elements.
- Manage phase
  - Raise cybersecurity awareness: Spread cybersecurity awareness training, as the program designed in ProTego.
  - Perform asset inventory and configuration management: The IT department will have the detailed information of the system acquired, and later modifications that will need to be performed, by using the form included in the APPENDIX A of this document.
  - Dedicated access control mechanisms for medical device facilities: MDS will keep its own access control mechanism, and the credentials will be managed by the IT staff with password managers. If the provider needs to perform a maintenance task, a temporary credentials will be provided, and will be disabled once the maintenance operation concludes.

- Schedule penetration testing frequently or after a change in the architecture/ system: MDS will be considered in the penetration testings performed by the hospital.

VI.8.3. ProTego for IO(m)T procurement

The elements produced within the ProTego project (the toolkit regarding technical elements and the educational framework regarding educational purposes) may help to achieve the previous commented good practices. In this section we will describe the good practices each component of ProTego is related to.

SSM: The SSM will allow performing the initial risk assessment both before the MDS would be acquired and after any significative change to the system (for example when any new MDS get included in the hospital infrastructure). It also allows to foreseen sources of threads and to conduct the DPIA.

DGW+A.C.: This component of the ProTego toolkit may serve as a data repository for the medical data acquired by the MDS. If the data would be sent to the DGW and no longer kept inside the MDS, the appropriate measures for data at rest protection could be more easily ensured (minimization of existing health data sources).

NSL: As it has been previously explained, to avoid private WLAN with broadcasting should be a priority for the IT staff. The segregation of the network could be achieved by the technology provided by the network slicing, isolating the traffic of each MDS and providing the appropriate resource allocation, what will also have positive impact regarding the continuity plan.

C.A.: At this point the C.A. may not be applied to IO(m)T devices since the human interaction over the devices tends to be minimized. But it would be of interest for any MDS in which the frontend for the final user will be a mobile device (tablet, etc.) offering an entry of behavioural data that would allow to create user profiles with a real time level of trustworthiness.

SIEM: The MDS should be integrated with the SIEM. The providers should identify the log sources and the patterns that may indicate a threat. This is further explained in the section VII.6. SIEM. The gateways are the elements of the MDS that must provide the logs to the SIEM.

Educational framework: It is closely related to the “Raise cybersecurity awareness” good practice suggested. Despite the strategy described tries to minimize the operational actions from final users (health staff) it is important that they are aware of the interest of the cyber criminals in healthcare data, and the potential impact of an attack.

In that way, and as a conclusion, an organization that would adopt ProTego would be better positioned to achieve the accomplishment of the good practices regarding medical devices procurement dictated by ENISA.

VII. EDUCATIONAL MATERIAL FOR EXTERNAL PROVIDERS

VII.1. INTRODUCTION

As described in previous sections of this document, the ProTego toolkit is made up of a set of components that offer functionalities for the risk assessment and risk mitigation.

This section describes how external applications can be integrated with the ProTego toolkit to take advantage of its features, so that application providers could understand how to perform such integration.

ProTego toolkit does not offer a single point of integration, but rather allows external applications or devices to be integrated with each of its components. This minimizes incompatibilities since each application or device can "choose" the degree of integration according to its possibilities (architecture, base platform, data model, etc.).

For an organization that has adopted ProTego, the degree of integration of external applications should be an indicator to consider when adding new elements to the systems map, so that when faced with two alternatives that cover the same functionality, the one that have a higher integration rate with Protego should be selected, since it would be the safest option in terms of cybersecurity.

The integration with each of the components is described below, indicating the requirements that the application should meet, the technical instructions for such integration and the benefits obtained.

VII.2. System Security Modeller (SSM):

The SSM provides a mean to identify the strength of the external system in terms of cybersecurity. By describing the system (see later) the SSM will identify the risks intrinsic to the architecture, and allows assessing the improvements that could be applied by putting in place suggested controls. Ideally, this evaluation should be performed before the acquisition of the external application, in a way that ”weak” external systems of devices should never be adopted since they might increase the overall risk level of he IT map of the organization.

Is the IT staff who must perform the assessment by introducing the external system into the system model of the whole organization. That is because it is the IT staff who will decide the way in which the system under study will be integrated into the global IT map, taking into account the description provided by the external providers.

To let the IT staff make such assessment, the external provider must describe the elements that are part of their system, precisely:

- The applications or processes, describing the functionality they perform, the need of an application server and hardware requirements
- The data assets, describing the data format, sensitivity, need for a database server and intended use.
- The communications between processes and the network requirements

Based on this description, the IT staff will conduct the first version of the system model, by deciding the final placement of the software components (new servers or already existing ones), network architecture and physical spaces where the hardware assets will be placed in.

Besides this first description, the external provider must collaborate with the IT staff to find the best possible configuration of the system, identifying the possible controls that each component of the system allows to put in place. Such controls will be different depending on the type of asset. To explain this concept the following table shows most relevant controls for different and commonly used assets:

TYPE OF ASSET	CONTROL
Notebook /mobile device	Antimalware
	Biometric ID Identifier
	Physical lock
	Logging
	Encryption power
	Password verifier
	Software patching
Physical data centre	Biometric ID Identifier
	Password verifier
	Physical checks
	Physical ID verifier
	Physical locks
SW Host	Antimalware
	Clustering
	Independent instances
	Secure BIOS
	Secure enclave
	Penetration testing
	Password quality check
	Load monitoring
Process	Access control
	Authentication proxy
	Password
	Logging
	Access key
	Software certification
	TLS
	X509 Verifier

Table 21: Data requested for the SSM model

Summarizing, the task for the external providers regarding the SSM is to provide enough descriptive information to the IT staff so they can build the model of the provided system or application and assess the risks it might introduce.

VII.3. Data Gateway (DGW) + Access Control Framework (A.C.)

The DGW and A.C. components together act as the interface to the data or, in other words, the persistence layer offered by ProTego. They will be considered jointly as it makes no sense to use one without the other. To integrate with it, external providers should avoid using its own persistence layer and make use of them instead.

The basic request flow for an application making use of this is illustrated in the following figure:

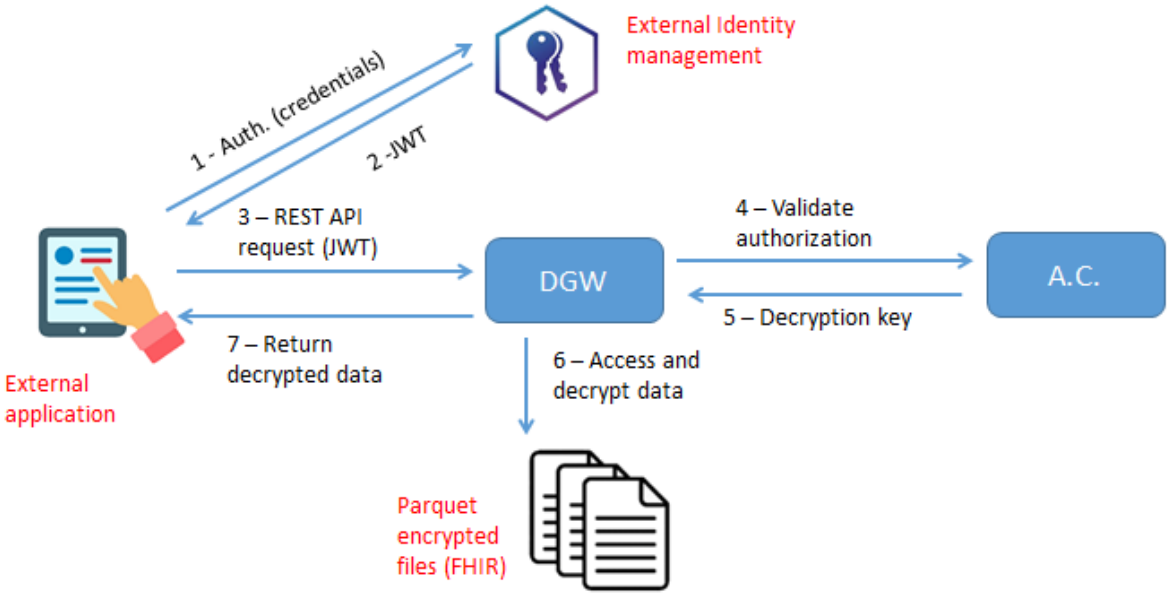


Figure 24: Dataflow for authorization in data access

And this is the sequence of events that will be performed:

1. The application uses an external identity management (IAM) as authentication system. It sends an authentication request containing the user credentials.
2. The IAM authenticates the user and provides a valid (JWT) token, including the user role that will be later used by the A.C. to allow/deny the access to the data.
3. Then the external application requests access to the data via a REST API request to the services exposed by the DGW. In the request, the full JWT should be included as a parameter. The DGW exposes two different endpoints for write or read data:
    a. Write requests are made through the FHIR-SERVER endpoint. It accepts standards FHIR objects that should be passed as parameters in the request, jointly with the JWT.
    b. Read access are meant to be made through the QUERY-GW endpoint. It allows sending SQL queries instead of requesting specific FHIR objects. That gives more flexibility as a ”SELECT * FROM XXXX” would return an entire FHIR object (or bundle), it can be specified which concrete fields of the FHIR object are required, and reduces the data sent back. This is aligned with the GDPR principle of *Data minimization*.
4. The DGW delegates the authorization to the A.C. It request for the approval to access the data by providing the JWT and identifying the data (FHIR objects) requested.
5. The A.C. validates, based on the role inside the JWT, if the user is granted to access the requested data and, if so, it reveals the decryption key to the DGW.
6. The DGW accesses the data stored within the parquet encrypted files and, using the decryption key provided by the A.C., decrypts it.
7. The requested data has been decrypted and is sent to the client (external application)

To make possible such behavior, external providers need to adapt their application to make use of that persistence layer. Precisely:

i. Use JWT as credentials management.
ii. Make use of the external IAM offered by the healthcare organization

iii. Perform data requests through the REST API exposed by the Data Gateway

iv. Ensure the application is FHIR compliant and is able to manage FHIR data objects

The integration with the DGW and the A.C. offers advantages for both the external provider and the healthcare organization:

1. The use of an external IAM prevents the external providers the need of implementing an authentication system, as it has been delegated to an external one.
2. The permissions to access the medical data will be managed by the healthcare organization's IT staff from a centralized point, so the external application will not be impacted if the grant policies change the visibility that each role must have over the data.
3. The external application will no longer need internal data sources, so the external provider will not be asked to provide mechanisms to ensure data safety. As it will reside in an external data source governed by ProTego, the IT staff will be in charge of ensuring the appropriate security measures to that data.

VII.4. Continuous authentication (C.A.)

The C.A. provides a mean of authenticate the person operating a mobile device, that is, ensure that the person operating the device is who it is meant to be. Because of that, its scope is limited to application with mobile frontends installed as mobile applications.

It has two main components:

- C.A. agent, installed in the frontend (mobile device) retrieves behavioural data of the user and sends it to the C.A. API
- C.A. API is the backend component. It builds IA models from the data sent by the C.A. agent and obtains a trustworthiness level of the users.

Therefore, the integration with the C.A. component is constructed at two levels:

1. Frontend: The C.A. agent is a mobile JAVA app that should be installed in the mobile device. The frontend of the external app must integrate whit if by sending the JWT obtained from the IAM once the user has logged in. From this point, the C.A. app must be allowed to collect keyboard data, since this is going to be the source of data used by the C.A. backend to build the IA model and calculate the trust level of the user. To send the JWT from the external app, C.A. allows both JAVA native integration by creating instances of the C.A: interfaces and make use of its methods, and integration at the level of "broadcast receiver", which allows its integration with any other programming language rather than JAVA. With this, there are no restrictions in terms of compatibility of programming languages to make use of this functionality. The only requisite is that the JWT must contain a custom tag "aud" with its value set to the URL of the endpoint published so the agent can make periodic requests to the C.A. backend to perform continuous authentication of the user. As an example, in MS's Pocket EHR use case it's been set to *https://840yr281lj.execute-api.eu-west-1.amazonaws.com/Stage* as it is the AWS endpoint provided to access the C.A: backend from the internet (where the mobile devices are).
2. Backend: The C.A. API is the IA engine. By receiving the behavioural data collected by the A.A. agent, it will periodically rebuild the model for the user, and calculate the trustworthiness level, which will be a value between 0 (total distrust) and 1 (total trust). This value could be requested via a REST API and may be used both by the C.A. agent, to perform any action at the frontend level, or by the external application, to invalidate the user and discontinue the session by expiring user's JWT token and, with that, his possibilities to access the data.

It is worth to mention that the presence of the C.A. can be informed as a control for the ”mobile device” kind of elements in the SSM model and it will be considered and will reduce the risk of the system.

The C.A. offers the external providers an extra security layer, not tackled by current mobile apps, to ensure their mobile frontends are used by authenticated users. And also allows detecting fraudulent uses and reacting to avoid further damages. In addition, if the evaluation of the external application is performed taking into account the risk level offered by the SSM, the use of the C.A. will increase the chances of the external application to be approved and adopted.

VII.5. Network slicing (NSL)

NSL is the most transparent component of the ProTego toolkit from the perspective of external providers. Its functionality consists on create virtual networks (slices) over the physical network, and provide isolation and appropriate resources allocation to each slice, in a way that an event occurred in one slice will not affect the others, even sharing the same physical infrastructure.

External providers should describe the communications that their applications will perform in terms of origin, destination, ports used and protocols. They will need to describe the required bandwidth allocation as well. From this information, the network operator will create the slices needed and allocate the resources to grant a successful deployment of the external application.

Despite it may seem the NSL will have no impact for the external provider, it will. By ensuring the isolation and resources needed by each slice, the incidences will be reduced and with them, the requests made to the external providers, since problems in the network infrastructure and communications are usually mistaken as errors in the underlying applications.

VII.6. SIEM

The SIEM acts as the central risk monitoring point and is the channel through which any threat or risk detected in the external applications will be informed to the IT staff, as responsible to take appropriate response actions. More than that, it is even possible that those potential risks or threats may not be detected by events within the external application and could only be detected by correlation of their logs with those provided by different elements of the IT map.

To perform this surveillance and log correlation, the external providers will be in charge of:

- identify the log sources provided by the application
- describe the type of log sources, so an appropriate SIEM agent could be deployed and connected to the log source to gather the data. As an example, if the application provides its logs in a plain text format, a ”Filebeat” agent should be deployed and connected to the log text file, while if the external application is a cloud application that provides logs via S3 bucket, a WAZUH agent would be the correct one to collect those logs. Apart from this type of integration, the ProTego SIEM covers the possibility that it would the external application who sends the logs to the SIEM, by exposing KAFKA topics that may be used by making use of REST services to send the events (logs) gathered by the application.
- Identify those *patterns* that, if found in the application logs, could lead to discover a potential threat.
- Identify those patterns that, despite may not suppose any threat by themselves, may be risky if combined with certain events in external elements.

The ProTego SIEM offers to the external providers the possibility to integrate their applications with the centralized threat detection and notification system, allowing them to avoid such logic in their applications and taking advantage of the functionalities of an expert system.

By this, the applications they provide will be considered as early detection and response in terms of cyber-security.

VII.7. IoT devices

At this point it has been described in the previous sections the mechanisms to be used to integrate external applications with the ProTego toolkit. But it is worth to dedicate a section to the IoT devices, since they have significative differences compared with regular applications that imply certain modifications in the process.

IoT devices, mostly in the shape of wearables, are becoming part of the healthcare IT ecosystem since they allow the acquirement of health related data that is very useful for patients monitoring. And attending to the mechanisms that could be introduced to improve the cyber security we are dividing them into:

- Connected IoT devices: those able to connect to other systems like applications running on the same smartphone or device, cloud repositories, etc. This category of devices would admit, thus, the integration with the ProTego toolkit to take advantage of its features, but it is needed to add some logic by the vendors to perform that integration. An example has been included in the MS's Pocket EHR use case.
- Non connected IoT device: those not able to connect to any external data source or application. They use to act as a removable storage device. An example has been included in the OSR's Food Coach use case.

Each of this type of devices is considered in the following sub-sections.

VII.7.1. Connected IoTdevice

They use to be a compound of a hardware piece plus a thin application layer, usually in charge of store data inside the device, and send it to a data repository (provider's cloud, etc.), directly or via an smartphone or mobile device that acts as gateway.

The "thin" software layer may make use of the ProTego features by integration with the different components of the toolkit, in the way described in the previous sections.

But the integration with the DGW+C.A. which controls the access to the data, as well as other integrations, are based on the existence of a JWT obtained via a log-in action performed by the user. And this is a major difference between IoT devices and regular applications: in an IoT device there is no login action for every use, the process must be transparent for the user and should not imply any explicit action.

In this section we will describe the scenario to cover such requirement. It has been implemented in the Pocket EHR use case by simulating an IoT device, as it is not possible to modify the logic of the application layer present in those already in the market.

The basic idea is to keep a JWT Refresh Token inside the device and use it to obtain a full valid JWT that can be used to request data through the DGW. The following figure illustrates the first use of the IoT device:

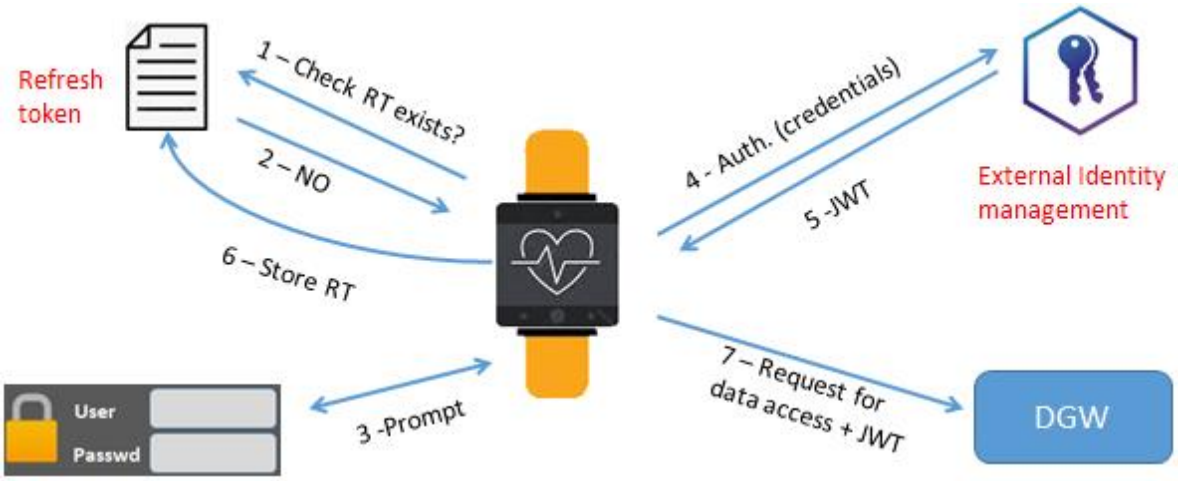


Figure 25: IOT first request for data

1. The device, as the very first action, checks if a file containing the JWT Refresh Token exists within the device.
2. In the first use, it does not exist
3. Because of that, the device prompts the user requesting user and password.
4. Then, it performs the authentication using these credentials on the corporate IAM
5. If the authentication succeed, the IAM returns a full valid JWT
6. The device stores only the ”Refresh token” (RT) section of the JWT in an internal file. The Refresh token does not contain any credential, and its TTL is configured in the IAM. TTL for Refresh Tokens is usually set to several weeks, and can be set up to years range. From ProTego we recommend set it up to 30 days. This controls how often the device will prompt the user to enter the credentials again to perform a user validation.
7. With the full JWT obtained, the IoT device request data access to the DGW

In this first use, that is, when the Refresh Token does not exist, the interaction with the user is needed to provide valid credentials (user + password). In later requests for data and during the TTL of the Refresh Token (while it is valid and has not expired) the process is more transparent and does not require such an interaction. The following figure illustrates the process:



Figure 26: IOT subsequent requests for data

1. The device, as the very first action, checks if a file containing the JWT Refresh Token exists within the device.
2. This time the Refresh Token exists and is retrieved
3. Then, the device uses it as a parameter to request a full and valid JWT. The IAM allows the authentication via both user + password pair, and via a valid Refresh Token
4. The IAM returns a valid JWT
5. The JWT is then used to make data requests to the DGW

This approach introduces a series of benefits regarding cyber-security and easy management:

- allows the authentication of the users to be made against the corporate IAM.
- makes the user credentials volatile, that is, not persisted in any support from where they can be thrived
- the periodicity with which the credentials will need to be introduced can be controlled by the IT staff in the corporate IAM, by setting the desired TTL of the Refresh Tokens
- it also allows a response if any threat is detected, by expiring the Refresh Token and making necessary to introduce valid credentials at that point
- in the case of non-personal IoT devices, that is, devices that the hospital assign to patients for a certain period, once the owner of the device is changed, the IT staff should only delete the Refresh Token file and the new user (patient) will be prompted to introduce his credentials
- the data ”produced” by the IoT device will be persisted (stored) in a centralized repository under the data gateway, encrypted at rest with the parquet modular encryption mechanism

VII.7.2. Non connected IoT device

OSR has developed a nutritional use case that involves the adoption of a web application, FoodCoach together with a non-connected device, AX3 activity tracker.

The activity tracker aims to support one of the FoodCoach features which is to show the statistics on the patient's physical activity. The data is collected by the device and subsequently uploaded to FoodCoach via the nutritionist's computer USB port. Image x depicts the interaction among the components that are involved in this use-case. Being the AX3 activity tracker a non-connected device, it is not connected to the Internet, but only to the doctor’s computer. This connection is the main source of the risks that will be discussed in the following paragraphs.

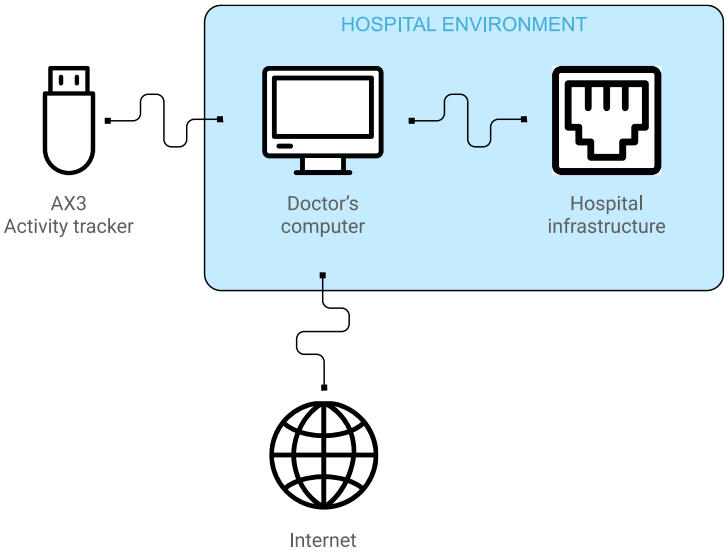


Figure 27: Non connected IoT device

In this scenario, the activity tracker introduces cyber security risks related to the use of non-connected devices.

However, ProTego does not aim to implement secure devices, but to secure the medical data within the hospital infrastructure. To contribute to the security of medical data, the devices adopted in the hospital should be built with a "secure by design" approach.

Security by design (or secure by design), is a new industry term for a range of security practices built on one fundamental idea that security should be built into a product by design, instead of being added on later by third-party products and services [20].

In order to secure the data on the AX3 activity tracker, some possible mechanisms have been considered to be implemented after the device was purchased off the shelf.

One such example is stream-based encryption, with the caveat that it would have to be carefully managed if the stream restarts (e.g., to not recycle the same encoding sequence). However, it may be possible to trick the device into repeating the same sequence (e.g., by truncating the file, resuming the recording, and comparing the two versions) and finally breaking the security.

Another example is the use of a pre-shared key (typical for low-power applications). Though, this is not an option since we cannot store the pre-shared key on the device itself because an attacker can extract the key from the program memory or from the NAND flash directly.

For these reasons the security mechanisms mentioned above are not sufficiently effective to protect medical data on the device.

Moreover, the implementation of security mechanisms can compromise the operation of the devices if carried out subsequently by third parties, for example: impacting battery life, overflowing the stack, causing data races with interrupts, etc.

Security by design methodology usually starts with the evaluation of risks related to the system under consideration. Considering the OSR scenario mentioned above, the doctor would have to receive the device from the patient and connect it to his/her own personal computer to examine the data. In this scenario, the device is not a "trusted element" since an external actor (i.e., the patient) has access to the device, and he/she could infect the device with a USB malware, either willingly or by accident. For example, more specifically, the doctor's computer could be exposed to risks such as a virus being executed automatically as soon as the device is plugged into it. Moreover, because the USB storage is not READ-ONLY, anyone could write data on it, meaning that data could be modified or replaced with non-valid data or non-supported file types.

This risk, known as USB tampering, leads to a violation of data integrity. On the other hand, a violation of data confidentiality is also a possibility, since an attacker could steal the device from the patient, and then read the data on it.

To mitigate the risks related to AX3 activity tracker, security mechanisms should be planned at design time and then be embedded into the device when it is manufactured. More specifically, to mitigate the risks related to USB malware and USB tampering, there are various authentication strategies already used throughout the computer industry that could be exploited. Authentication can be defined as "the process or action of verifying the identity of a user", which, in OSR scenario, is intended to prevent the patient or an attacker from writing data on the device. One example is two-factor authentication (2FA) in which devices request biometrics, such as fingerprints, retina scans or facial recognition to grant access to the user. Some non-connected devices already have this security measure in place. For example, there are USB storage devices with fingerprint scanners, so that the user is authenticated by comparing the fingerprint stored on the device and the fingerprint of the person trying to connect the device to a computer. Another example is password authentication in which the user must supply a password, the device checks the entered password, and, in case it matches with the previously saved password, it grants user access to the device. The AX3 activity tracker supports password authentication through USB serial commands, so, in our case, doctors can simply lock the device with a password before giving it to the patient. This measure effectively prohibits access to the file system of the device so that the stored data cannot be tampered with, and therefore data integrity is preserved. For the sake of completeness, it should be noted that this method protects the device against casual misuse, but a skilled attacker could dump the device firmware and potentially have access to the stored password on the device.

On the other hand, data confidentiality can be guaranteed by means of data encryption, which, in turn, can be broadly divided into two categories: software-based encryption and hardware-based encryption [21]. Software-based encryption refers to methods of protecting internal data using only software and includes the data encryption/decryption method and the access control method. The data encryption/decryption method uses a mathematical tool to encode and decode the data to prevent the inference of plain text, in order to solve the problem of data being stored in plain text. Hardware-based encryption refers to the methods by which a device takes advantage of a dedicated hardware chip for the purpose of securing the device. Hardware encryption modules use dedicated hardware security modules to make it difficult to access secret information using reverse engineering, which is the fundamental problem of the software method.

From the perspective of a third party, software-based encryption is easier to implement (for example, by building the firmware of the device from scratch, adding new features such as support of public/private keys and data encryption), but it offers a weaker protection. For this reason, hardware-based encryption should be preferred, although it is only achievable by the device vendors, as they have more control over the device architecture and the internal components. Once again, this shows the importance of planning security mechanisms as early as possible (i.e., at design time) and incorporating them into the device directly when it is manufactured.

VIII. REFERENCES AND INTERNET LINKS

[1] ISO 27001:2013, A.6.2.1, “Segregation of duties”

[2] EU GDPR, recital 81

[3] https://whatis.techtarget.com/definition/information-security-management-system-ISMS

[4]https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[5] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[6] https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive

[7] https://www.nist.gov/cyberframework/framework

[8] Brown (2001). "The Privacy Paradox"

[9] Sören Preibusch (2015). "Privacy Choices Behavioural Economics Review"

[10] Spyros Kokolakis (2017). "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon"

[11] https://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html

[12] https://rightcarealliance.org/about/what-is-right-care/

[13] John Badham (1983). “WarGames”

[14] https://www.hindawi.com/journals/scn/2019/8715264/

[15] https://www.gartner.com/en/documents/2410615/definition-people-centric-security`

[16] https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

[17] https://www.youtube.com/watch?v=YiRPt4vrSSw

[18] https://www.youtube.com/watch?v=5rPKeUXjEvE

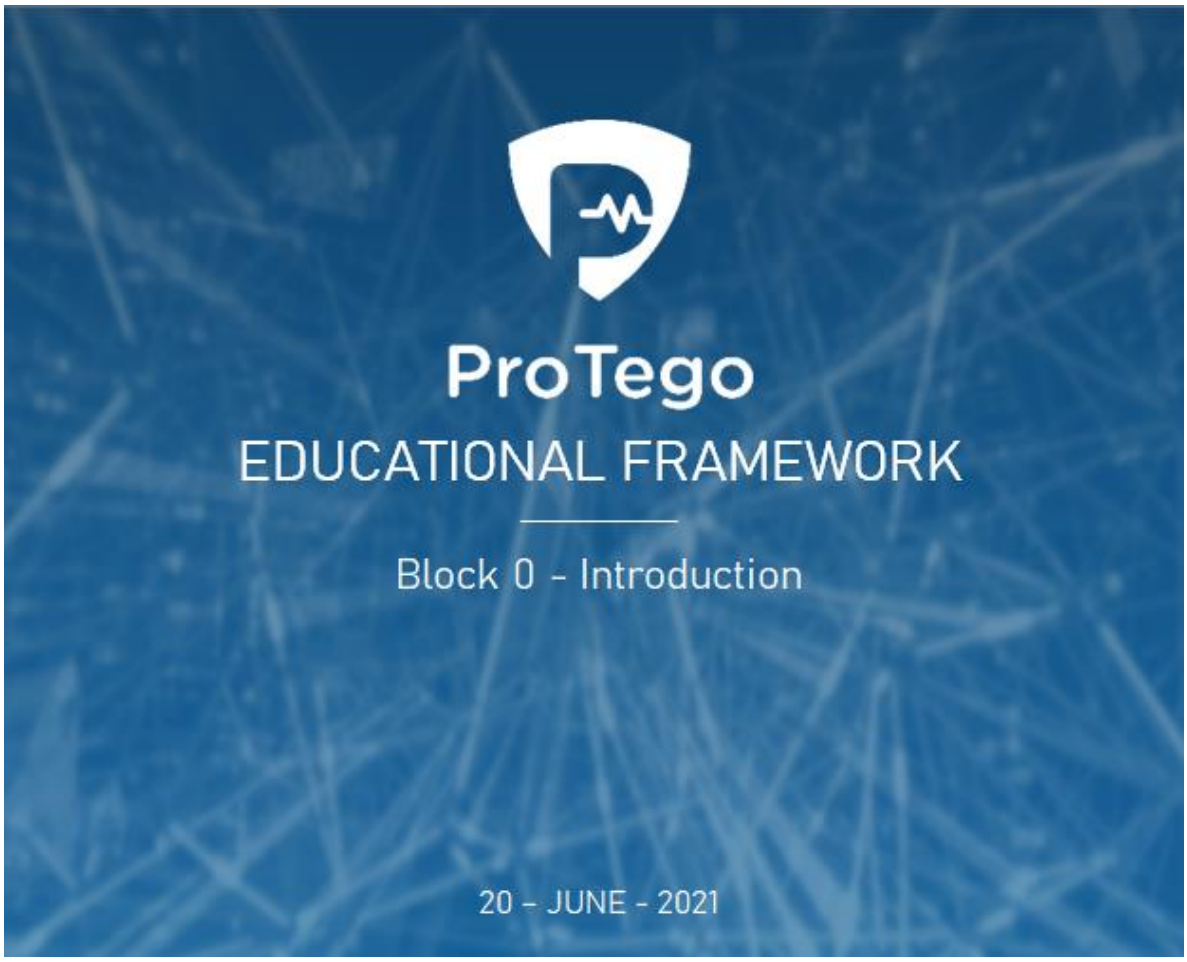
[19]https://www.enisa.europa.eu/publications/report-files/translation-procurement-guidelines-for-cybersecurity-in-hospitals/procurement-guidelines-full-version-es.pdf

[20] https://www.techopedia.com/definition/34101/security-by-design-sbd

[21] Kyungroul Lee et al. «A Study on a Secure USB Mechanism That Prevents the Exposure of Authentication Information for Smart Human Care Services». In: J. Sensors 2018. Available: https://www.hindawi.com/journals/js/2018/2089626/

[22] ISO 9241-11:2018, Ergonomics of human-system interaction

APPENDIX A. INTRODUCTION TO CYBERSECURITY AWARENESS



Block 0 – Introduction to cybersecurity



Rank of objectives for cyber-criminals

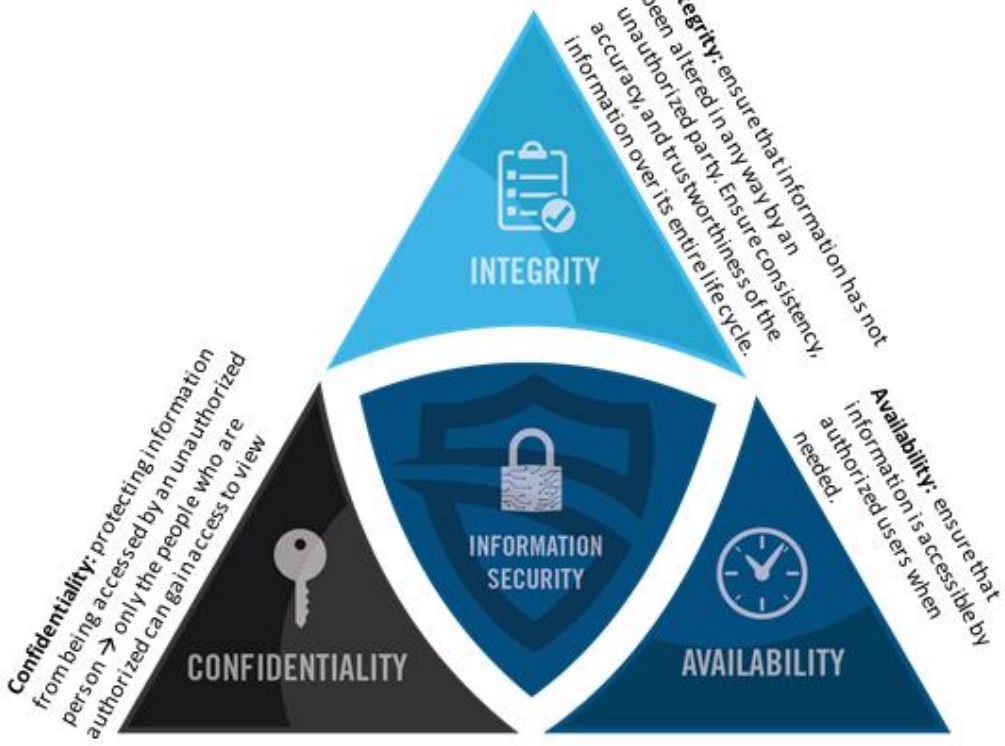
#1  Healthcare data

#2  Financial data

#3 

Personal Data

Block 0 – Dimensions of information security



Block 0 – Potential impact for patients



Sell medical data to insurance companies → increase insurance prices

Sell medical data to external companies → prevent hiring

Spread of medical data → social discrimination



Incorrect data can lead to **misdiagnose** patients

Errors in treatments, drug administration, cares …

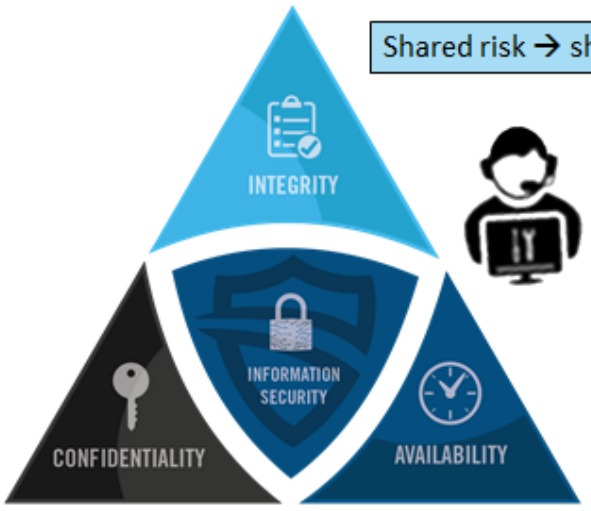
Threads get increased with automated **medical devices**



Pretty similar to threads related to integrity, if the actions are performed with no available data

Delay in treatments → serious impact for patients

Block 0 – Not a technical issue



Shared risk → shared responsibility → shared task




ProTego
EDUCATIONAL FRAMEWORK
Block 0 - Introduction
END
20 – JUNE- 2021

APPENDIX B. FORM FOR MEDICAL DEVICES MAINTENANCE

This form includes all the data that need to be registered when any maintenance operation needs to be planned. It should be fulfilled by the medical devices provider in the notification of any planned maintenance operation, so the IT staff could review it in advance, know any change that would be made, evaluate the possible risks, and keep the information regarding the medical device system (MDS) up to date.

CONTACT PERSON - HOSPITAL	
Name of the contact person (Hospital)	
Department or function	
Date of request	
CONTACT PERSON - PROVIDER	
Provider (Company)	
Name of the contact person (Provider)	
Position	
Phone number	
E-mail address	
INFORMATION ABOUT THE DEVICE	
Brand	
Model	
Description (use, utility)	
Medical service of destination	
DEVICE CONNECTIVITY	
Device MAC address	
Integrate in Hospital network (YES/NO)	
Integrate in own VPN (YES/NO)	
Integrate with DICOM network (YES/NO)	
Physical location to be placed	
Code of network plug (to be connected at)	
Replace another device (YES/NO)	
IP of replaced device	
Location of replaced device	
Network plug of replaced device	

OTHER
Describe the maintenance operation requested for planning

APPENDIX C. SSM TUTORIAL

This appendix includes already existing training information about the SSM.



UNIVERSITY OF Southampton

System Security Modeller (SSM) Tutorial

Mike Surridge
ms@it-innovation.soton.ac.uk

IT Innovation Centre, Southampton
30 April 2020 Update

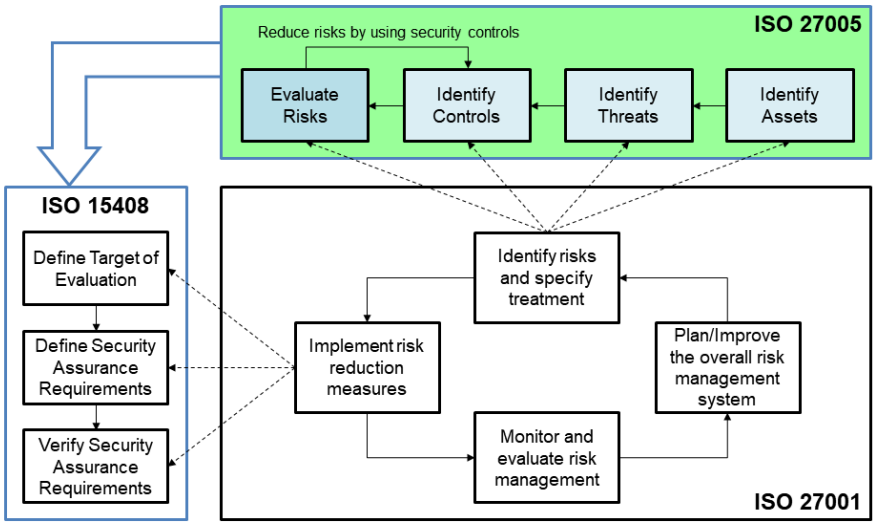
Contents

- Introduction to the SSM tool: what it does, user manual
- Example of ISO 27005 risk assessment using SSM
- Guidelines on how to create SSM models by building in layers
- Data and data flow modelling specifics and guidellines

© University of Southampton IT Innovation Centre 2020

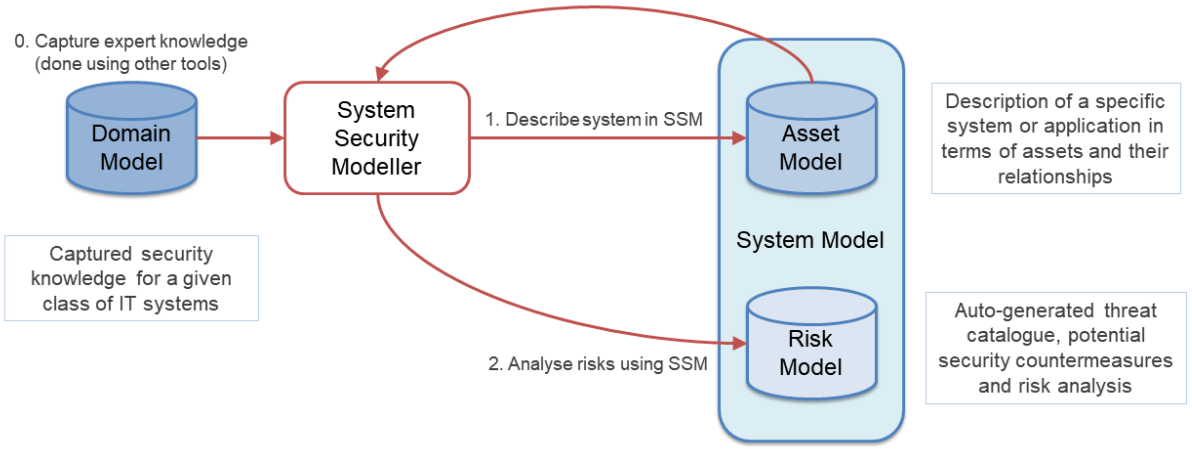
Introduction: SSM User Guide

System Security Modeller



© University of Southampton IT Innovation Centre 2020

System Security Modeller



© University of Southampton IT Innovation Centre 2020

Main Functions of SSM

- Registration and login procedures
- System model management: the Dashboard
- System model construction: the Canvas
- System analysis and threat identification
  - including potential regulatory compliance issues (compliance threats)
- Risk level analysis
- Navigating attack paths and secondary effect cascades
- Compliance threats and modelling errors

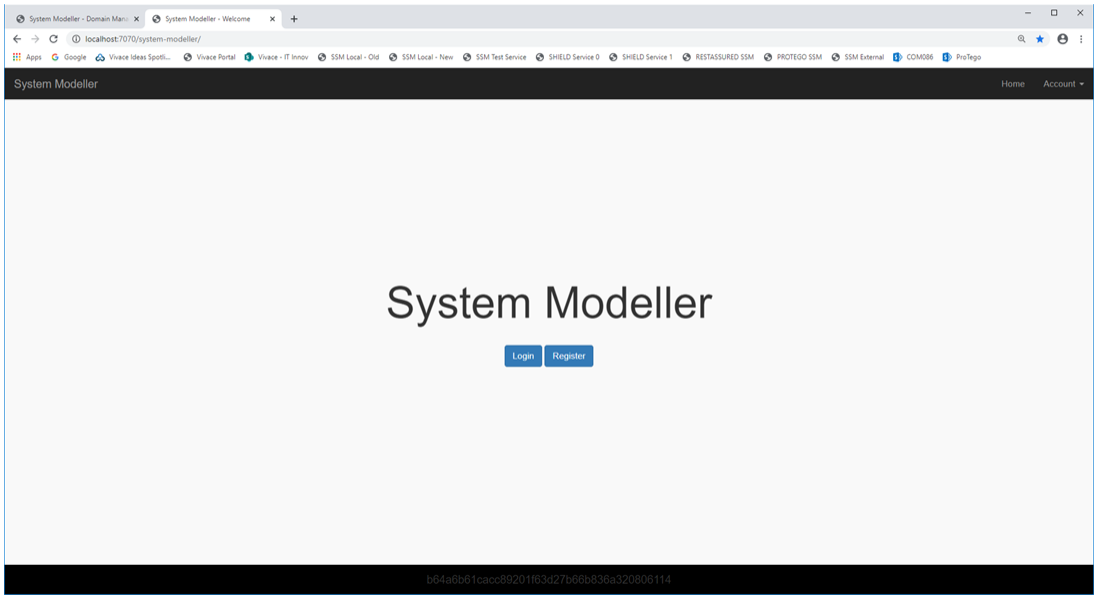
© University of Southampton IT Innovation Centre 2020

Terminology

- Asset: something that has value within the system
  - it contributes to the purpose of the system, there is a cost if that contribution is lost
- Misbehaviour or Effect: an unwanted change in asset behaviour or status
- Threat: a situation or event that could lead to such a change
  - threat effects or threat consequences: the misbehaviours caused by a threat
  - secondary threat: a threat representing a mechanism for the propagation of effects
- Risk level: the severity of a misbehaviour (or threat) based on
  - the Likelihood of occurrence
  - the Impact it would have
- Trustworthiness: propensity of an asset to avoid/resist threats
- Control: a security measure protecting an asset that helps it resist threats
- Control strategy: a combination of controls that address one or more threats
  - or that represent a cause or target for some types of threat

© University of Southampton IT Innovation Centre 2020

Registration and Login



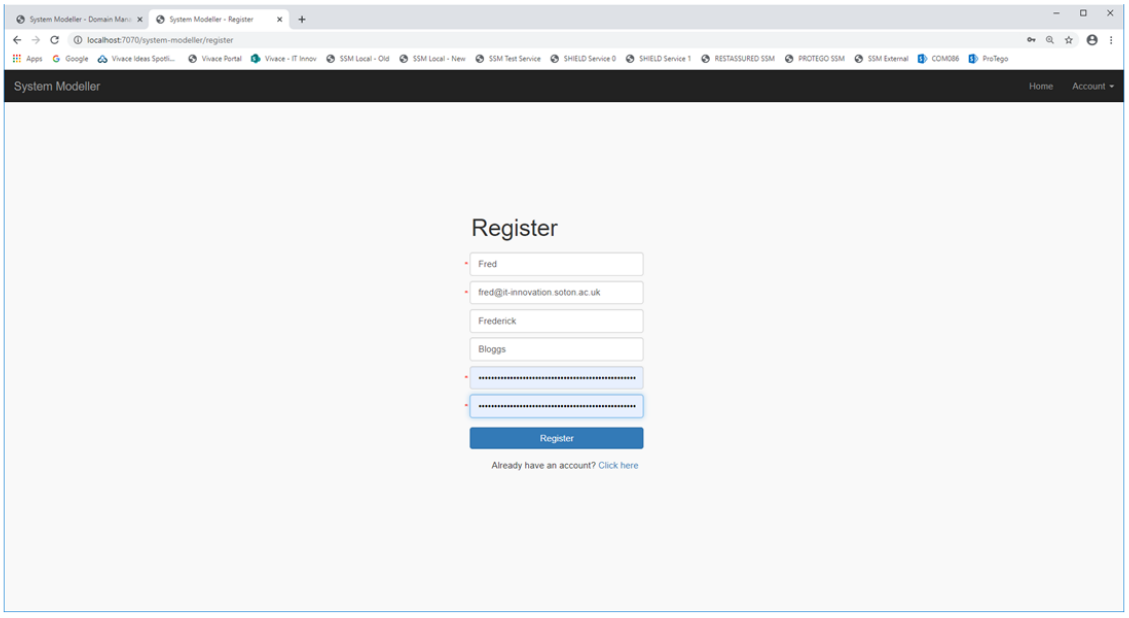
© University of Southampton IT Innovation Centre 2020

Registration and Login

- To log in you must have an account on the SSM service instance
- There are two ways to get an account
  - by invitation: the service administrator sends an email inviting you to use the service
  - register: requests the service administrator to grant access
- Either way you must define a username and password, which are used to log in after that
- We are working on a single-sign on mechanism, so this procedure may change in future

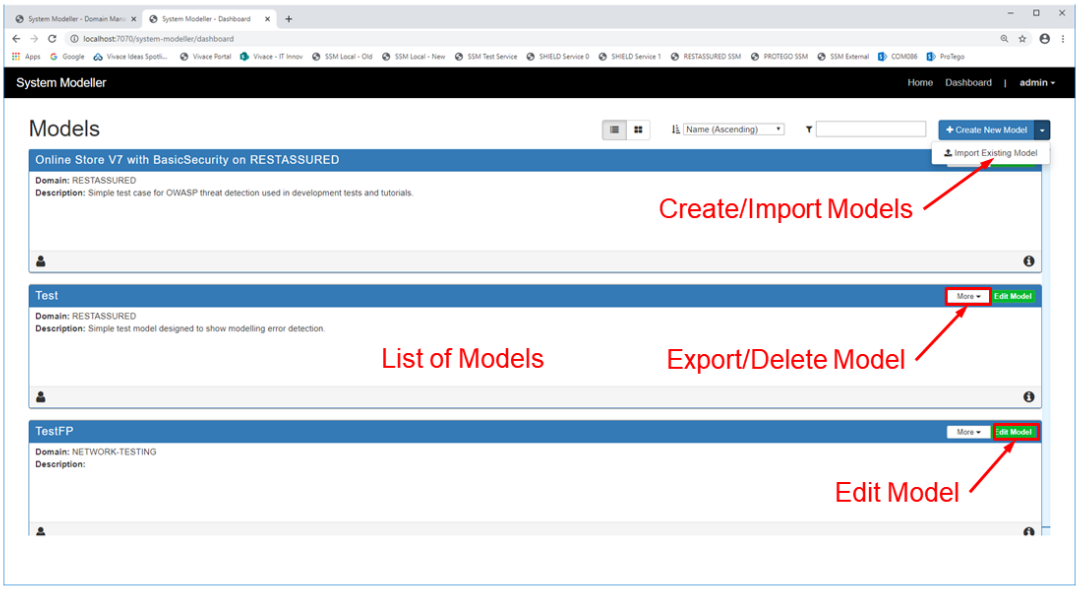
© University of Southampton IT Innovation Centre 2020

Registration and Login



© University of Southampton IT Innovation Centre 2020

System Model Management Dashboard



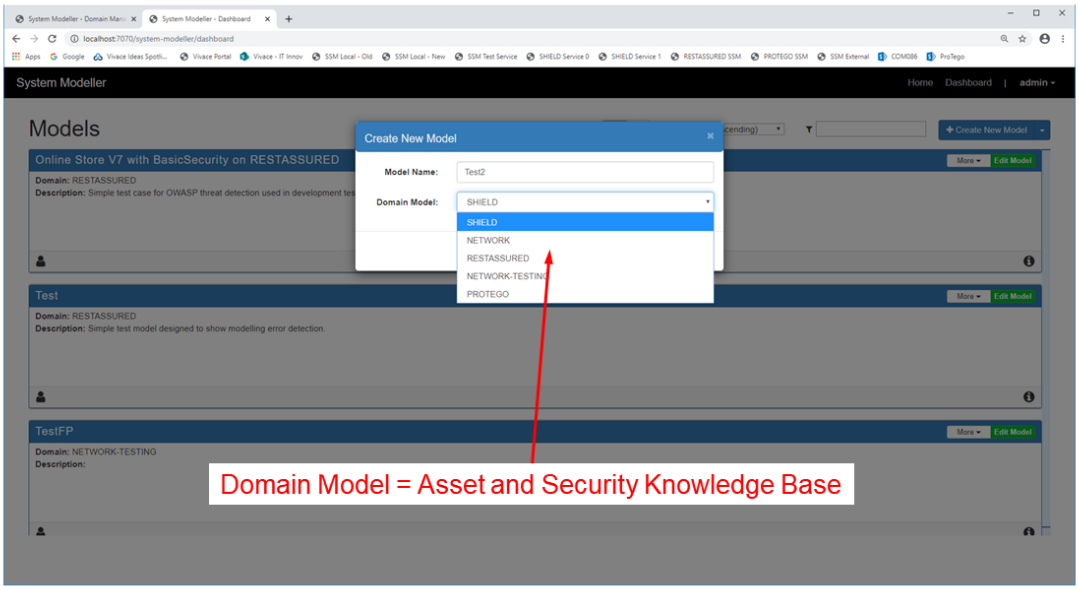
© University of Southampton IT Innovation Centre 2020

System Model Management Dashboard

- This version of SSM is a research prototype
  - we do not routinely produce security patches for the software
  - any installation is temporary and may be overwritten at any time
  - access to system models depends only on knowing the (hard to guess) URL
    - so users in research projects can easily get a second opinion without their colleagues having to register
- Therefore you should
  - export copies of models you need to keep, and store them elsewhere, e.g. on the shared project filespace
  - ensure you do not include commercially sensitive or security sensitive data in any system model created in the project
- The software is not security hardened, but please do use it securely:
  - use strong passwords, share model URLs only with trusted friends, etc

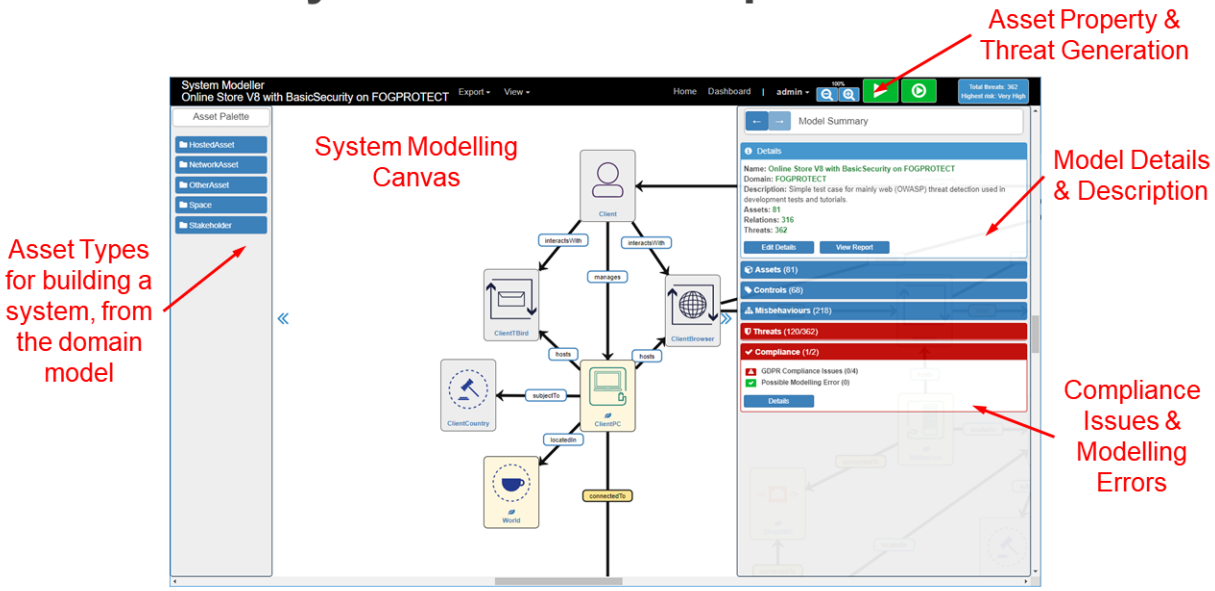
© University of Southampton IT Innovation Centre 2020

System Models and Domain Selection



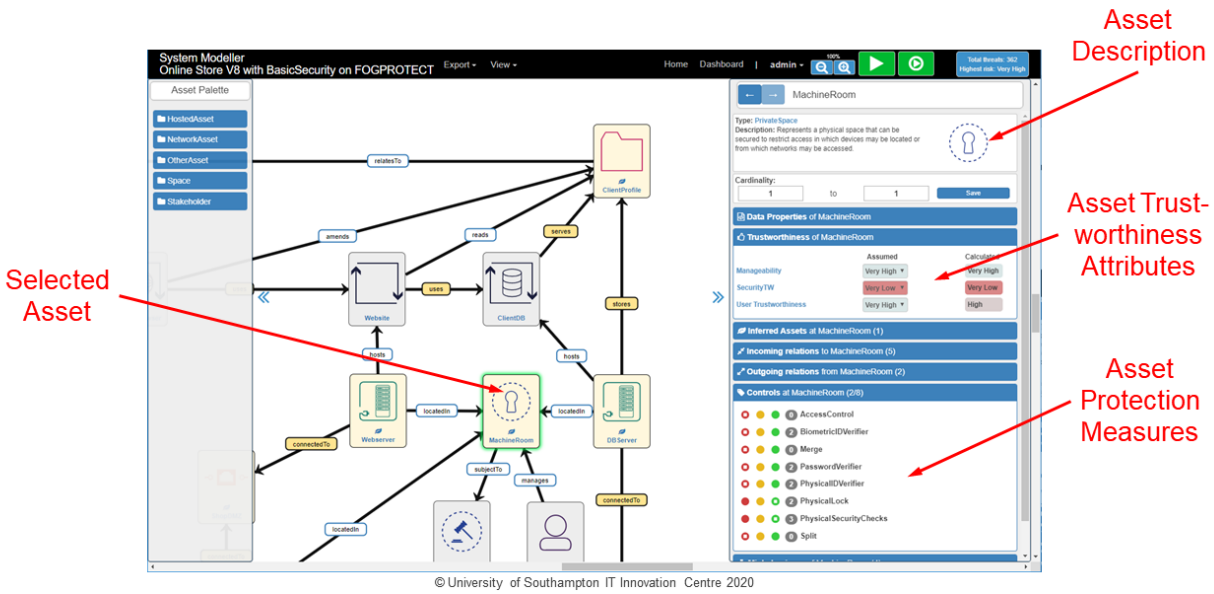
© University of Southampton IT Innovation Centre 2020

System Model Composition



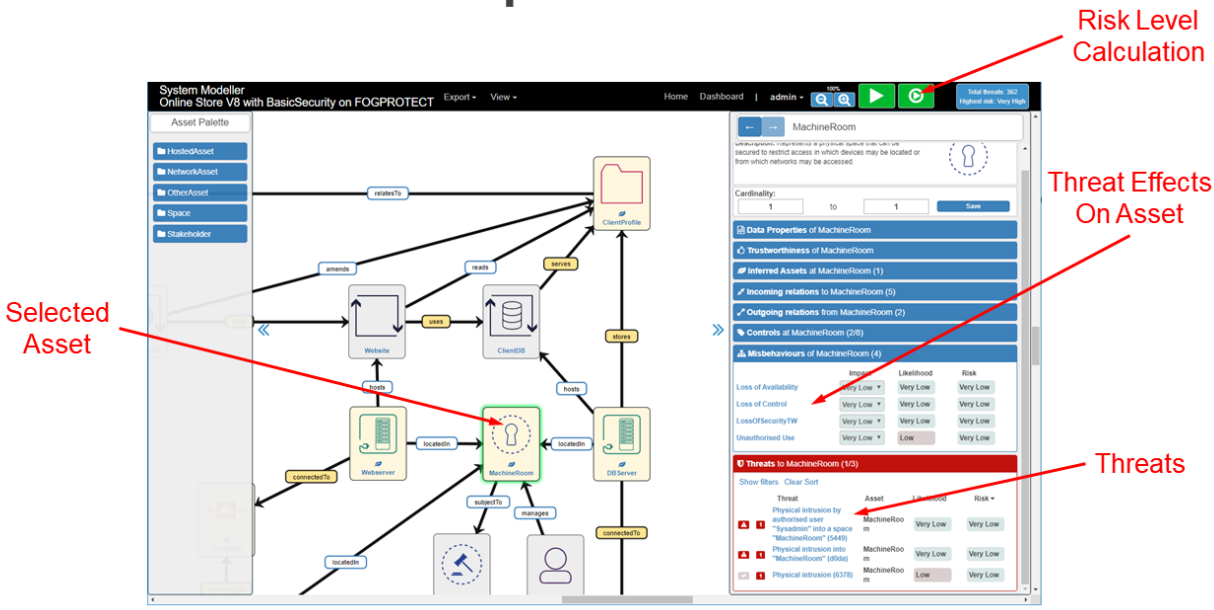
© University of Southampton IT Innovation Centre 2020

Asset Properties & Threats



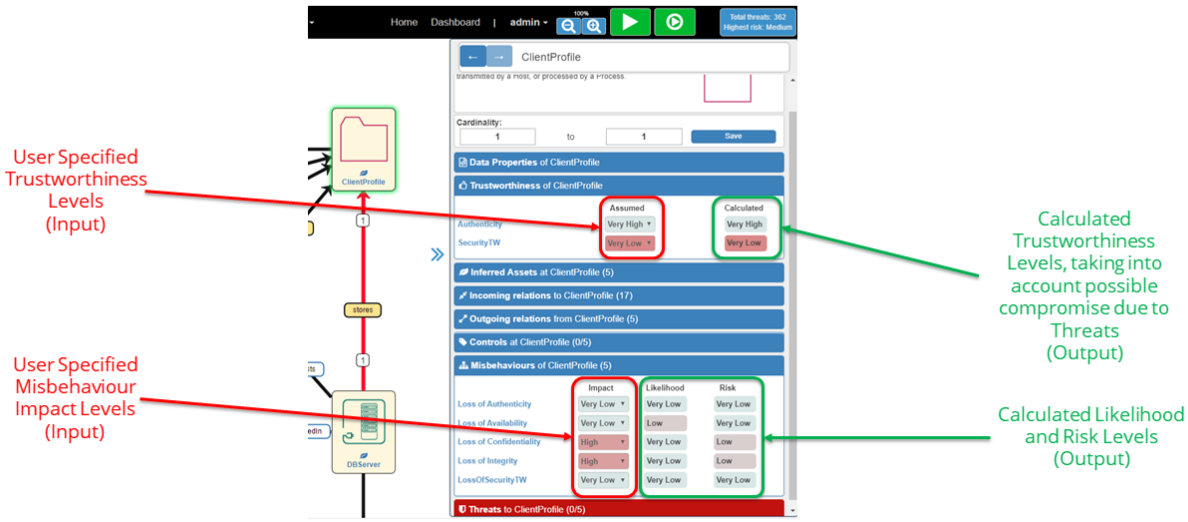
© University of Southampton IT Innovation Centre 2020

Asset Properties & Threats



© University of Southampton IT Innovation Centre 2020

Risk Level Calculation



© University of Southampton IT Innovation Centre 2020

Likelihood and Trustworthiness

Likelihood	Means	Trustworthiness
Very high	Something will definitely go wrong if the possibility exists even only for a short time	Very low
High	Something is likely to go wrong if the possibility exists even only for a short time Something will definitely go wrong if the possibility exists for very long	Low
Medium	Something is likely to go wrong if the possibility exists for very long, but not otherwise	Medium
Low	It is unlikely that anything will go wrong without very prolonged exposure to the possibility	High
Very low	It is unlikely that anything will ever go wrong	Very high

- Likelihood: how likely is it that something will go wrong?
  - a threat or a misbehaviour
- Trustworthiness: how unlikely is it that something will go wrong?
  - associated with asset characteristics related to the asset's role(s) in threats

© University of Southampton IT Innovation Centre 2020

Impact Levels

Misbehaviour impact level	Means
Very high	This misbehaviour in this asset will be fatal to key business interests. Very few misbehaviour sets will be at this level, but those that are must be prevented at all costs.
High	This misbehaviour in this asset has a serious impact on the business, and will be fatal if not addressed quickly.
Medium	This misbehaviour in this asset can be tolerated for a time, but will become serious if not addressed.
Low	This misbehaviour in this asset can be tolerated, but it does degrade business function or efficiency.
Very low	This misbehaviour in this asset has negligible impact on the business.

- Impact: how bad is it if something goes wrong
  - specified for each possible asset misbehaviour
  - impact of threats = impact of the misbehaviours they cause

© University of Southampton IT Innovation Centre 2020

Risk Levels

Risk level	Means
Very high	The risk cannot be allowed to arise.
High	The risk cannot be allowed to persist even for a short time. Parts of the system must be shut down to prevent the risk if control measures cannot be introduced immediately.
Medium	The risk can be tolerated for a short time while control measures are introduced to address it.
Low	The risk can be tolerated for a long period if necessary. Control measures should be used to prevent it, if they are available and cost effective.
Very low	The risk can be accepted, no control measures are needed.

- Risk level measures the significance of a threat or misbehaviour
  - determined from the likelihood and impact
  - taking into account any security controls

© University of Southampton IT Innovation Centre 2020

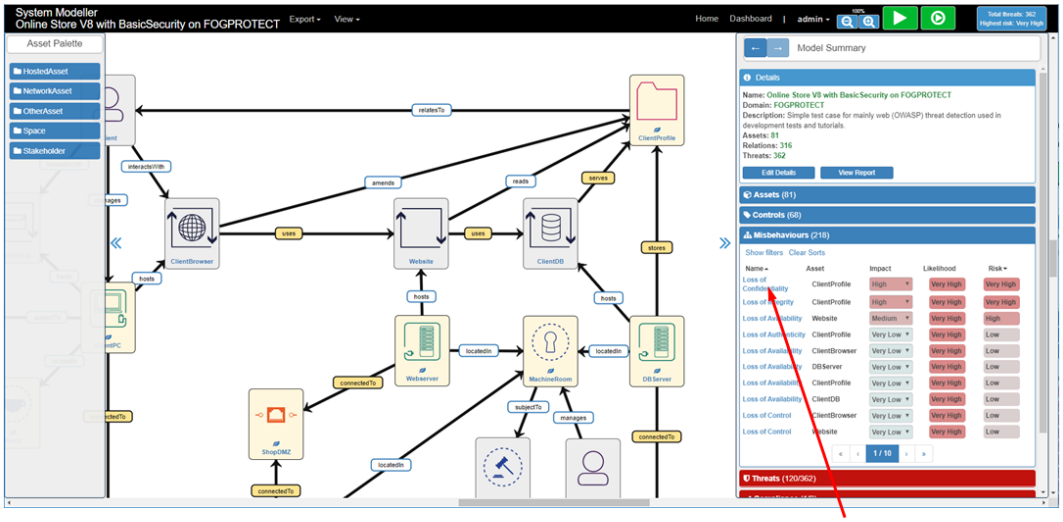
Risk Levels

Impact	Likelihood				
	Very Low	Low	Medium	High	Very High
Very Low	Very Low	Very Low	Very Low	Low	Low
Low	Very Low	Very Low	Low	Low	Medium
Medium	Very Low	Low	Medium	High	High
High	Low	Medium	High	Very High	Very High
Very High	Low	Medium	High	Very High	Very High

- Risk level measures the significance of a threat or misbehaviour
  - determined from the likelihood and impact
  - taking into account any security controls
- Note: likelihood, impact and risk level scales are part of the domain model, and cannot be changed per system

© University of Southampton IT Innovation Centre 2020

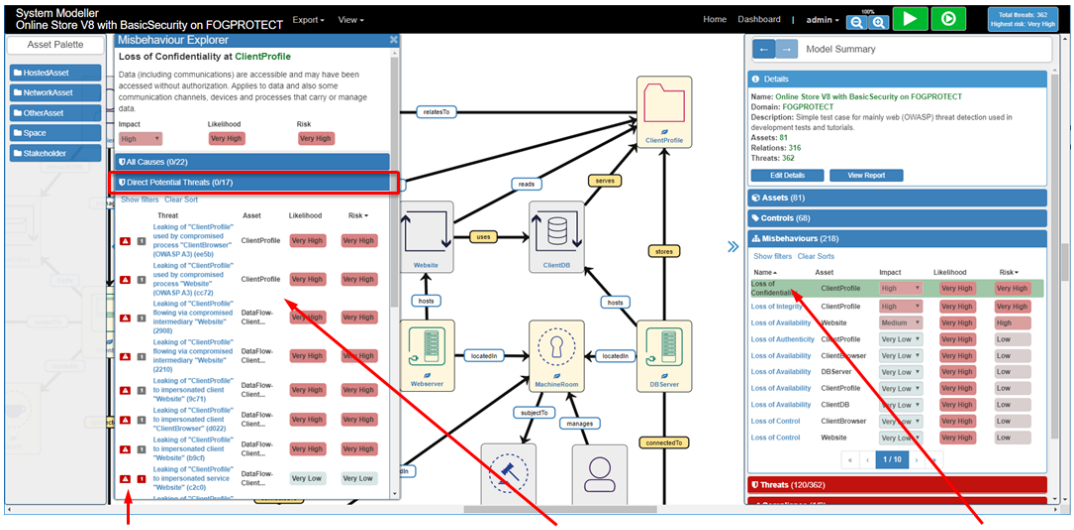
Attack Paths and Secondary Effects



Click on a threat
Effect to find causes

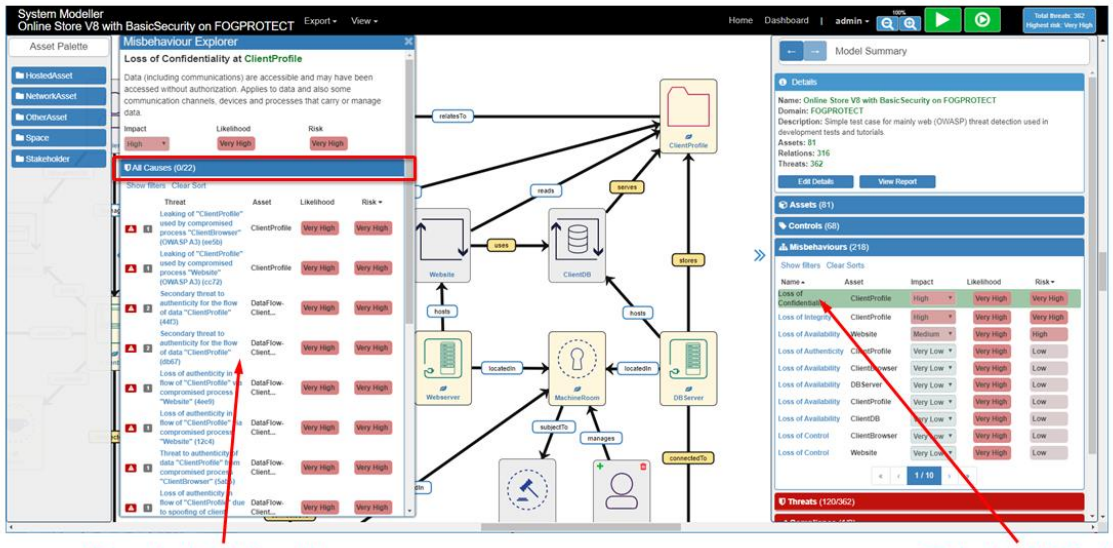
© University of Southampton IT Innovation Centre 2020

Attack Paths and Secondary Effects



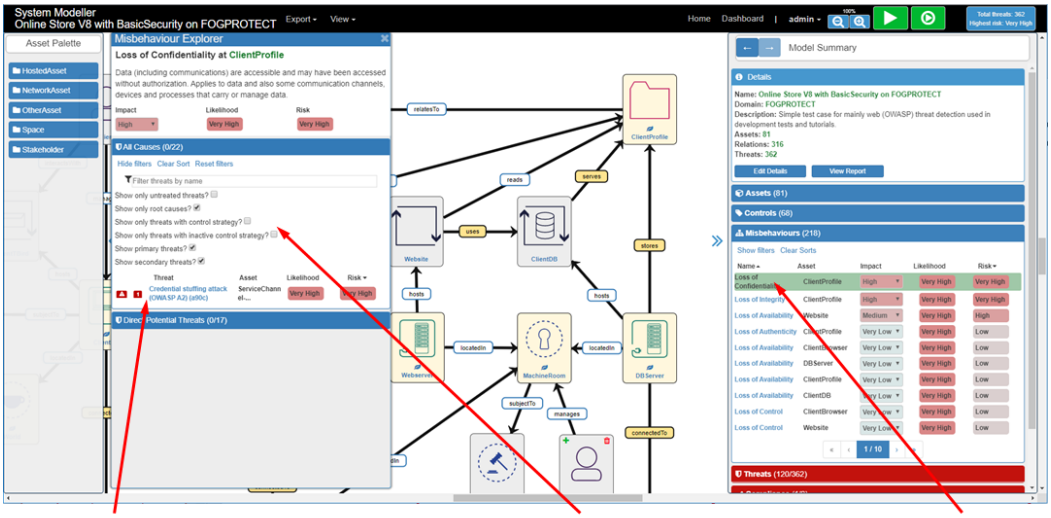
© University of Southampton IT Innovation Centre 2020

Attack Paths and Secondary Effects



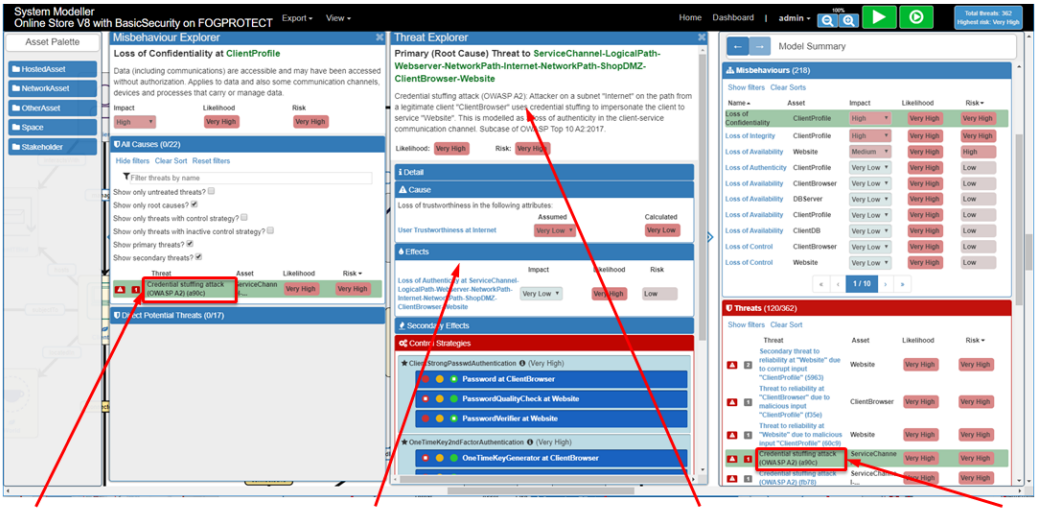
© University of Southampton IT Innovation Centre 2020

Attack Paths and Secondary Effects



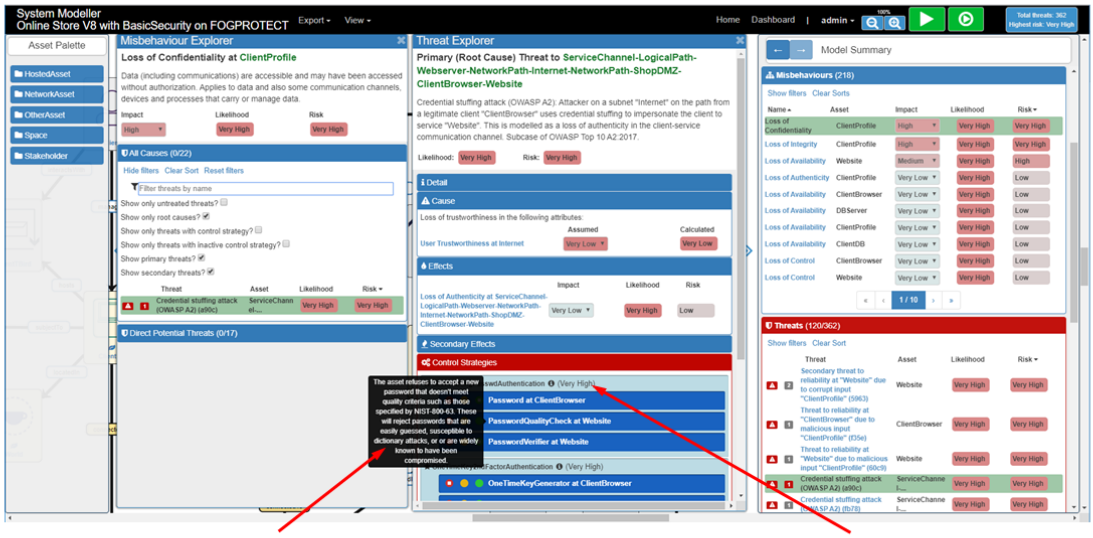
© University of Southampton IT Innovation Centre 2020

Addressing Threats



© University of Southampton IT Innovation Centre 2020

Addressing Threats

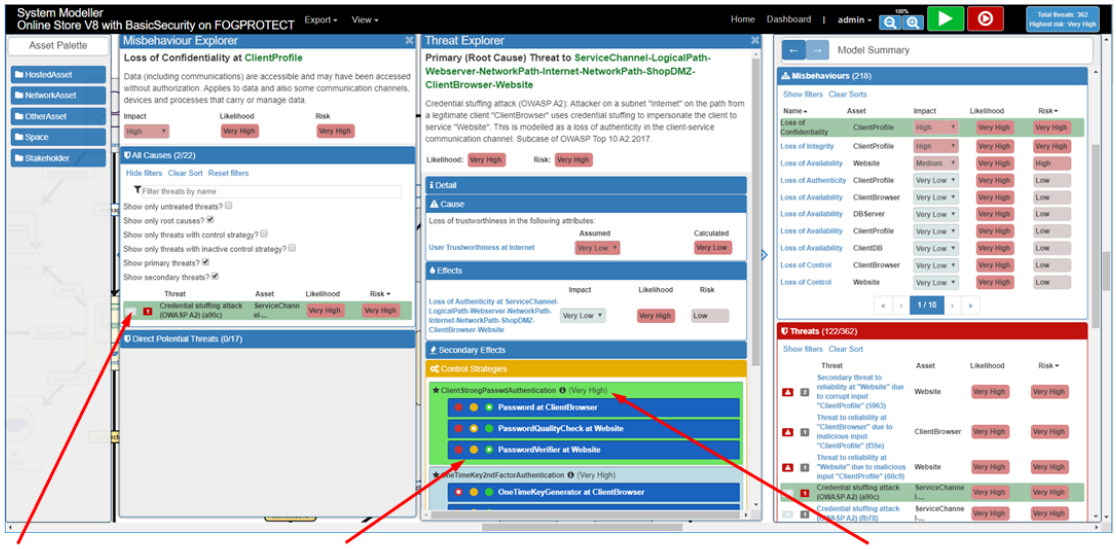


Tooltips explaining controls (here a password quality check)

Possible Control Strategy: a set of security measures that block/mitigate the threat

© University of Southampton IT Innovation Centre 2020

Addressing Threats



Threat is now addressed

Control selections: implemented, planned or not implemented

Effect of Control Strategy, expressed as a level of trustworthiness

© University of Southampton IT Innovation Centre 2020

Addressing Threats

- The future risk levels are calculated assuming the 'planned' controls will be implemented
- In future we may add a report generator that extracts the planned changes

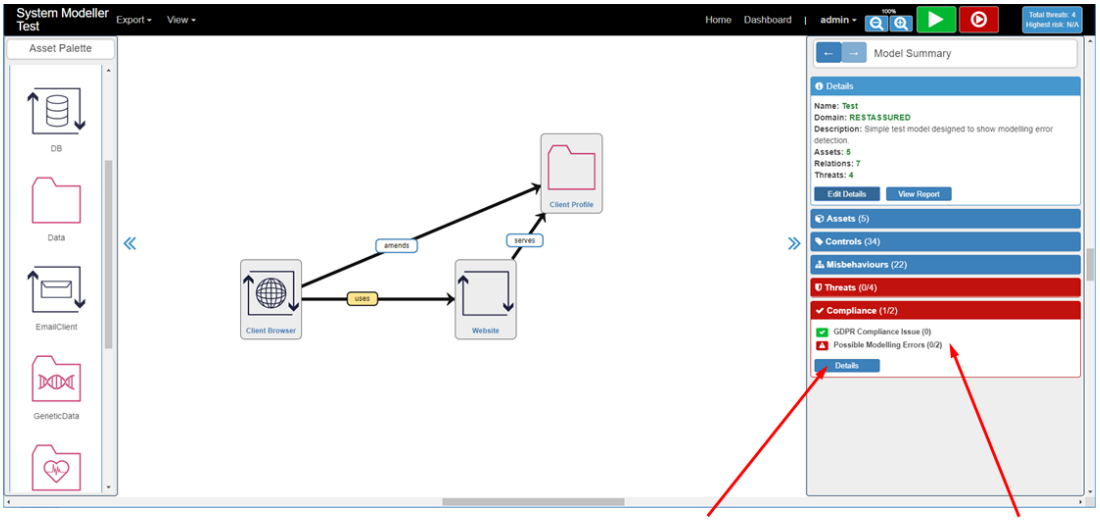
© University of Southampton IT Innovation Centre 2020

Compliance Threats

- Special type of threat used to model situations that may not comply with laws or regulations, best practice guidelines, etc
  - they don't represent security issues, so they don't have causes, effects or likelihood and risk levels
  - they may have control strategies corresponding to security or other measures with which the situation represented by the threat would comply
- When creating a model, the Modelling Error compliance set can be helpful – it models guidelines on how to build a valid SSM model
  - detects internal consistencies within the model, e.g. communication between processes where there is no network path between devices
  - detects inconsistency with domain model assumptions, e.g. if the domain model assumes every run-time Process must have a Host device

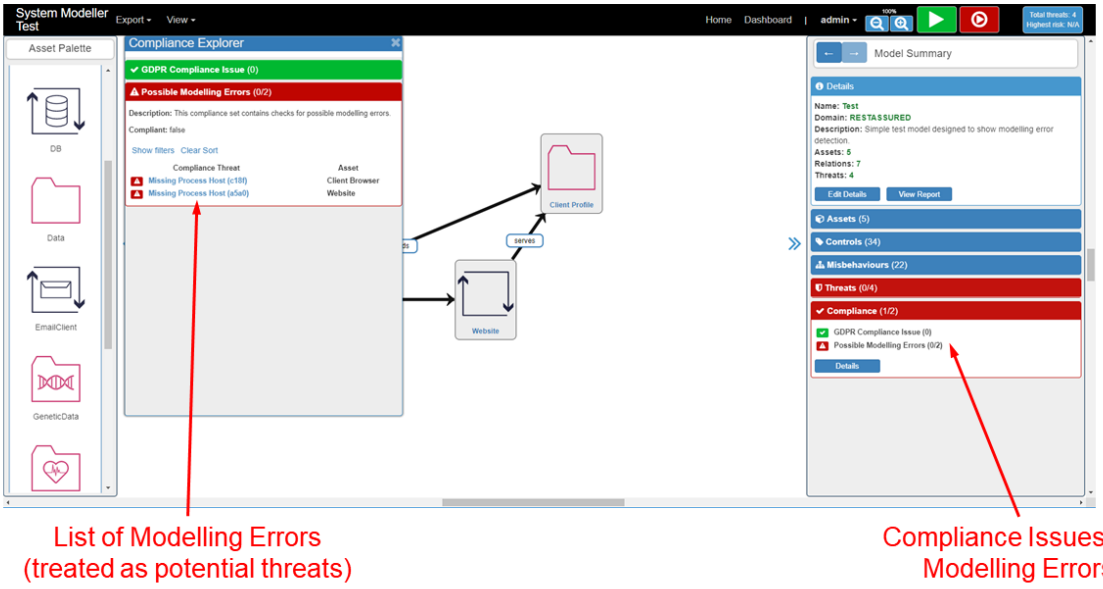
© University of Southampton IT Innovation Centre 2020

Model Error Checking



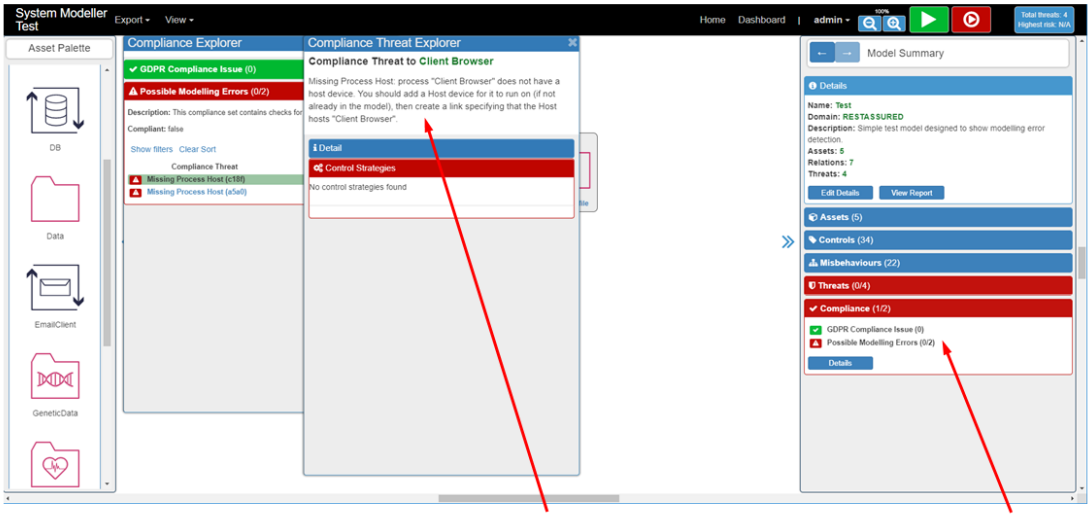
© University of Southampton IT Innovation Centre 2020

Model Error Checking



© University of Southampton IT Innovation Centre 2020

Model Error Checking

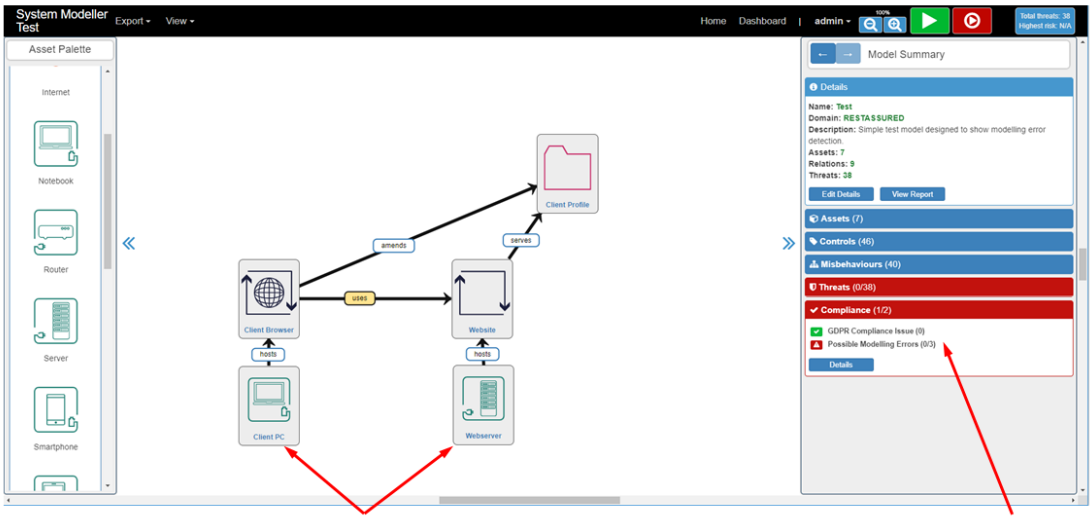


Details of the Error (in this case a Process is executing but doesn't have a Host)

Compliance Issues and Modelling Errors

© University of Southampton IT Innovation Centre 2020

Model Error Checking

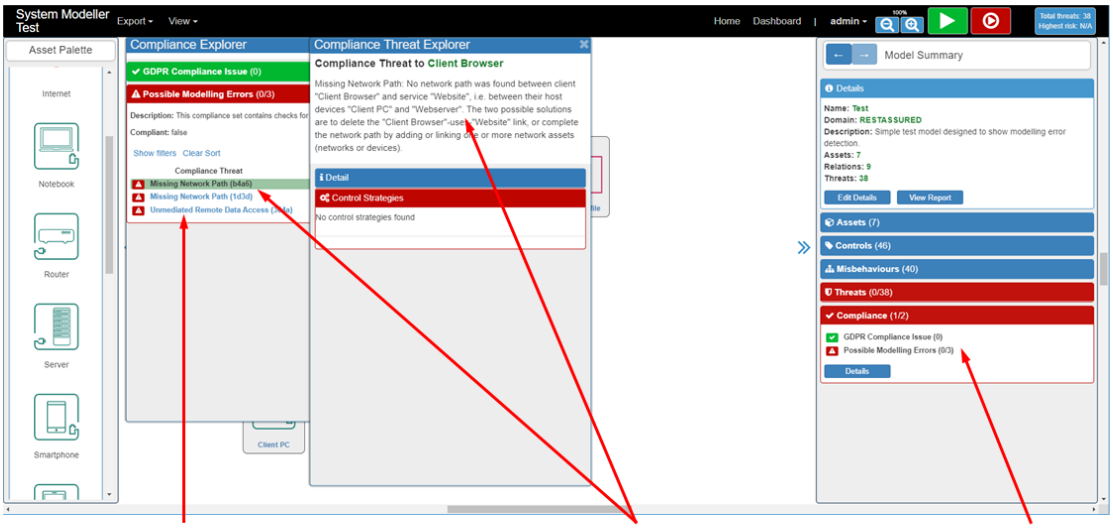


Fixed errors by adding host devices for each process

We now have some new Modelling Errors

© University of Southampton IT Innovation Centre 2020

Model Error Checking



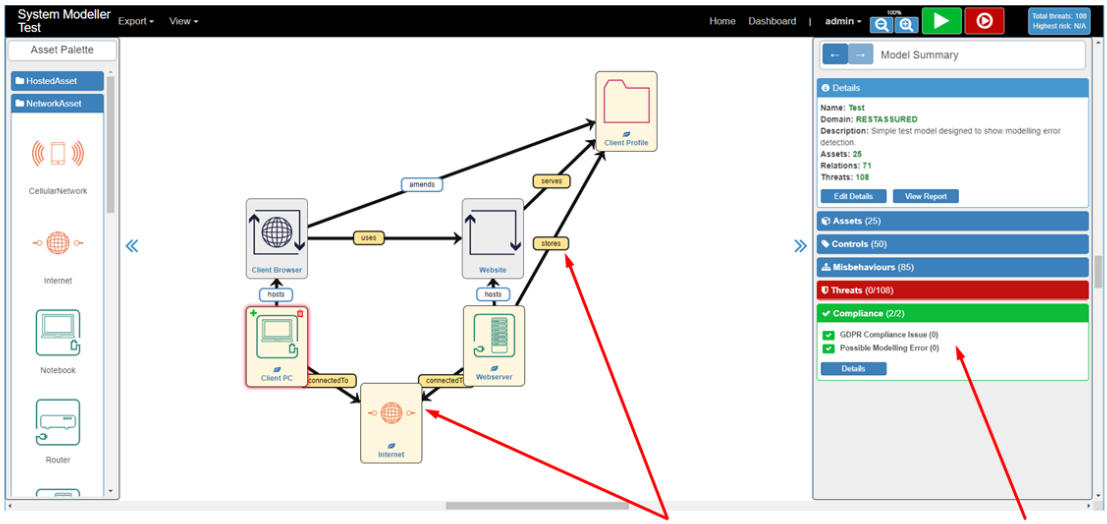
Data is being served but not stored

Problems due to communication without a network path

We now have some new Modelling Errors

© University of Southampton IT Innovation Centre 2020

Model Error Checking



Connected devices via a network subnet and specified data storage

No Modelling Errors

© University of Southampton IT Innovation Centre 2020

ISO 27005 Risk Assessment
Residual Risk Reduction Analysis Exercise
(Online Store v8 and Domain Model v3i)

ISO 27005 Risk Assessment

1. Identify system assets and relationships and build a system model
2. Autogenerate hidden (inferred) assets, asset properties, and threats
3. Specify input assumptions by overriding defaults where necessary
   – impact levels for different threat effects on primary assets
   – trustworthiness levels for shared assets
4. Add security measures already specified or implemented
5. Calculate likelihood and risk levels
   – threat likelihood based on trustworthiness assumptions, plus attack path and secondary effect propagation
   – effect likelihood and (by combining with impact level) associated risk level
   – degraded trustworthiness levels caused by threat effects
6. If the risk levels are not acceptable
   – add more security measures and go to step (5), or
   – go to back to step (1) and change the design (i.e. asset composition)

© University of Southampton IT Innovation Centre 2020

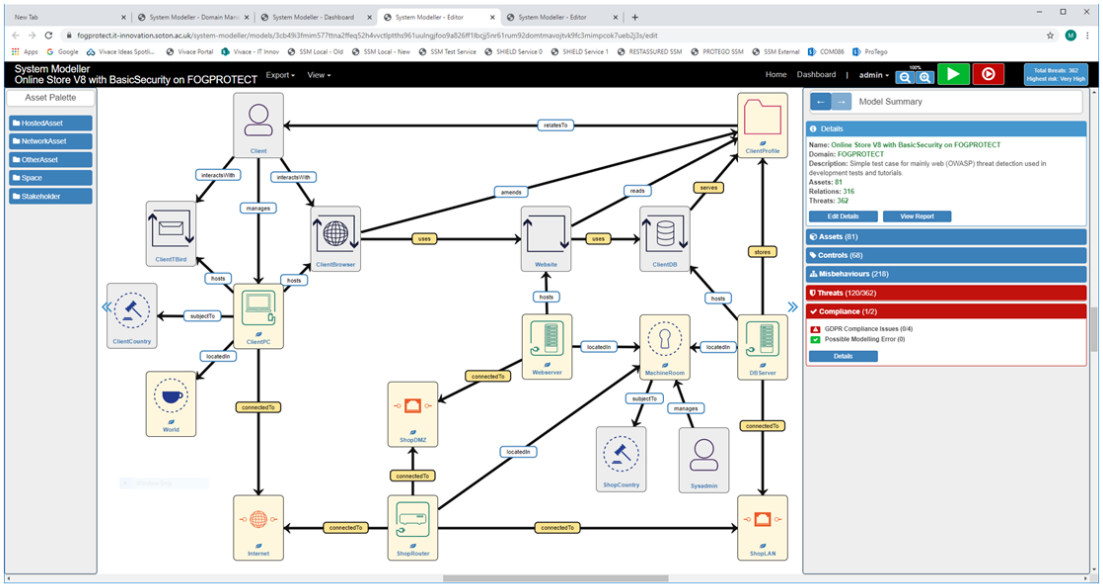
Step 1: Identify Assets

Example: Online Shop

- An online retailer has a traditional network protected by a firewall router divided into two subnets
  - a DMZ containing a web server running their online shop website
  - a LAN containing a data server hosting a DB serving client profiles
- The website uses the DB to access the client profiles
- Both servers and the firewall are in a machine room at the retailer's premises, which may be in a different jurisdiction from the client
- Clients access the website via a browser over the Internet using a mobile device (laptop, tablet or phone), which we assume
  - may be used in a public place (somewhere in the world)
  - is also used to run an email client and read email
- We created a model for this earlier, called 'Online Store'

© University of Southampton IT Innovation Centre 2020

Step 1: An Example System Model



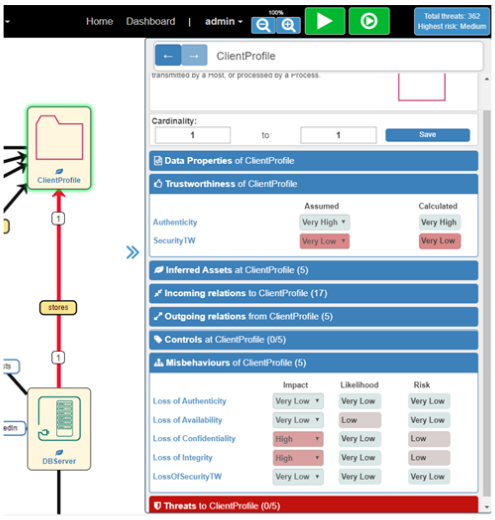
© University of Southampton IT Innovation Centre 2020

Step 2: Validate the Model to find Threats

- Generates dozens of 'inferred' assets representing points of attack or defence, e.g. network interfaces, network paths, data flows, etc
- Adds asset trustworthiness and misbehaviours attributes with default trustworthiness and impact levels depending on asset type
  - revalidation retains previously asserted overriding of these default levels
- Adds security control attributes (but with all controls deselected)
  - revalidation retains previously asserted control selections
- Generates a threat catalogue containing over 300 threats
  - the exact number depends on the domain model

© University of Southampton IT Innovation Centre 2020

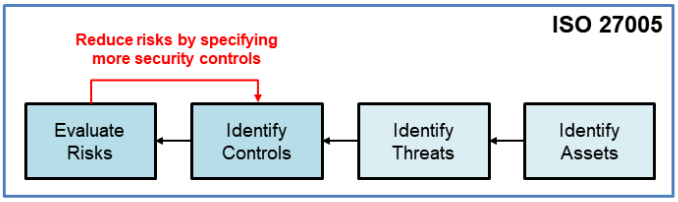
Step 3: Add Risk Assessment Inputs



- Add impact levels for threat effects on primary assets
  - data, key processes – which are they?
  - SSM calculates asset dependencies so usually we can ignore secondary assets
- Add trust assumptions especially for shared assets
  - default values are mostly OK, e.g. very low user trustworthiness for the Internet
  - main concern is usually human assets
  - how trustworthy are people in each user role?
- Without this step risks levels are low!!!

© University of Southampton IT Innovation Centre 2020

Step 4: Add Security Measures



- One can start with no security, e.g. if one is modelling a new system design
  - this is not recommended, as you will get hundreds of high risk threats
- Best to start by adding basic security measures, e.g.
  - firewall restrictions for Interfaces to public networks or paths (logical network 'segments') through routers leading from public to private networks
  - software patching for devices, and malware protection for personal devices
  - access control for services and key data assets
  - at least username/password authentication and transport security for client-service comms
  - physical security for private spaces (if appropriate)

© University of Southampton IT Innovation Centre 2020

Step 5: Calculate Risk Levels

- If risk levels are relatively low then either
  - you didn't specify an impact for compromises of your primary assets, or
  - you did a brilliant job when selecting security measures
- Most people overlook something, unless they are robots(!)
- SSM can help (at design time) with iterative residual risk reduction
  - automatically finding attack paths and secondary effect cascades
  - finding gaps between the specified security measures whereby these can have an unacceptable impact
  - adding more security to fill those gaps, and analysing its effectiveness
  - occasionally rethinking the trust/impact assumptions or the entire system design

© University of Southampton IT Innovation Centre 2020

Step 6: Reduce Risk Level

- Recalculate the risk level – what do you see?
- How could you reduce the risk level by specifying security measures
  - from Very High to High: possible by finding and blocking a single attack path
  - from High to Medium: requires more than one attack path to be countered
  - from Medium to Low: what do we need?
- Tips: look for threats with high risk levels that have control strategies
  - start from the system level list of threat effects (Misbehaviours)
  - find causes of high risk effects by using the Misbehaviour Explorer
  - use filters to find root causes or other threats with viable control strategies
  - select appropriate controls to fulfil a control strategies that is strong enough to reduce the threat likelihood

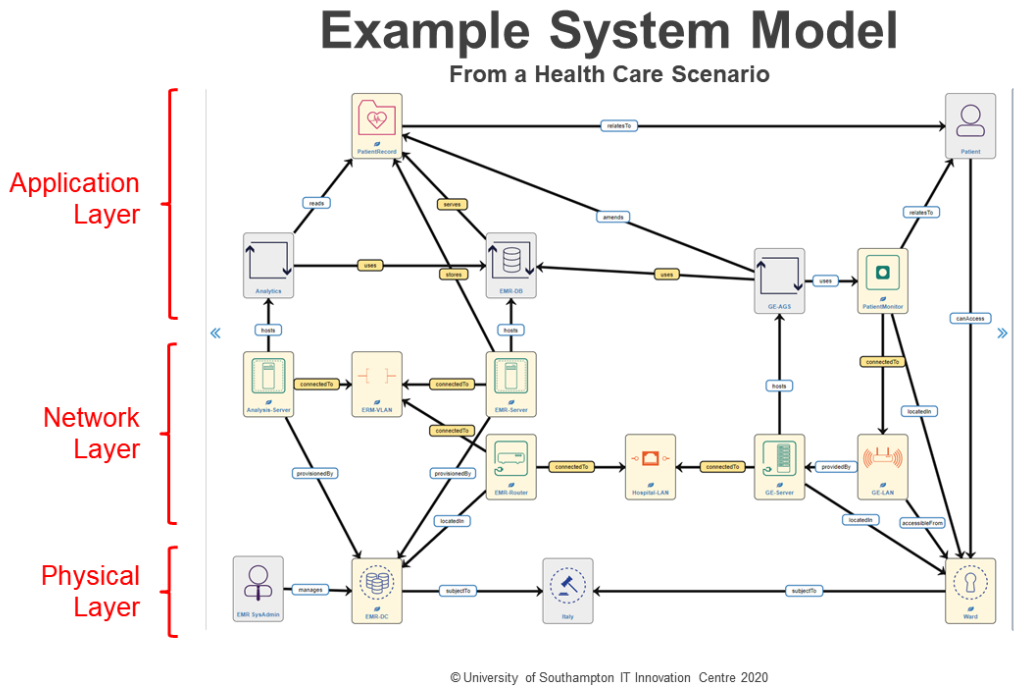
© University of Southampton IT Innovation Centre 2020

Step 6: Reduce Risk Level

- Recalculate the risk level – what do you see?
- How could you reduce the risk level by specifying security measures
  - from Very High to High
    - strong passwords to block a credential stuffing attack
  - from High to Medium
    - XSS sanitisation (using code analysis tools) to exclude reflective XSS attacks to steal session keys
    - 2FA to block phishing attacks to steal passwords (even strong ones)
  - from Medium to Low
    - restricted shell or pen testing to prevent command injection via the website
    - pen testing to prevent query injection via the website
    - counter DoS attacks from the Internet by arranging for the ISP to provide some protection for the website IP address (i.e. the address of the router Interface on the Internet)

© University of Southampton IT Innovation Centre 2020

How to Build a System Model in Layers



System Model Building

- Always start with the application layer
  - including IoT Things (if relevant)
  - including Humans with relationships to Data or Process assets
- Then add other physical and virtual devices
- Then add spaces, jurisdictions and other users
  - including Humans that manage spaces and/or devices

© University of Southampton IT Innovation Centre 2020

Example System Model

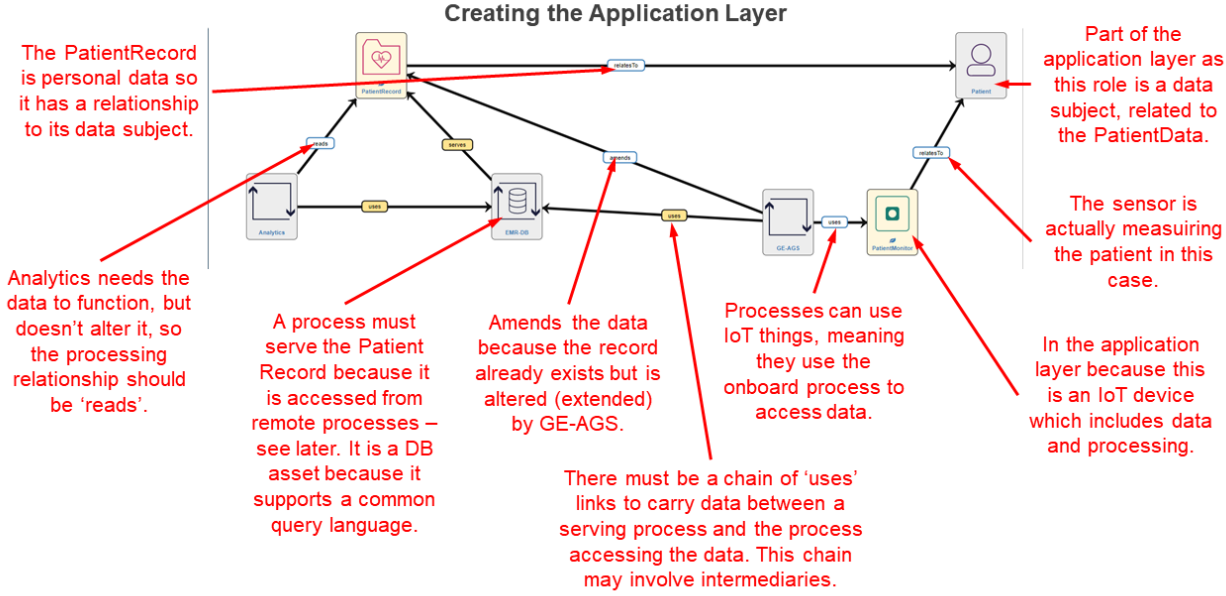
From a Health Care Scenario

- The IoT example model is a simplified medical scenario
- Patients are cared for in a Ward, where sensors are used to monitor their vital signs
- Measurements are written to the patient record database running on a VM in the hospital's data centre
- A data analytics process is run every hour, looking for patterns that indicate changes in patient status in the next 24 hours
- This information is used to prioritise the use of time by consultants who are responsible for planning treatment given to each patient

© University of Southampton IT Innovation Centre 2020

Example System Model

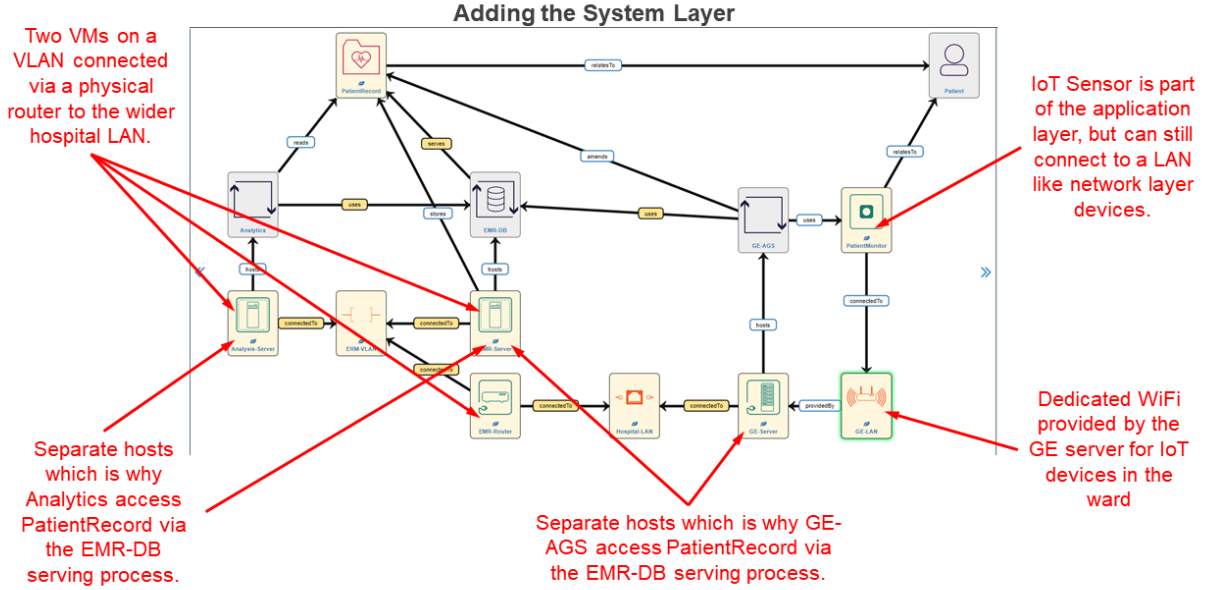
Creating the Application Layer



© University of Southampton IT Innovation Centre 2020

Example System Model

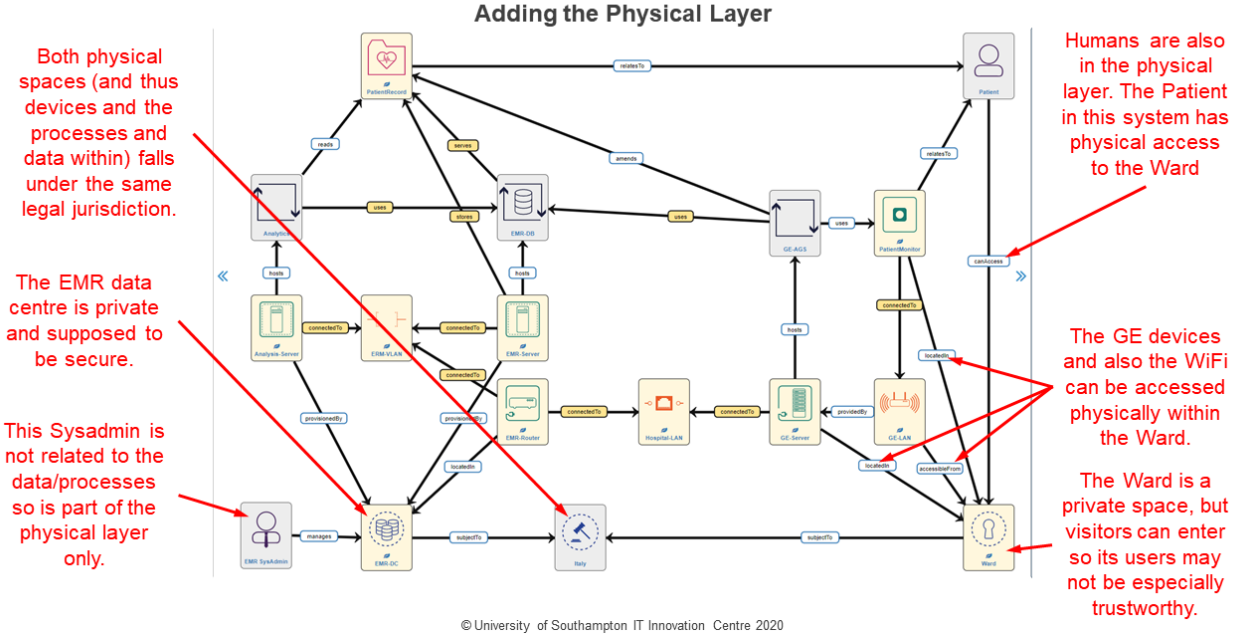
Adding the System Layer



© University of Southampton IT Innovation Centre 2020

Example System Model

Adding the Physical Layer



© University of Southampton IT Innovation Centre 2020

Summary

- Model systems in layers: application, network, physical
  - bearing in mind that IoT devices are really application processes and data
- Try to include everything unless you are sure it cannot be a source of threats, e.g. only leave out spaces if they are 100% secure
- Express process-data relationships in accordance with the model
  - use different relationships to encode read/write access and process dependency on data
  - access to stored data is either on the same device or via a remote serving process
  - remember this is a security model: try to express where the data really comes from and where it goes to
- When the model gets big, don't get confused by the crossing lines

© University of Southampton IT Innovation Centre 2020

System Security Modeller (SSM) Tutorial

Mike Surridge
ms@it-innovation.soton.ac.uk

IT Innovation Centre, Southampton
30 April 2020 Update

APPENDIX D. SURVEY TO ASSESS THE TRAINING PROGRAM

#ID	SECTION	QUESTION	ANSWERS
1	Risk Awareness Profile	Which area do you work in?	IT Support Physician Nurse Nurse assistant
2	Risk Awareness Profile	How would you define your current technological expertise?	**Beginner**: for example I am able to use a mouse and keyboard, create a simple document, send and receive e-mail, and/or access web pages **Intermediate:** for example I am able to format documents using styles or templates, use spreadsheets for custom calculations and charts, and/or use graphics/web publishing **Expert:** for example I am able to use macros in programs to speed tasks, configure operating system features, create a program using a programming language, and/or develop a database.
3	Risk Awareness Profile	Which tools does the Hospital provide to inform its employees on cybersecurity? (It's possible to select more than one options)	A regulation for the usage of computing resources Cybersecurity training courses Informative materials on cybersecurity sent by e-mail I don't know None Other: (Indicate)
4	Risk Awareness Profile	To carry out your working activities you use:	Mainly personal devices (smartphone, computer, tablet) Mainly business devices (smartphone, computer, tablet provided by the Hospital) Both None of them
5	Risk Awareness Profile	Which of the following behaviors do you adopt in the working environment? (It's possible to select more than one options)	I use different passwords for my different accounts I don't install freeware I don't write my passwords on paper supports I don't share my passwords with my colleagues I don't save my passwords on the browser I am using I don't install pirated software I check the security setting of a web site before entering any private information I don't open e-mail attachments from people I do not know I don't use USB key that I don't None of these
6	Risk Awareness Profile	Which of the following measures do you apply to protect your devices (both personal and/or business) from cyber attacks? (It's possible to select more than one options)	I manage the privacy settings of web sites I keep the antivirus updated I block the pop-up I backup business data on business network drives I set the web browser to stricter security levels I use a firewall I use filters for e-mail

			I keep the operating system updated None of these
7	Risk Awareness Profile	Which tool do you use for sharing personal data and/or sensitive data of other people? (It's possible to select more than one options)	Business application Business file sharing Business e-mail Personal e-mail External Cloud Business Cloud (Dropbox Enterprise) External USB/HD key Skype WhatsApp None of these Other: (Indicate)
8	Risk Awareness Profile	Which of the two screens do you think is potentially risky in terms of cybersecurity?	(Select 1 among the two offered) Both of them I don't know
9	Risk Awareness Profile	**I feel that** I could fall victim to a malicious attack If I failed to comply the regulation for the usage of computing resources	1 - Totally disagree 2 3 4 - Neither disagree nor agree 5 6 7 - Totally agree
10	Risk Awareness Profile	**It is inconvenient to** spend time on cybersecurity training courses	1 - Totally disagree 2 3 4 - Neither disagree nor agree 5 6 7 - Totally agree
11	Effectiveness / Opinion	How did you land on the educational website?	Through the link on the email that I received from the hospital Through a QR code on a poster that I came across in the hospital Through a QR code on the tips that I came across in the hospital Other Please enter a description:
12	Effectiveness / Opinion	Which of the following videos of the educational website did you watch?	The Good Employee Safe Passwords Social Engineering Mobile Devices I haven't watched any of these videos
13	Effectiveness / Opinion	When I have to share a document that contains sensitive data	USB keys and digital devices are always safe It is not risky to leave the paper document on my colleague's desk I should always encrypt it and then share it through authorized platforms It's safe to send it via email as long as I am completely sure I'm sending it to the correct recipient It's safe to send it while I am connected to public network
14	Effectiveness / Opinion	When I need to remember a complicated password	I never write it down anywhere, I just tell it to a trustworthy person I never write it on paper, it's better to keep a digital sheet like an excel document I write it down on a very little piece of paper to be sure to always keep it with me I avoid using a password manager software, it could be hacked by a cybercriminal I should use a password manager or define the password starting from something that

			only I know
15	Effectiveness / Opinion	When I receive an email asking for some sensitive data	If in the text there are no grammar or spelling errors it is always a safe message It is not necessary to check where the link points to it is ok to click on a link even if I don't know the sender's address It is always better to check if the text contains grammar or spelling errors and the email address of the senders I don't have to check the sender's domain, email are always safe
16	Effectiveness / Opinion	When I receive an email asking for some sensitive data	Operating systems for mobile are always safer than computer ones Sometimes it's better to download apps from unofficial sources to protect your device Malwares rarely aim to infect mobile devices, because most of the data is kept in computers It's better to avoid updates because they always contain some bugged features Protection software are useful against known risks but not against unknown ones
17	Effectiveness / Opinion	Overall, I think that the material provided was	Useful …….. (1 to 5 scale) Clear ……(1 to 5 scale) Motivating...(1 to 5 scale)
18	Effectiveness / Opinion	Overall, I am satisfied with the amount of time it took to consult the material	Strongly Disagree Disagree Neither Agree nor Disagree Agree Strongly Agree
19	Effectiveness / Opinion	Overall, I think that the educational material has increased my awareness of cybersecurity	Strongly Disagree Disagree Neither Agree nor Disagree Agree Strongly Agree
20	Effectiveness / Opinion	On a scale of 0 to 10, how likely are you to recommend the ProTego platform to a friend or colleague?	(1 to 10 scale)
21	Effectiveness / Opinion	What aspects of the material did you like the most?	Free text
22	Effectiveness / Opinion	What aspects of the material would you improve?	Free text