

D2.8 - SPHINX Requirements and Guidelines v2

WP2 – Conceptualisation, Use Cases and System Architecture

Version: 1.00



SPHINX

A Universal Cyber Security Toolkit for
Health-Care Industry



Disclaimer

Any dissemination of results reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.

Copyright message

© SPHINX Consortium, 2019

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

Document information

Grant Agreement Number	826183	Acronym	SPHINX
Full Title	A Universal Cyber Security Toolkit for Health-Care Industry		
Topic	SU-TDS-02-2018 Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures		
Funding scheme	RIA - Research and Innovation action		
Start Date	1 st January 2019	Duration	36 months
Project URL	http://sphinx-project.eu/		
EU Project Officer	Reza RAZAVI (CNECT/H/03)		
Project Coordinator	Dimitris Askounis, National Technical University of Athens - NTUA		
Deliverable	D2.8 - SPHINX Requirements and Guidelines v2		
Work Package	WP2 – Conceptualisation, Use Cases and System Architecture		
Date of Delivery	Contractual	M24	Actual M24
Nature	R - Report	Dissemination Level	P - Public
Lead Beneficiary	POLARIS MEDICAL		
Responsible Author	Sergiu Marin	Email	sergiu.marin@polarismedical.ro
		Phone	+40732320779
Reviewer(s)	Nikolaos Angelopoulos and Panagiotis Panagiotidis [KT], Vagelis Papakonstantinou [VUB-LSTS]		
Keywords	User Requirements, Cyber Security Management Cycle, Framework for Improving Critical Infrastructure Cybersecurity		





Document History

Version	Issue Date	Stage	Changes	Contributor
0.1	22/11/2020	Draft	First draft from v1	Sergiu Marin (POLARIS MEDICAL)
0.2	25/11/2020	Draft	Update and revised requirements	Athanasios Tzikas, Fotios Gioulekas, Konstantinos Gounaris, Evangelos Stamatiadis (DYPE5)
0.3	11/12/2020	Draft	Updates	Yannis Nikoloudakis (HMU)
0.4	11/12/2020	Draft	Updates	Luís Landeiro Ribeiro (PDMFC)
0.5	15/12/2019	Pre-final	Update to reflect the reviewers' comments	Sergiu Marin (POLARIS MEDICAL)
0.6	18/12/2020	Draft	Review 1	Prof. Vagelis Papakonstantinou (VUB-LSTS)
0.7	22/12/2020	Draft	Review 2	Nikolaos Angelopoulos and Panagiotis Panagiotidis (KT)
0.8	22/12/2020	Pre-final	Update to reflect the reviewers' comments	Sergiu Marin (POLARIS MEDICAL)
0.9	23/12/2020	Pre-final	Quality Control	George Doukas (NTUA)
1.0	23/12/2020	Final	Final	Christos Ntanos (NTUA)





Executive Summary

This document is the next iteration of the requirements and guidelines for the SPHINX System from the end-user's perspective. In particular, this document provides an overview and the main outcomes of the work performed by the SPHINX Consortium on the SPHINX requirements and guidelines, as part of Task 2.3 - Stakeholders' Requirements.

This deliverable describes the methodological approach that has led to the definition of eighty-five requirements for SPHINX. The identified user requirements are distinguished between functional and non-functional requirements and, while the functional requirements highlight a specific functionality domain concerning the SPHINX user interface, the non-functional requirements are further classified with respect to the associated usability, maintainability and support, security and legal and ethical aspects.

The SPHINX requirements are also introduced with two categorisation methods, which serve as means for understanding the end-users' needs when addressing cybersecurity protection, in particular the design and development of the SPHINX System. The first categorisation method is based on the structure of Information Technology (IT) systems and considers the main IT components (IT Hardware Infrastructure, Networking, Applications and Security/Privacy), whereas the second categorisation method considers the five functions within the Cyber Security Management Cycle, well-known for advancing cybersecurity policies and operations in organisations.

The key innovation attained in this document is therefore the consideration of the latest cybersecurity needs and expectations on the part of healthcare organisations' IT professionals, at a time when the healthcare sector is challenged by digital transformation, the emergence of electronic and mobile health services, the integration of the Internet of Medical Things (IoMT) devices and the sharing and exchange of sensitive patient data, even in cross-border environments. Importantly, the SPHINX end-users are keen on the proactive assessment and mitigation of cyber security vulnerabilities and threats, the verification and certification of medical devices and equipment, as well as the preservation of healthcare data privacy and integrity.

The next iteration of this deliverable (D2.10) will focus in depth on the refinement of SPHINX's user requirements considering the traceability to the SPHINX use cases. Further, the SPHINX requirements will serve as the basis for the elicitation of the technical specifications leading to the actual design and implementation of the different SPHINX cyber security tools.





Contents

1	Introduction.....	7
1.1	Purpose and scope	7
1.2	Structure of the deliverable	7
1.3	Relation to other WPs & Tasks	7
1.4	Methodology	8
2	SPHINX Requirements and Guidelines	11
2.1	Functional Requirements and Guidelines	11
2.1.1	User Interface Functional Requirements and Guidelines	32
2.2	Usability Requirements and Guidelines	38
2.3	Maintainability and Support Requirements and Guidelines	39
2.4	Security Requirements and Guidelines	41
2.5	Legal and Ethical Requirements and Guidelines	43
3	SPHINX Requirements and Guidelines Matrix	46
4	Conclusion	51
5	References.....	52

Table of Figures

Figure 1: Cyber Security Management Cycle.....	10
Figure 2: Interactive Dashboard Mock-up.....	33

Table of Tables

Table 1: The Template for the SPHINX Stakeholders' Requirements.....	8
Table 2: SPHINX Requirements and Guidelines Matrix	50





Table of Abbreviations

ABBREVIATION	EXPLANATION
AAAC	Authentication and Authorisation Access Control
BYOD	Bring Your Own Device
CSMC	Cyber Security Management Cycle
CVS	Comma-Separated Values
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
ENISA	European Union Agency for Network and Information and Security
EU	European Union
GDPR	General Data Protection Regulation
HW	Hardware
IEEE	Institute of Electrical and Electronics Engineers
IoMT	Internet of Medical Things
IP	Internet Protocol
IT	Information Technology
JSON	JavaScript Object Notation
NIST	National Institute of Standards and Technology





1 Introduction

1.1 Purpose and scope

This report is the second version of the SPHINX requirements and guidelines, developed as an iteration of Task 2.3 - Stakeholders' Requirements. It incorporates all actions involved in updating the requirements for SPHINX Ecosystem from end-users' perspective, aligned with developing components functionalities.

In this context, information changing between end-users and technical partners about developing components, derive in updating the requirements as well as adding more functionalities to SHINX Ecosystem. The update process aims to align requirements with technical specifications and architecture as derived from development process of SPHINX components.

The updated requirements are mostly functionals ones coded as STA-F-xxx, but also one Security coded STA-S-xxx:

- in terms of Customer Value: STA-F-030, STA-F-050, STA-F-060, STA-F-110, STA-F-130, STA-F-160, STA-F-570, STA-F-580, STA-F-590, STA-F-600, STA-F-610, STA-F-620, STA-F-770.
- in terms of description and rationale: STA-F-020, STA-F-030, STA-F-040, STA-F-050, STA-F-060, STA-F-070, STA-F-080, STA-F-90, STA-F-100, STA-F-110, STA-F-120, STA-F-130, STA-F-150, STA-F-160, STA-F-190, STA-F-210, STA-F-220, STA-F-230, STA-F-240, STA-F-250, STA-F-260, STA-F-310, STA-F-320, STA-F-330, STA-F-340, STA-F-350, STA-F-370, STA-F-380, STA-F-500, STA-F-510, STA-F-530, STA-F-560, STA-F-570, STA-F-590, STA-F-600, STA-F-610, STA-F-620, STA-F-710, STA-F-750, STA-F-760, STA-F-770, STA-F-780, STA-S-010

Serving to report the findings of Task 2.3, this document provides the necessary updated guidelines to foster the identification of the SPHINX technical specifications and detailed architectural design, leading to the implementation of the SPHINX System. It will be updated by a third version (D2.10 - SPHINX Requirements and Guidelines v3) due for submission in June 2021, taking into consideration updates to the requirements and guidelines deriving from the work conducted on the SPHINX use cases, technical specifications and architecture.

1.2 Structure of the deliverable

This document is structured as follows: section 2 presents the users' perspective on the requirements and guidelines for the SPHINX System; section 3 describes the categorisation of the SPHINX requirements and guidelines, considering the main IT components and the cyber security management cycle; section 4 provides the matrix overview of the requirements and guidelines; section 5 presents the conclusions and future work; and section 6 collects the bibliographical references used in this document.

1.3 Relation to other WPs & Tasks

The definition of the SPHINX requirements and guidelines builds on the results of Task 2.1 on the analysis of the cyber threats and cyber security landscape and leverages the iterative work ongoing by other Tasks within WP2: the Ethical Requirements as part of Task 2.2, the SPHINX Use Cases as part of Task 2.4 and the SPHINX Technical Specifications and Architecture as part of Task 2.5. As Tasks 2.4 and 2.5 evolve, refinements are made to the initial requirements and guidelines and the updated version will be made available in the next iteration of this document (D2.10 - SPHINX requirements and guidelines v3).

The requirements and guidelines will also influence SPHINX's high-level architecture and detailed technical specifications as it determines the implementation of the SPHINX components to be conducted throughout





WP3 to WP5, the integration efforts to be conducted in WP6 and the definition of the pilot scenarios and sub-use cases to be implemented as part of the validation activities conducted in WP7.

1.4 Methodology

When defining requirements and guidelines for the SPHINX System, diverse data was utilised. The discussion of partners' experience and know-how, reflected in the definition of the cybersecurity landscape presented in Task 2.1 - Cyber Situation Awareness Trend Analysis, in the elicitation of ethical requirements in Task 2.2 - Basis of Legal and Ethical Requirements and in the identification of the SPHINX use cases in Task 2.4 - Reference Scenarios and Pilot Operations Specifications and KPIs, was fundamental to address the SPHINX requirements and guidelines from the users' perspective. Moreover, it was combined with relevant literature and the results of the end-user survey conducted in the SPHINX Workshop on Cyber Security Situation Awareness for Health Organisations (CYBERSEC4HEALTH) held in July 2019.

To deliver a structured perspective, the SPHINX requirements and guidelines follow the VOLERE methodology [1], adapted to meet the SPHINX research activities and allow agile refinement. Based on this adapted methodology, each SPHINX requirement and guideline is identified as follows:

Requirement ID:	A unique identifier, as follows: <STA><type><sequential-number> Once numbered, it shall not be changed.
Requirement Type	<p>Functional requirements (F) are the fundamental or essential subject matter of the product and are measured by concrete means like data values, decision-making logic and algorithms.</p> <p>Non-functional requirements (see letter below) are the behavioural properties that the specified functions must have. Non-functional requirements can be assigned a specific measurement. It includes:</p> <ul style="list-style-type: none"> • (U) Usability and Look and Feel Requirements; • (P) Performance Requirements; • (M) Maintainability and Support Requirements; • (S) Security Requirements; • (L) Legal and Ethical Requirements.
Use Case	Number of the use case it refers to (if applicable). Use cases are defined in D2.4, D2.7 and D2.9.
Customer Value	Mandatory: 1 to 5 scale (5 being highest; use of "shall" in description); Optional: 0 (use of "should" in description).
Description and Rationale	A one sentence statement describing the specification, highlighting the context of the specification.

Table 1: The Template for the SPHINX Stakeholders' Requirements

The information on the *Use Case* element will be part of the next iteration of this document (D2.8 - SPHINX Requirements and Guidelines v2) deriving from the work conducted iteratively with Task 2.4 concerning the SPHINX use cases (Task 2.4 - Reference Scenarios and Pilot Operations Specifications and KPIs).

Requirements are defined by a set of attributes that aim to ensure that the stakeholders obtain what they need from the requirements. However, not every stakeholder needs to know all attributes in a requirement. Hence,



categorising requirements helps to improve the communication of the different levels of requirements to the appropriate audience.

Herein, the SPHINX requirements and guidelines are classified in four major contextual categories, based on main IT components (such as the ones present in the SPHINX System) and translating both functional and non-functional requirements:

- **IT Hardware Infrastructure** – referring to the SPHINX physical system, including servers, computers, data centres, switches, hubs, routers and other equipment.
- **Networking** – referring to the SPHINX network infrastructure, including network communications, operations and management enablement and internet connectivity.
- **Applications** – referring to the SPHINX virtual system, including software components and services, middleware software, operating systems, mainframe infrastructure and mobile and wireless infrastructure.
- **Security/Privacy** – referring to the SPHINX security and privacy technologies, including security software, controls and measures.

Further, these four main categories are complemented with a total of five (5) sub-categories based on the Cyber Security Management Cycle (CSMC) established in the Framework for Improving Critical Infrastructure Cybersecurity published by the National Institute of Standards and Technology (NIST) [2]:

- **Identify** – this function starts with an assessment of the security risks in order to identify what assets to protect, their relative importance, and each asset's priority ranking for urgency and required level of protection. It also identifies what security measures are required to establish a cost-effective cyber security programme. Based on the assessment results, appropriate security protection policies, systems and safeguard guidelines are implemented to maintain a secure protection framework. A cyclic compliance or certification review follows, designed to provide assurance that security controls are in place properly and meet the users' security requirements and cope with rapid technological and environmental changes.
- **Protect** – this function allows to build user awareness on whether the appropriate level of security protection systems, measures and safeguards are implemented in a way that builds a secure and strengthened protection framework. It includes developing security policies and guidelines, assigning security responsibilities and implementing technical and administrative security measures. This step requires constant monitoring, auditing and recording so that vulnerabilities are eliminated or mitigated, and proper protective arrangements are activated when addressing security events, incidents and attacks.
- **Detect** – this function aims to develop and implement the appropriate cyber security activities to early identify the occurrence of a cyber security event, by establishing a sound monitoring and measuring of the status of security across the organisation's IT ecosystem. All deployed security systems, measures and safeguards are examined either continually or periodically to identify new developed vulnerabilities and detect cyber security events, incidents or attacks that are reported or notified to system administrators, functioning as alerts or mere information.
- **Respond** – this function implements the incident or attack response plan, based on the characteristics of the cyber incident, event or attack and the severity of the attack. The mitigation of the attack and its effects, the analysis of the organisation's response to the attack and the handling of all communication in the process are key to understand the cyber security protection in place and its compliance to the organisation's security policy.
- **Recover** – this function encompasses the implementation of appropriate activities to maintain the organisation's resilience and to restore any capabilities or services that were impaired due to a cyber security attack. It also allows to identify any enhancements necessary on the deployed cyber security framework to strengthen its protection level, update security practices and strategies and accommodate the organisation's evolving cyber security needs.

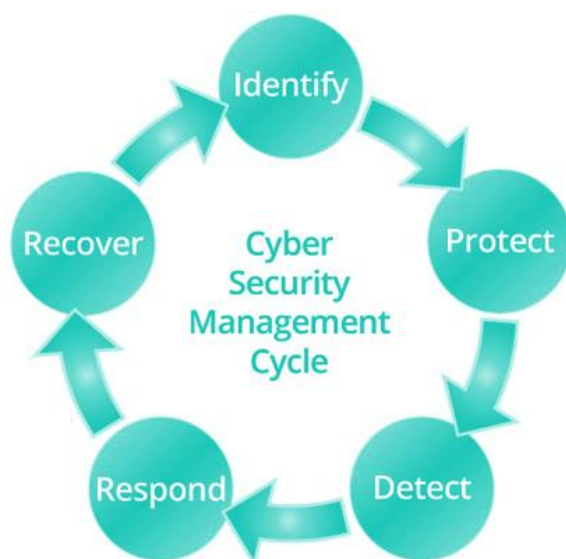


Figure 1: Cyber Security Management Cycle



2 SPHINX Requirements and Guidelines

According to the Institute of Electrical and Electronics Engineers (IEEE) Standard 729, a requirement is defined as a condition or capability needed by a user to solve a problem or achieve an objective, which may include increased productivity, enhanced quality of work, reduction in training costs and improved user satisfaction. That condition or capability must be met by a system or system component to satisfy a specification of a technical nature. In this context of the use of the system, the requirements identify the users' needs that *express the intended interaction the system will have with its operational environment and that are the reference against which each resulting operational capability is validated* [3].

The SPHINX Requirements and Guidelines reflect the project partners' insight on the needs, gaps and ambition involving the design, implementation and operation of cybersecurity systems for healthcare IT environments.

Cybersecurity is a continuous improvement process in all organisations and the incredible dynamics of today's cyber threat landscape renders the protection of the modern enterprise an enormous challenge. Configurations are in constant flux, hardware is being cycled, software is being updated, workloads are moving to the cloud and users are bringing devices in and out of the network. At the same time, random attacks are entering the system, and there is the danger of well-funded, determined external attackers trying to steal valuable data from healthcare organisations. Protect, Detect and Respond are key to a secure organisation.

By summarising the opinions, viewpoints and experiences of actual end-users, SPHINX establishes the requirements that specify the needs in terms of the cyber security tasks to be performed, the healthcare IT environment's specificities as well as the risks to be considered and mitigated within SPHINX. The definition of requirements and guidelines also contribute to the development of an intuitive, easy-to-use and efficient user interface, allowing SPHINX users to supervise and guide the SPHINX System in cybersecurity management tasks.

The SPHINX Requirements and Guidelines are presented next.

2.1 Functional Requirements and Guidelines

Functional requirements and guidelines are identified by end-users as the basic facilities that the system shall offer. These specific functionalities need to be necessarily incorporated into the system in the form of input to be given to the system, the operation performed, and the output expected. For the SPHINX System, relevant functional requirements and guidelines are presented next.

SPHINX shall support advanced cyber security capabilities.	
Requirement ID	STA-F-010
Requirement Type	Functional Requirements
Use Cases	-
Customer Value	5
Description and Rationale	The SPHINX Platform shall detect intrusions, attacks, misuse or infections (in second and minute timeframes), transform raw data and records of activity or changes into real actionable intelligence (insights the user can act upon), propose rapid, accurate, consistent and reliable courses of action considering the nature of a breach, its effects and the consequences of the suggested actions (enhanced decision support) and respond immediately to contain infections, avert data losses and prevent onward intrusion.





Categorisation	per IT Domain	per Function of the CSMC
	IT Hardware Infrastructure; Networking; Applications.	Protect; Detect; Respond.

SPHINX shall enable interactions with existing cyber security tools.		
Requirement ID	STA-F-020	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall enable a seamless interaction with cybersecurity detection, monitoring and reaction tools (e.g., firewall, antivirus software, email monitoring software, blockers of unauthorised Internet sites, log analysers) already in use by healthcare organisations, considering the existing IT ecosystem and contributing to advance the overall level of security and to reduce the users' workload. In greater detail SPHINX Platform shall support commonly deployed security devices by allowing the integration and consumption of their audit and transaction logs.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Detect; Respond.

SPHINX shall focus on preventing human errors.		
Requirement ID	STA-F-030	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	4	
Description and Rationale	The SPHINX Platform shall aim to prevent human errors, as much as malicious actions. It will map the login user names to certain security levels and actions. SPHINX shall contribute to educate and train the healthcare organisations' employees on best cybersecurity practice and shall implement automated functions to assist in preventing phishing, poor password practices, mis delivery and the sharing of access to devices and systems with unauthorised parties. The SPHINX automated functions shall also contribute to reduce users' security fatigue (the condition when users feel so burdened by following cybersecurity procedures that they stop trying).	
Categorisation	per IT Domain	per Function of the CSMC
	Applications; Security/Privacy.	Protect.



SPHINX shall be designed to support business continuity.		
Requirement ID	STA-F-040	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall be designed to significantly contribute to business continuity aspects, implementing security measures that streamline a timely and effective response and prevent the loss of data, compromised information and unplanned downtime, while advancing the overall healthcare organisations' system resilience. It should provide alternative solutions and work path to follow in the case of a security incident. It should consider ongoing attacks on priority assets and their pivoting potential to other devices and networks, providing a holistic risk view for situational awareness.	
Categorisation	per IT Domain	per Function of the CSMC
	IT Hardware Infrastructure; Applications; Security/Privacy.	Protect; Respond; Recover.

SPHINX shall identify new, modern and advanced cyber threats.		
Requirement ID	STA-F-050	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	4	
Description and Rationale	The SPHINX Platform shall have the capability to continuously monitor the cyber ecosystem and to identify new, modern and advanced cyber threats in order to facilitate the protection of the healthcare organisations' assets, as well as the detection and response to cyber incidents. It should be able to be trained to detect anomalies inside the healthcare networks by recourse to user and device profiling.	
Categorisation	per IT Domain	per Function of the CSMC
	IT Hardware Infrastructure; Networking; Applications.	Identify.

SPHINX shall interact with existing and well-known cyber threat intelligence repositories.		
Requirement ID	STA-F-060	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	4	
Description and Rationale	The SPHINX Platform shall integrate relevant information provided by third-parties' highly-regarded security and threat intelligence repositories to support security assessment functions and to better inform the decision-making process of healthcare organisations' IT administrators and operators.	





Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Identify.

SPHINX shall protect against known cyber-attacks.		
Requirement ID	STA-F-070	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall integrate the knowledge of how to protect against the most common cyber threats, how to respond to known cyber-attacks and which are the associated consequences of the proposed response, in order to facilitate the users' decision-making process and to support business continuity. This knowledge should be well formulated and freely available on a central knowledge base, clearly marked it is already known and validated.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Protect; Respond.

SPHINX shall provide a personalised data security management tool.		
Requirement ID	STA-F-080	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall deliver a personalised data security management tool, allowing the users to setup and configure the specific tools required by the underlying IT ecosystem. The ecosystem should be customisable matching the variances of the different Health Organisations. It should allow for different tools to be turn on and off on demand per installation. This should provide a degree of freedom to integrate with 3rd parties through the properly specified APIs.	
Categorisation	per IT Domain	per Function of the CSMC
	IT Hardware Infrastructure; Networking; Applications; Security/Privacy.	Identify; Protect; Detect; Respond; Recover.

SPHINX shall provide a cyber security inspection, discovery and decision toolset (cyber security toolkit).		
Requirement ID	STA-F-090	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	





SPHINX shall provide a cyber security inspection, discovery and decision toolset (cyber security toolkit).		
Description and Rationale	The SPHINX Platform shall deliver a cyber security toolkit, comprising a set of available security services, that are capable of providing users with a wide range of options, such as inspection, discovery, monitoring, analysis, decision support and protection including distributed denial of service (DDoS) protection, advanced threat intelligence and identity and access management. The users are able to select the security services that meet their needs when designing the security strategies and defining a clear and actionable roadmap towards enhancing the level of protection of the healthcare organisation's assets.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Identify; Protect; Detect; Respond.

SPHINX shall be able to handle and process data originated by a large number of devices and services.		
Requirement ID	STA-F-100	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall have the capability to handle and process the data produced by a large number of devices and services, maintaining adequate quality of service (this capability cannot affect the normal operations of devices and services). The SPHINX Platform shall provide a comprehensive overview of the collected data to the users, to facilitate the users' awareness and decision-making processes. The SPHINX platform must be robust and stable, and data shall be coherently overviewed and presented to the users. It should be able to process within reasonable time, the massive volumes of information collected from all devices and services already deployed.	
Categorisation	per IT Domain	per Function of the CSMC
	IT Hardware Infrastructure; Networking; Applications.	Protect; Detect.

SPHINX shall provide cybersecurity vulnerability assessments.		
Requirement ID	STA-F-110	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	4	
Description and Rationale	The SPHINX Platform shall perform continuous assessments of the IT ecosystem to identify and assess existing cyber vulnerabilities, based on the information collected on the underlying IT ecosystem. The cybersecurity vulnerability assessments shall be based on the Common Vulnerability Scoring System CVSS 3.0 assessment model and	



	consider the compliance with the ISO/IEC 27001 standard. The SPHINX Platform shall report the results of the cybersecurity vulnerability assessments, ascertaining their potential impact and presenting the information to the user for decision-making purposes. The assets and devices to be scanned should be configurable by the end-users, as well as the type and safety of the scans. It should be possible to schedule multiple scans, with different frequencies and scan profiles.	
Categorisation	per IT Domain	per Function of the CSMC
	IT Hardware Infrastructure; Networking; Applications.	Identify; Detect.

SPHINX shall enable the vulnerability assessment of devices to be connected to the organisation's IT ecosystem.		
Requirement ID	STA-F-120	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall perform continuous assessments of medical and IoT-based devices in the network against patches and operating systems' versions. Newly added devices, including Bring Your Own Device (BYOD), shall be first scanned for vulnerabilities, considering the categories based on the Common Vulnerability Scoring System CVSS 3.0 assessment model. The SPHINX Platform shall also consider the compliance with the ISO/IEC 27001 standard and the NIST 800-X family standard and future amendments. The SPHINX Platform shall report the results of the cybersecurity vulnerability assessments performed on the network's devices.	
Categorisation	per IT Domain	per Function of the CSMC
	IT Hardware Infrastructure; Networking.	Identify; Protect; Detect.

SPHINX shall provide vulnerability assessment checklists to users.		
Requirement ID	STA-F-130	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	4	
Description and Rationale	The SPHINX Platform shall provide vulnerability assessment checklists for the users, allowing them to employ effective tools for evaluating the state of readiness and the potential exposures and vulnerabilities of the IT ecosystem. It shall have reminders, alerts associated with levels of security. It should be possible to report the recommended actions for correcting or mitigating the vulnerabilities in question, and not only report the vulnerability itself, it's impact and scope.	



SPHINX shall provide vulnerability assessment checklists to users.		
Categorisation	per IT Domain	per Function of the CSMC
	IT Hardware Infrastructure; Networking; Applications.	Protect.

SPHINX shall deliver a cyber risk assessment report.		
Requirement ID	STA-F-140	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall deliver a cyber risk assessment report that allows for the healthcare organisation to understand, manage, control and mitigate cyber risks across the IT ecosystem. The cyber risk assessment shall identify and prioritise assets, identify threats and vulnerabilities, analyse controls and propose new controls, calculate the likelihood and impact of different security scenarios and prioritise cyber risks based on the cost of prevention versus the assets' value. The cyber risk evaluation shall also include actionable recommendations to improve security (reduce risk, minimise breach impact and protect against future cyber-attacks), using best practices.	
Categorisation	per IT Domain	per Function of the CSMC
	IT Hardware Infrastructure; Networking; Applications; Security/Privacy.	Identify.

SPHINX shall provide an automated zero touch device and service verification toolkit.		
Requirement ID	STA-F-150	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall provide an automated zero-touch verification toolkit that will perform vulnerability and cyber risk assessment of devices and services entering or connected to the network. The verification toolkit shall generate detailed reports of possible misuse or vulnerabilities identified. The verification process will require little or no operator intervention. The user will be notified in case issues and risks are detected. Detail reports shall be easily generated in a machine-readable format (json, csv).	
Categorisation	per IT Domain	per Function of the CSMC
	IT Hardware Infrastructure; Networking; Applications.	Detect.



The SPHINX device and service verification toolkit shall be easily integrated to existing healthcare IT infrastructures.		
Requirement ID	STA-F-160	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	4	
Description and Rationale	The SPHINX Platform shall allow the easy integration of the automated zero touch device and service verification toolkit within the existing healthcare IT infrastructure. This integration enables the implementation of a device and service verification toolkit that respects service continuity with no impact during device/service creation, modification and removal, automating the network's configuration changes as pre-defined by the user. In other words, it should be possible to deploy the sandboxing and certification tools on the existing resources without them creating additional risks or threats when running validations of untrusted code or devices.	
Categorisation	per IT Domain	per Function of the CSMC
	IT Hardware Infrastructure; Networking; Applications.	Detect.

SPHINX shall enable the certification of devices (to be) connected to the organisation's IT ecosystem.		
Requirement ID	STA-F-170	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall perform the certification of the medical and IoT-based devices in the network as <i>safe</i> , meaning that they do not present any vulnerability to the overall IT ecosystem. The SPHINX Platform shall first verify newly added devices and certify them as safe in order for them to be allowed to connect to the network. Whenever a device is assessed as not being safe, the SPHINX Platform shall propose the actions to be taken in order to eliminate all existing device vulnerabilities.	
Categorisation	per IT Domain	per Function of the CSMC
	IT Hardware Infrastructure.	Identify; Protect.

SPHINX shall provide an automated certification service.		
Requirement ID	STA-F-180	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	



SPHINX shall provide an automated certification service.		
Description and Rationale	The SPHINX Platform shall deliver an automated certification service to devices and services, assessing their cybersecurity and protection status and contributing to facilitate the user's cyber security monitoring responsibilities. The SPHINX automated certification service shall also be available to third-parties' devices and services, allowing to ascertain their readiness to become connected to the organisation's IT ecosystem (certification as <i>safe</i>).	
Categorisation	per IT Domain	per Function of the CSMC
	IT Hardware Infrastructure; Applications.	Identify; Protect.

SPHINX shall detect anomalous behaviour in the organisation's IT ecosystem, based on its discovered behavioural patterns.		
Requirement ID	STA-F-190	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall discover patterns in the data produced by the healthcare organisation's IT ecosystem and capture its normal behaviour (e.g., wait time, number of queries, DICOM characterised traffic). Being aware of the system's normal behaviour, SPHINX shall be capable of not only reducing the amount of time users spent on routine cyber security tasks, but also, more importantly, of identifying suspicious (potentially malicious) behaviour to be considered in cyber risk assessment reports, learning from it to prevent similar attacks and to apply resources more strategically. The SPHINX Platform shall enable the early detection of anomalies (anomalous and malicious behaviour) in the IT ecosystem, promoting network probes, traffic inspection and user profiling techniques. Overall, these capabilities support the users' decision-making with respect to the prevention of cyber threats and the response to active cyber-attacks.	
Categorisation	per IT Domain	per Function of the CSMC
	IT Hardware Infrastructure; Networking; Applications.	Protect; Detect; Respond.

SPHINX shall detect and alert users in case of abnormal network traffic.		
Requirement ID	STA-F-200	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall detect the presence of abnormal (likely non-legitimate) network traffic that exhibit patterns indicating a breach or malicious software. Suspicious and abnormal patterns may consist in irregular traffic flows, large amounts	



	of transmitted data, connections to malicious IPs and unauthorised access attempts to devices. Overall, these capabilities support the users' decision-making with respect to the prevention of cyber threats and the mitigation of cyber-attacks, including DDoS attacks and botnets.	
Categorisation	per IT Domain	per Function of the CSMC
	Networking; Applications.	Detect; Respond.

SPHINX shall provide a fully adaptable (near real-time) automated intrusion detection and data filtering algorithms on the individual user profile characteristics.		
Requirement ID	STA-F-210	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall enable the profiling of user behaviour, considering the common characteristics and patterns. Based on registered user profiles, SPHINX shall be capable of flagging and classifying in near real-time generated abnormal traffic and cyber attack patterns, in order to early detect suspicious user behaviour and perform automated intrusion detection. Overall, these capabilities support the users' decision-making with respect to the prevention of cyber threats and the mitigation of cyber-attacks.	
Categorisation	per IT Domain	per Function of the CSMC
	Networking; Applications.	Detect.

SPHINX shall provide an advanced data analysis engine.		
Requirement ID	STA-F-220	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall provide an advanced analytic engine that is capable of visually presenting intuitive data on the IT ecosystem's network and users' behaviour. Descriptive statistics and graphs (pie, bar and scatter plots) allow the IT operator to rapidly acknowledge detected suspicious network and user behaviour and take appropriate mitigation measures. Overall, this capability supports the users' monitoring tasks and decision-making with respect to the prevention of cyber threats and the mitigation of cyber-attacks. Detail reports shall be easily generated in a machine-readable format (json, csv).	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Protect; Detect.



SPHINX shall enable the analysis of successful and unsuccessful cyber-attacks.		
Requirement ID	STA-F-230	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall deliver the capability to analyse successful and unsuccessful cyber-attacks, including access attacks (software, biometric access), network attacks (firewall, routers, switches) and device attacks, based on the information provided by the IT ecosystem. Overall, this capability supports the users' decision-making with respect to the prevention of cyber threats and the mitigation of cyber-attacks. Detail reports shall be easily generated in a machine-readable format (json, csv). The system should provide a central place where all the events from an incident are stored together and can be viewed by the security analysts.	
Categorisation	per IT Domain	per Function of the CSMC
	IT Hardware Infrastructure; Networking; Applications.	Protect; Detect.

SPHINX shall be able to recognise the typology of known cyber-attacks.		
Requirement ID	STA-F-240	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall have the capability to identify and recognise the typology of known (already documented) cyber-attacks, with known effects, outcomes and consequences. The SPHINX Platform shall identify cyber-attacks' paths and patterns and establish reliable and valid chains of evidence that support the appropriate system response. Overall, this capability supports the users' decision-making with respect to reacting to known cyber-attacks. This knowledge base should be updatable with common security information exchange formats, such as STIX.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Detect; Respond.

SPHINX shall enable the categorisation of cyber events and potential cyber-attacks.		
Requirement ID	STA-F-250	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall have the capability to categorise cyber events and potential cyber-attacks, based on the significance of those potential cyber incidents, following specific user behaviour (determined by the user's role and duties concerning the	



	operation of the IT ecosystem). Overall, this capability supports the users' decision-making with respect to the prevention of cyber threats and the mitigation of cyber-attacks. This knowledge base should be updatable with common security information exchange formats, such as STIX.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Identify. Detect.

SPHINX shall provide patterns of cyber security incidents.		
Requirement ID	STA-F-260	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall have the capability to acknowledge, recognise, identify and analyse the patterns of cyber security incidents (attempted and successful cyber-attacks). The SPHINX Platform shall have the capability to gather information from external data sources regarding attack patterns and the related components that could be affected by them. All these patterns shall be efficiently visualised and presented to the users and prompt the user to take actions. Overall, these capabilities support the users' decision-making with respect to the prevention of cyber threats and the mitigation of cyber-attacks.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Detect; Respond.

SPHINX shall generate forecasts of cyber security incidents and their associated consequences.		
Requirement ID	STA-F-270	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall have the capability to generate forecasts (near future timeframe) of cyber security incidents and consider their potential impact to the IT ecosystem. Overall, these capabilities contribute to the SPHINX forecasted cyber risk analyses and assessments and support the users' cyber security awareness and decision-making with respect to the prevention of cyber threats.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Identify.



SPHINX shall implement forensic mechanisms to investigate cyber incidents.		
Requirement ID	STA-F-280	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall have the capability to implement forensic analysis mechanisms to investigate cyber incidents and associated compromised or affected assets, thus producing a meaningful, reliable and valid chain of evidence that support appropriate system responses. Overall, this capability supports the users' cyber security awareness and decision-making with respect to the prevention of cyber threats and the mitigation of cyber-attacks.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Detect; Respond.

SPHINX shall facilitate the collection of evidence concerning cyber incidents.		
Requirement ID	STA-F-290	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall include specialised auditing and logging mechanisms that facilitate the collection of evidence concerning cyber incidents, in order to support the forensic investigation of suspected or confirmed data breaches. Overall, this capability supports the users' cyber security awareness and decision-making with respect to the prevention of cyber threats and the mitigation of cyber-attacks.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Protect.

SPHINX shall collect log entries of security incidents and threats in a privacy-aware manner.		
Requirement ID	STA-F-300	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall collect log entries of security incidents and threats to support investigation and analysis of incident-related information and data from different patterns and contexts in a privacy-aware manner. Overall, this capability supports the users' cyber security awareness and decision-making with respect to the prevention of cyber threats and the mitigation of cyber-attacks.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications; Security/Privacy.	Protect.



SPHINX shall deliver enhanced anonymisation and encryption capabilities.		
Requirement ID	STA-F-310	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall provide advanced anonymisation and encryption capabilities, namely through the use of anonymisation techniques and homomorphic encryption, to be applied to personal and sensitive data in full compliance with the General Data Protection Regulation (GDPR). Overall, this capability addresses the users' privacy and security obligations with respect to the operation of the IT ecosystem. When generating security incident reports, sensitive data that is not relevant for detection should be scrubbed before the reports can be shared to 3rd parties. This will require attribute-based encryption and should be processed on well-known common formats such as STIX 2.0.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications; Security/Privacy.	Protect.

SPHINX shall enable search and querying features, including in the encrypted domain.		
Requirement ID	STA-F-320	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall allow users to perform searches or queries and obtain an overview of the results, based on the information existing within the IT ecosystem. The available search and query features also consider the system's encrypted domain, maintaining high-level security of the personal and sensitive data in a privacy-aware environment. This should enable sharing of encrypted data across multiple entities and allow for operations to be executed on that data and producing results without requiring the original data to be decrypted, effectively using homomorphic encryption techniques.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications; Security/Privacy.	Protect.

SPHINX shall deliver a secure threat registry.		
Requirement ID	STA-F-330	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	





SPHINX shall deliver a secure threat registry.		
Description and Rationale	The SPHINX Platform shall provide a threat registry that, acting as a chain of evidence, allows connected organisations using SPHINX to synchronise their registries and be timely informed or notified of registered cyber threats and attacks, including new cyber incidents. This knowledge base should enforce authentication and authorization features including role-based access.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications; Security/Privacy.	Protect.

SPHINX shall enable a secure sharing of SPHINX cyber threat and attack information among SPHINX users.		
Requirement ID	STA-F-340	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall allow the secure sharing of cyber threat and attack information among SPHINX users, delivering an unalterable and synchronised mechanisms for users to be up to date on new cyber threats and attacks. Overall, this capability supports the users' cyber security awareness and decision-making with respect to the prevention of cyber threats and the mitigation of cyber-attacks. Should ensure integrity has strong guarantees.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications; Security/Privacy.	Protect.

SPHINX shall deploy services and systems emulating those existing in IT infrastructure.		
Requirement ID	STA-F-350	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall integrate the capability to emulate services and systems within the IT ecosystem that are considered probable targets for cyber-attacks. This capability is relevant to lure attackers to fake systems and prevent them from attacking the real ones. These honeypots or honeynets should simulate low level interaction and collect relevant attack intelligence. Of the utmost importance these fakes should not compromise the overall security of the existing infrastructure.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Protect.



SPHINX emulated services and systems shall detect attempted cyber-attacks and notify the users.		
Requirement ID	STA-F-360	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall integrate the capability to detect cyber attack attempts on the emulated services and systems and promptly notify IT administrators (actionable alerts) so that proper courses of action may be considered at the real IT ecosystem level. Overall, this capability supports the users' cyber security awareness and decision-making with respect to the prevention of cyber threats and the mitigation of cyber-attacks.	
Categorisation	per IT Domain	per Function of the CSMC
	IT Hardware Infrastructure; Networking; Applications; Security/Privacy.	Protect; Detect.

SPHINX emulated services and systems shall operate in an isolated and safe environment.		
Requirement ID	STA-F-370	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall enable the emulated IT ecosystem services and systems to be isolated from the real IT environment, protecting the latter from being affected by malicious actions or software. The emulated IT ecosystem shall implement security mechanisms for access control. Security checks should be available to detect malicious devices or services deployed on this environment.	
Categorisation	per IT Domain	per Function of the CSMC
	IT Hardware Infrastructure; Networking; Applications; Security/Privacy.	Protect; Detect.

SPHINX shall deliver automated alerts including recommendations and response plans related with the systems under attack.		
Requirement ID	STA-F-380	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall automatically alert users whenever a system is under attack. The alert shall include recommendations and treatment plans to support the IT's	



	decision-making process. These alerts should be weighed against past alerts, and not repeat multiple times for the same attack.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Detect; Respond.

SPHINX shall implement an early warning system with different warning levels.		
Requirement ID	STA-F-460	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall implement an early warning system to notify and alert users of suspicious user or network activity, massive data processing and unusual access patterns. The SPHINX Platform shall establish different warning levels to enable users to easily identify situations referring to vulnerabilities, risks, threats, events, incidents or attacks, as well as to clearly classify the situations worth monitoring or requiring urgent intervention. The notification shall be as clear as possible, also defining the risk level corresponding to the specific incident (e.g. different notifications shall apply in case of a data breach compared to data tampering). Overall, this capability supports the users' cyber security awareness and decision-making with respect to the prevention of cyber threats and the mitigation of cyber-attacks.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Identify; Protect; Detect.

SPHINX shall include contact information of individuals to be alerted in case of cyber security incidents.		
Requirement ID	STA-F-470	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall include a list of individuals to be alerted in case of forecasted, suspected or ongoing cyber security incidents. Alerting mechanisms should include dashboard displays, emails and text messages to ensure appropriate recipients are informed at all times. The alerts shall consider rules such as incident classification and severity type. The SPHINX Platform shall provide this functionality in compliance with the guidelines of the GDPR. Therefore, the list of individuals shall be kept secure. Overall, this capability supports the users' cyber security awareness and decision-making with respect to the prevention of cyber threats and the mitigation of cyber-attacks.	



SPHINX shall include contact information of individuals to be alerted in case of cyber security incidents.		
Categorisation	per IT Domain	per Function of the CSMC
	Applications; Security/Privacy.	Identify; Detect; Respond.

SPHINX shall provide actionable alerts.		
Requirement ID	STA-F-500	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	<p>The SPHINX Platform shall produce high priority action notifications, summarising the reason for the alert and, if applicable, indicating appropriate response measures. These high-level notifications should only be sent when an end-user can effectively activate a countermeasure, that stops or mitigates an ongoing attack.</p> <p>Overall, this capability supports the users' decision-making with respect to the response and mitigation of cyber-attacks.</p>	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Respond; Recover.

SPHINX shall provide specific means for establishing the authenticity of alerts.		
Requirement ID	STA-F-510	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	<p>The SPHINX Platform shall establish sound mechanisms to determine the authenticity of the automated alerts or notifications issued by the system to warn the organisation's IT administrators of imminent, ongoing and forecasted cyber threats, incidents and attacks requiring prompt intervention. As a global rule, alerts should have a traceability id, that can be verified through cryptographic hashes or MACs.</p>	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Protect.

SPHINX shall allow the classification of automated alerts.		
Requirement ID	STA-F-520	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	<p>The SPHINX Platform shall enable the classification of the automated alerts or notifications issued of imminent, ongoing and forecasted cyber threats, incidents and</p>	



	attacks. The classification scheme shall allow the easy identification of vulnerabilities, risks, threats, events, incidents or attacks, as well as of situations worth monitoring or requiring urgent intervention. The SPHINX Platform shall allow users to filter the registered alerts by category.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Protect.

SPHINX shall provide configurable dashboard views per user.		
Requirement ID	STA-F-530	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall enable users to establish the parameters of their own dashboard views, based on their role and duties concerning the operation of the IT ecosystem. Overall, this capability supports the users' cyber security awareness, monitoring activities and decision-making with respect to the prevention of cyber threats and the mitigation of cyber-attacks.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Not applicable.

SPHINX shall deliver query features.		
Requirement ID	STA-F-560	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	3	
Description and Rationale	The SPHINX Platform shall allow users to query the system concerning its prevailing risk status and incident reports to facilitate prompt intervention, whenever required, and to support incident notification obligations.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Identify; Detect.

SPHINX shall allow for predefined data retention periods		
Requirement ID	STA-F-561	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform when operating will deal with large volumes of data, this data is only useful for a given period. Following the least privilege principles and applying them to data, SPHINX should allow for data retention to be defined for user sensitive	



	information. Might that be, events, network captures, incident data or other sources of critical data.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Protect

SPHINX shall provide a sandboxed environment to deploy and test devices, software and services.		
Requirement ID	STA-F-570	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	4	
Description and Rationale	The SPHINX Platform shall provide a safe and isolated sandboxed environment that is isolated from the IT infrastructure and its main services, therefore enabling the users to test devices, software and services in a valid environment, without disrupting or affecting the normal operations in the IT ecosystem.	
Categorisation	per IT Domain	per Function of the CSMC
	Networking; Applications; Security/Privacy.	Identify.

SPHINX shall provide third-party access to SPHINX functionalities.		
Requirement ID	STA-F-580	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	53	
Description and Rationale	The SPHINX Platform shall provide the opportunity for third-parties to access the SPHINX cyber security services and to extend their own products, solutions and services by incorporating SPHINX features. This should work through dynamically orchestrating the different tools inside SPHINX. A stable user API shall be delivered to ensure backward compatibility for updates.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Not applicable.

SPHINX shall require the authentication of third-parties accessing the SPHINX functionalities.		
Requirement ID	STA-F-590	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	4	
Description and Rationale	The SPHINX Platform shall enable the protection of a third-party's access to the SPHINX functionalities by means of authentication, that in turn ensure privacy and confidentiality of information and of the certification results. The process to generate	



	authentication credentials to third parties shall be efficient and, preferably, automated. The credentials might be revoked by either the third-party or the SPHINX system. Auditing records for the authentication and authorization shall be kept for a pre-defined retention period and shall be consumable inside the SPHINX system.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications; Security/Privacy.	Not applicable.

SPHINX shall allow third-parties to discover and retrieve the available SPHINX functionalities.		
Requirement ID	STA-F-600	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	3	
Description and Rationale	The SPHINX Platform shall enable third-parties to discover and access the different SPHINX data protection and information cyber security services that are available to them. A discovery system should provide the list of services as well as a description of the common features, versions and added value they provide.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications; Security/Privacy.	Not applicable.

SPHINX shall allow third-parties to request a cyber certification of their IT components.		
Requirement ID	STA-F-610	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	3	
Description and Rationale	The SPHINX Platform shall enable third-parties to submit information concerning their IT components (e.g., medical devices, software components, services) in order to receive their cyber certification by SPHINX. The information submitted shall be the minimum necessary to enable the SPHINX system to perform the cyber certification process.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications; Security/Privacy.	Identify.

SPHINX shall allow third-parties to receive a certification report of their IT components.		
Requirement ID	STA-F-620	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	3	



SPHINX shall allow third-parties to receive a certification report of their IT components.		
Description and Rationale	The SPHINX Platform shall perform the certification process of a third-party's IT component upon receiving a cyber certification request by the third-party. The certification report shall declare either the full compliance of the IT component to SPHINX cyber security standards or the list of detected issues/vulnerabilities that deem the third-party IT component unsafe and the proposed alterations required to be implement in the third-party IT component for it to become fully compliant to SPHINX cybersecurity standards.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications; Security/Privacy.	Identify.

SPHINX shall provide customised cyber security reports.		
Requirement ID	STA-F-700	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	<p>The SPHINX Platform shall provide customised cyber security report containing:</p> <ul style="list-style-type: none"> comprehensive visual analytics (e.g., charts, tabular information, statistics); statistical information on registered cyber security events and incidents in the IT ecosystem, including successful and unsuccessful hacking attempts and type of attack: spam, email trap, malware, phishing, database injection, anomalous user and network behaviours; time and duration of successful cyber-attacks to the IT ecosystem along with list of the affected assets; identification and location of the organisation affected by the cyber attack. <p>Overall, this capability supports the users' cyber security awareness and decision-making with respect to the prevention of cyber threats and the mitigation of cyber-attacks. In addition, it also assists the organisations with fulfilling their incident notification obligations concerning cybersecurity incidents, particularly data breach events.</p>	
Categorisation	per IT Domain	per Function of the CSMC
	Applications; Security/Privacy.	Identify; Detect; Protect.

2.1.1 User Interface Functional Requirements and Guidelines

The SPHINX System interacts with the user in order to develop cyber awareness concerning risks, vulnerabilities and incidents within the IT network and connected devices. Moreover, it allows the user to perform vulnerability assessment and certification of devices. In this regard, the user interface needs to be designed according to the user's needs and expectations in order to ensure the utility of SPHINX. This subsection presents the user interface requirements for the SPHINX system, with the aim to guide detailed implementation of the applicable SPHINX components.



The SPHINX component aggregating the most relevant information and cyber security status is the Interactive Dashboard (SPHINX Dashboard). From the users' perspective, the Interactive Dashboard is the main *screen* of the SPHINX System. A first mock-up, providing a high-level conceptual view, is illustrated in Figure 2 and described next. Based on the provided mock-up, the Interactive Dashboard will be detailed and implemented as part of WP5 (Analysis and Decision Making) under Task 5.2 - Advanced Visualisation Dashboards.

The Interactive Dashboard is composed by the following main elements:

- A menu bar including at least 3 fields: number of critical alerts; access to visualisation options; access to user customisation area;
- The top part that aggregates the alerts generated by the individual SPHINX tools;
- In the upper right corner, information concerning the user (including name and role);
- In the central part, an area allowing users to visualise data using various graphs, such as time-series, alert statistics;
- In the right part, a list of all the SPHINX tools and services, allowing users to be redirected to the selected tool or service.

The Interactive Dashboard enables the user to customise/configure the interface. In this way, the user can, for example, select which information to display, in which form and where.



Figure 2: Interactive Dashboard Mock-up



The SPHINX Dashboard shall display alerts generated by SPHINX components.		
Requirement ID	STA-F-710	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	<p>All the alerts generated by the individual SPHINX tools should be aggregated and depicted in tabular format as follows:</p> <ul style="list-style-type: none"> • The first column displays the number alert. • The second column displays a brief description of the alert. • The third column shows the timestamp. • The fourth column has the location of the alert. • The fifth column classifies the alert (i.e., CRITICAL, ALERT, ERROR, INFORMATIONAL). • The sixth column displays the SPHINX tool that detected the alert. • The seventh column shows the proposed actions in order to mitigate the problem. • The eighth column presents details about the alert (which can include the affected system, based on the report of the SPHINX tool). • The last column displays the actual status (i.e., OPEN, CLOSED) that can be modified in case it was resolved. <p>The user may sort the alert table by date, alert classification, SPHINX tool and alert status. The table shall support pagination.</p>	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Not applicable.

The SPHINX Dashboard shall present spatiotemporal information about each generated alert.		
Requirement ID	STA-F-720	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	<p>The SPHINX Dashboard shall include spatiotemporal information about each generated alert, such as the date and time and the location (i.e., the location of the targeted hospital).</p>	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Not applicable.

The SPHINX Dashboard shall display a menu bar with alert information and access to specific functions.		
Requirement ID	STA-F-730	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	



Description and Rationale	The SPHINX Dashboard menu bar shall include at least 3 fields: the first field shall display the number of critical alerts; the second field shall provide an option menu allowing the user to visualise various graphs on alert statistics in a separate webpage and to export the alert table in csv or excel files; the third field refers to the dashboard's settings, which enable the user to easily customise/configure the area below the alerts table. This area may display different graphs associated to the operations of specific SPHINX tools or services. Other fields that the menu bar should include could be: a field for selecting the display language, a field for searching and querying features and a button to display the list of individuals to contact in case of a cyber security event or incident.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Not applicable.

The SPHINX Dashboard shall allow the selection of different statuses for each alert.		
Requirement ID	STA-F-740	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Dashboard shall allow the user to select a status for each alert (i.e. Closed, Open, Ignore, Acknowledge and Empty Field), depending on the action that he wants to take for that specific alert.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Not applicable.

The SPHINX Dashboard shall display the proposed action for each alert.		
Requirement ID	STA-F-750	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall suggest actions that can be taken in order to mitigate common-incidents. These suggestions shall be displayed in the SPHINX Dashboard. Suggestions should be continuously improved by either ingesting data from the knowledge base regularly or by accepting user provided suggestion based on the lessons learned from previous incidents.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Not applicable.



The SPHINX Dashboard shall allow the creation user accounts with different roles.		
Requirement ID	STA-F-760	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	Via the SPHINX dashboard, the SPHINX administrator shall be able to create users and assign roles (e.g. administrator, operator, and observer) in SPHINX. SPHINX users shall be able to login, logout, setup profile (e.g., name), email and change the password, customize own dashboard items.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Not applicable.

The SPHINX Dashboard shall allow the selection of different tools and services.		
Requirement ID	STA-F-770	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	4	
Description and Rationale	The SPHINX Dashboard shall display a list of all the SPHINX tools and services, including a short description of the tool or service (with an overlay window). The user may choose an item by clicking on it and be redirected to the selected tool or service, without having to login again. In other words, SPHINX shall provide an SSO service that provided the authentication mechanisms for all internal tools.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Not applicable.

The SPHINX Dashboard shall present data in visual and rich forms.		
Requirement ID	STA-F-780	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Dashboard shall allow the user to visualise data using various graphs, such as time-series, alert statistics. The used visualisation mechanisms should enable the user to intuitively and efficiently understand the data, as well as customization of the visualization types and series.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Not applicable.



The SPHINX Dashboard shall allow the user to export data into different file formats.		
Requirement ID	STA-F-790	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Dashboard shall allow the user to export the data into different file formats, such as Comma-Separated Values (CSV), JavaScript Object Notation (JSON) and excel files.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Not applicable.

The SPHINX Dashboard shall allow the user to customise the interface according to their needs.		
Requirement ID	STA-F-800	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Dashboard shall contain a list of dashboard settings which enable the user to customise/configure the interface, by having a designated area which the user can modify. This area may display different graphs associated to the operations of specific SPHINX tools or services.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Not applicable.

The SPHINX Dashboard shall provide searching and querying features.		
Requirement ID	STA-F-810	
Requirement Type	Functional Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Dashboard shall contain a search bar which enables the user to easily search for different elements.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Not applicable.

In addition to functional requirements and guidelines, end-users also identified for the SPHINX System a set of quality constraints that the system must satisfy with respect to user interface, performance, operation and lifecycle. Overall, the quality factors are translated into non-functional requirements and guidelines that relate to usability, maintainability, security and legal and ethical aspects, specific to the functionality of the system and to the context within which the system will operate. For the SPHINX System, relevant non-functional requirements and guidelines are presented next.



2.2 Usability Requirements and Guidelines

The usability requirements and guidelines elicited by the end-users are specifications designed to ensure that the SPHINX System is easy to use. Specifically, usability refers to the ease of learning, the efficiency in performing tasks, the ease of remembering, understandability and user satisfaction [4]. The following usability requirements and guidelines were identified for the SPHINX System.

SPHINX shall be designed and implemented with a clear focus on usability.		
Requirement ID	STA-U-010	
Requirement Type	Usability Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall be designed and implemented to be as simple as possible and to facilitate its use or operation by IT administrators. IT personnel with special needs shall be considered and user interfaces should be intuitive and easy to navigate, easy to learn and be remembered and understood, preventing human errors, minimising cognitive load and facilitating the execution of tasks and operations.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Not applicable.

SPHINX shall provide interactive dashboards.		
Requirement ID	STA-U-020	
Requirement Type	Usability Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall allow users to visually observe and to intuitively compose and customise their own operational processes directly on the user interface. A set of interactive dashboards shall consider each user's role and duties regarding the operation of the system and deliver the comprehensive view of data and information as required by the user to perform the assigned tasks efficiently. The SPHINX Platform shall allow users to visually observe and to intuitively compose and customise their own operational processes directly on the user interface. A set of interactive dashboards shall consider each user's role and duties regarding the operation of the system and deliver the comprehensive view of data and information as required by the user to perform the assigned tasks efficiently.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Not applicable.

SPHINX shall deliver a web-based dashboard aggregating information from SPHINX tools.		
Requirement ID	STA-U-030	
Requirement Type	Usability Specifications	
Use Cases	-	





Customer Value	5	
Description and Rationale	The SPHINX Platform shall deliver a set of web-based dashboards to present summaries of the relevant data and information associated to each of the SPHINX cyber security tools and services. The main SPHINX dashboard shall aggregate the relevant data and information of all SPHINX tools and services.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications; Security/Privacy.	Not applicable.

SPHINX shall allow users to visualise the cyber security status related with the organisation's IT assets from a single location.		
Requirement ID	STA-U-040	
Requirement Type	Usability Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	SPHINX provides an overview of the cyber security status of an IT organisation. User shall be able to conveniently access this function from a single location (e.g., user workstation), provided it is authorised and complies with the SPHINX specifications.	
Categorisation	per IT Domain	per Function of the CSMC
	IT Hardware Infrastructure; Applications.	Not applicable.

2.3 Maintainability and Support Requirements and Guidelines

Dealing with system sustainability, maintainability and support requirements address the users' concern for the ease of up-keeping and repairing the system, aiming to perform preventive, corrective, adaptive and perfective maintenance while the number of system or service failures are close to zero. The following maintainability and support requirements and guidelines were identified for the SPHINX System.

SPHINX shall be a modular, scalable and interoperable cyber security platform.		
Requirement ID	STA-M-010	
Requirement Type	Maintainability and Support Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall be designed to be modular (capable of being flexible to address a panoply of threats and incidents), scalable (capable of coping with a potentially high number of inputs and interaction) and interoperable (capable of supporting the interaction of components to augment overall efficiency and effectiveness).	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Not applicable.



SPHINX shall be easily upgraded and maintained.		
Requirement ID	STA-M-020	
Requirement Type	Maintainability and Support Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	When any upgrades, bug and security fixes for the SPHINX Platform become available, the relevant IT staff should be notified and enabled to install it. An important part of cyber security programs is the timely application of upgrades and fixes. It is therefore important to notify the relevant IT personnel of those upgrades and offer them a way to automatically or manually install them.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Not applicable.

The installation and operation of the SPHINX Platform shall be as transparent as possible to the existing IT network infrastructure.		
Requirement ID	STA-M-030	
Requirement Type	Maintainability and Support Requirements	
Use Cases	-	
Customer Value	4	
Description and Rationale	The installation and operation of the SPHINX Platform should not lead to significant changes in the configuration of the IT infrastructure (e.g. changes in the routing between networks, changes in Internet Protocol or IP address space) so that normal operations are not disrupted.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Not applicable.

IT personnel should be notified of any upgrades to the SPHINX Platform and be able to install it.		
Requirement ID	STA-M-040	
Requirement Type	Maintainability and Support Requirements	
Use Cases	-	
Customer Value	0	
Description and Rationale	When any upgrades, bug and security fixes for the SPHINX Platform become available, the relevant IT staff should be notified and enabled to install it, either through manual or automated ways.	
Categorisation	per IT Domain	per Function of the CSMC
	Applications.	Not applicable.



2.4 Security Requirements and Guidelines

Security requirements refer to the features required by system's users to increase the users' trust in the system they operate, based on the fulfilment of confidentiality (only authorised users or applications are allowed to interact with the system), integrity (critical data cannot be changed in an improper way in the system), availability (system information and/or services are readily available to authorised users on demand) and accountability (once authorised users access the system, they are accountable for all of their actions) goals. The following security requirements and guidelines were identified for the SPHINX System.

SPHINX shall implement information security mechanisms.		
Requirement ID	STA-S-010	
Requirement Type	Security Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall implement information security mechanisms that uphold the confidentiality, integrity and availability of information, as well as the users' accountability and the ongoing resilience of processing services. It shall register audit records for the actions taken by the users and safekeep from tampering.	
Categorisation	per IT Domain	per Function of the CSMC
	Security/Privacy.	Not applicable.

SPHINX shall ensure that only authorised and authenticated users may access the system.		
Requirement ID	STA-S-020	
Requirement Type	Security Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall implement Authentication and Authorisation Access Control (AAAC) mechanisms to ensure that only authorised and authenticated users are capable of accessing the organisation's SPHINX System.	
Categorisation	per IT Domain	per Function of the CSMC
	Security/Privacy.	Not applicable.

SPHINX shall enforce secure management and storage of user credentials.		
Requirement ID	STA-S-030	
Requirement Type	Security Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall enforce proper security mechanisms for managing (add, edit, modify, delete) and storing user information, namely login credentials, providing role-based AAAC mechanisms.	



Categorisation	per IT Domain	per Function of the CSMC
	Security/Privacy.	Not applicable.

SPHINX shall enable authorised and authenticated access to sensitive information produced by the system.		
Requirement ID	STA-S-040	
Requirement Type	Security Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall enable authorised and authenticated users to access produced sensitive data within the system, in accordance to the GDPR guidelines.	
Categorisation	per IT Domain	per Function of the CSMC
	Security/Privacy.	Not applicable.

SPHINX shall allow third-parties accessing the SPHINX functionalities to remove own personal and registration information from the system.		
Requirement ID	STA-S-050	
Requirement Type	Security Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall allow a third-party to delete its SPHINX account, including, if applicable, personal information and any other information associated with its registration process in the SPHINX System, in accordance to the GDPR guidelines.	
Categorisation	per IT Domain	per Function of the CSMC
	Security/Privacy.	Not applicable.

SPHINX shall enable sessions management and re-authentication with single sign-on capabilities.		
Requirement ID	STA-S-060	
Requirement Type	Security Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall allow for the management of all user sessions, providing single sign-on capabilities in order to allow users to operate the different SPHINX tools and services once they are authenticated, without having to provide again their credentials.	
Categorisation	per IT Domain	per Function of the CSMC
	Security/Privacy.	Not applicable.



SPHINX should be able to verify the authenticity and integrity of data produced within SPHINX.		
Requirement ID	STA-S-070	
Requirement Type	Security Requirements	
Use Cases	-	
Customer Value	0	
Description and Rationale	SPHINX components produce various data relevant for purposes of cyber security. In order to prevent SPHINX from being compromised, data produced by SPHINX components should be verifiable in what regards their authenticity (validation of source/owner) and integrity (validation is has not been tampered with).	
Categorisation	per IT Domain	per Function of the CSMC
	Security/Privacy.	Not applicable.

SPHINX shall establish and implement security rules to handle cyber-attacks and incidents.		
Requirement ID	STA-S-080	
Requirement Type	Security Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall create security rules from the collected cyber security knowledge and implement them to support the users' decision-making process for addressing cyber security events, incidents and attacks.	
Categorisation	per IT Domain	per Function of the CSMC
	Security/Privacy.	Not applicable.

2.5 Legal and Ethical Requirements and Guidelines

Legal and ethical requirements deal with the users' obligation to enforce specific system features both required by law and/or determined by ethical concerns. The following security requirements and guidelines were identified for the SPHINX System.

SPHINX shall adopt a behavioural and ethical design for its advanced security framework.		
Requirement ID	STA-L-010	
Requirement Type	Legal and Ethical Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall adopt a behavioural and ethical design, compliant with applicable data protection and privacy standards. SPHINX shall be unobtrusive and deliver smart security services involving a wide range of cyber protection technologies.	
Categorisation	per IT Domain	per Function of the CSMC
	Security/Privacy.	Not applicable.





SPHINX shall process data in compliance to applicable European and national legal requirements.		
Requirement ID	STA-L-020	
Requirement Type	Legal and Ethical Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall be designed to consider the nature of the data collected and the applicable legal requirements, both at national and European levels, to ensure legal compliance in terms of data processing.	
Categorisation	per IT Domain	per Function of the CSMC
	Security/Privacy.	Not applicable.

SPHINX shall ensure that all collected sensitive information is encrypted and properly secured to avoid disclosure to unauthorised parties.		
Requirement ID	STA-L-030	
Requirement Type	Legal and Ethical Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall have the capability to ensure that all sensitive data and information in the IT ecosystem is adequately and securely encrypted, processed and stored. The SPHINX Platform shall ensure that only authorised authenticated users are capable of accessing to the sensitive information in the organisation's IT ecosystem.	
Categorisation	per IT Domain	per Function of the CSMC
	Security/Privacy.	Not applicable.

SPHINX shall apply data protection mechanisms.		
Requirement ID	STA-L-040	
Requirement Type	Legal and Ethical Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall include privacy by design and security by design data protection mechanisms to ensure the lawful and transparent processing of data, including sensitive or personal data.	
Categorisation	per IT Domain	per Function of the CSMC
	Security/Privacy.	Not applicable.

SPHINX shall provide a data protection risk assessment.		
Requirement ID	STA-L-050	
Requirement Type	Legal and Ethical Requirements	
Use Cases	-	
Customer Value	5	





Description and Rationale	The SPHINX Platform shall deliver a risk assessment report concerning data protection to be performed throughout the system's lifecycle. This risk assessment shall address the risks related to sensitive and personal data processing and the implementation of the safest solutions to keep these data safe.	
Categorisation	per IT Domain	per Function of the CSMC
	Security/Privacy.	Not applicable.

SPHINX shall provide GDPR compliance self-assessment procedures.		
Requirement ID	AP-L-060	
Requirement Type	Legal and Ethical Requirements	
Use Cases	-	
Customer Value	5	
Description and Rationale	The SPHINX Platform shall include procedures to conduct a self-assessment on GDPR compliance, addressing the principles of <i>lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality</i> . These procedures shall support the users' auditing responsibilities.	
Categorisation	per IT Domain	per Function of the CSMC
	Security/Privacy.	Not applicable.



3 SPHINX Requirements and Guidelines Matrix

ID #	SPHINX Requirements and Guidelines	Categorisation per IT Domain	Categorisation per Function of the CSMC
STA-F-010	SPHINX shall support advanced cyber security capabilities.	IT HW Infrastructure; Networking; Applications.	Protect; Detect; Respond.
STA-F-020	SPHINX shall enable interactions with existing cyber security tools.	Applications.	Detect; Respond.
STA-F-030	SPHINX shall focus on preventing human errors.	Applications; Security/Privacy.	Protect.
STA-F-040	SPHINX shall be designed to support business continuity.	IT HW Infrastructure; Applications; Security/Privacy.	Protect; Respond; Recover.
STA-F-050	SPHINX shall identify new, modern and advanced cyber threats.	IT HW Infrastructure; Networking; Applications.	Identify.
STA-F-060	SPHINX shall interact with existing and well-known cyber threat intelligence repositories.	Applications.	Identify.
STA-F-070	SPHINX shall protect against known cyber-attacks.	Applications.	Protect; Respond.
STA-F-080	SPHINX shall provide a personalised data security management tool.	IT HW Infrastructure; Networking; Applications; Security/Privacy.	Identify; Protect; Detect; Respond; Recover.
STA-F-090	SPHINX shall provide a cyber security inspection, discovery and decision toolset (cyber security toolkit).	Applications.	Identify; Protect; Detect; Respond.
STA-F-100	SPHINX shall be able to handle and process data originated by a large number of devices and services.	IT HW Infrastructure; Networking; Applications.	Protect; Detect.
STA-F-110	SPHINX shall provide cybersecurity vulnerability assessments.	IT HW Infrastructure; Networking; Applications.	Identify; Detect.
STA-F-120	SPHINX shall enable the vulnerability assessment of devices to be connected to the organisation's IT ecosystem.	IT HW Infrastructure; Networking.	Identify; Protect; Detect.
STA-F-130	SPHINX shall provide vulnerability assessment checklists to users.	IT HW Infrastructure; Networking; Applications.	Protect.
STA-F-140	SPHINX shall deliver a cyber risk assessment report.	IT HW Infrastructure; Networking; Applications; Security/Privacy.	Identify.





ID #	SPHINX Requirements and Guidelines	Categorisation per IT Domain	Categorisation per Function of the CSMC
STA-F-150	SPHINX shall provide an automated zero touch device and service verification toolkit.	IT HW Infrastructure; Networking; Applications.	Detect.
STA-F-160	The SPHINX device and service verification toolkit shall be easily integrated to existing healthcare IT infrastructures.	IT HW Infrastructure; Networking; Applications.	Detect.
STA-F-170	SPHINX shall enable the certification of devices (to be) connected to the organisation's IT ecosystem.	IT HW Infrastructure.	Identify; Protect.
STA-F-180	SPHINX shall provide an automated certification service.	IT HW Infrastructure; Applications.	Identify; Protect.
STA-F-190	SPHINX shall detect anomalous behaviour in the organisation's IT ecosystem, based on its discovered behavioural patterns.	IT HW Infrastructure; Networking; Applications.	Protect; Detect; Respond.
STA-F-200	SPHINX shall detect and alert users in case of abnormal network traffic.	Networking; Applications.	Detect; Respond.
STA-F-210	SPHINX shall provide a fully adaptable (near real-time) automated intrusion detection and data filtering algorithms on the individual user profile characteristics.	Networking; Applications.	Detect.
STA-F-220	SPHINX shall provide an advanced data analysis engine.	Applications.	Protect; Detect.
STA-F-230	SPHINX shall enable the analysis of successful and unsuccessful cyber-attacks.	IT HW Infrastructure; Networking; Applications.	Protect; Detect.
STA-F-240	SPHINX shall be able to recognise the typology of known cyber-attacks.	Applications.	Detect; Respond.
STA-F-250	SPHINX shall enable the categorisation of cyber events and potential cyber-attacks.	Applications.	Detect. Identify.
STA-F-260	SPHINX shall provide patterns of cyber security incidents.	Applications.	Detect; Respond.
STA-F-270	SPHINX shall generate forecasts of cyber security incidents and their associated consequences.	Applications.	Identify.
STA-F-280	SPHINX shall implement forensic mechanisms to investigate cyber incidents.	Applications.	Detect; Respond.
STA-F-290	SPHINX shall facilitate the collection of evidence concerning cyber incidents.	Applications.	Protect.
STA-F-300	SPHINX shall collect log entries of security incidents and threats in a privacy-aware manner.	Applications; Security/Privacy.	Protect.
STA-F-310	SPHINX shall deliver enhanced anonymisation and encryption capabilities.	Applications; Security/Privacy.	Protect.
STA-F-320	SPHINX shall enable search and querying features, including in the encrypted domain.	Applications; Security/Privacy.	Protect.
STA-F-330	SPHINX shall deliver a secure threat registry.	Applications; Security/Privacy.	Protect.





ID #	SPHINX Requirements and Guidelines	Categorisation per IT Domain	Categorisation per Function of the CSMC
STA-F-340	SPHINX shall enable a secure sharing of SPHINX cyber threat and attack information among SPHINX users.	Applications; Security/Privacy.	Protect.
STA-F-350	SPHINX shall deploy services and systems emulating those existing in IT infrastructure.	Applications.	Protect.
STA-F-360	SPHINX emulated services and systems shall detect attempted cyber-attacks and notify the users.	IT HW Infrastructure; Networking; Applications; Security/Privacy.	Protect; Detect.
STA-F-370	SPHINX emulated services and systems shall operate in an isolated and safe environment.	IT HW Infrastructure; Networking; Applications; Security/Privacy.	Protect; Detect.
STA-F-380	SPHINX shall deliver automated alerts including recommendations and response plans related with the systems under attack.	Applications.	Detect; Respond.
STA-F-460	SPHINX shall implement an early warning system with different warning levels.	Applications.	Identify; Protect; Detect.
STA-F-470	SPHINX shall include contact information of individuals to be alerted in case of cyber security incidents.	Applications; Security/Privacy.	Identify; Detect; Respond.
STA-F-500	SPHINX shall provide actionable alerts.	Applications.	Respond; Recover.
STA-F-510	SPHINX shall provide specific means for establishing the authenticity of alerts.	Applications.	Protect.
STA-F-520	SPHINX shall allow the classification of automated alerts.	Applications.	Protect.
STA-F-530	SPHINX shall provide dashboard views per user.	Applications.	Not applicable.
STA-F-560	SPHINX shall deliver query features.	Applications.	Identify; Detect.
STA-F-561	SPHINX shall allow for predefined data retention periods	Applications.	Protect.
STA-F-570	SPHINX shall provide a sandboxed environment to deploy and test devices, software and services.	Networking; Applications; Security/Privacy.	Identify.
STA-F-580	SPHINX shall provide third-party access to SPHINX functionalities.	Applications.	Not applicable.
STA-F-590	SPHINX shall require the authentication of third-parties accessing the SPHINX functionalities.	Applications; Security/Privacy.	Not applicable.
STA-F-600	SPHINX shall allow third-parties to discover and retrieve the available SPHINX functionalities.	Applications; Security/Privacy.	Not applicable.
STA-F-610	SPHINX shall allow third-parties to request a cyber certification of their IT components.	Applications; Security/Privacy.	Identify.





ID #	SPHINX Requirements and Guidelines	Categorisation per IT Domain	Categorisation per Function of the CSMC
STA-F-620	SPHINX shall allow third-parties to receive a certification report of their IT components.	Applications; Security/Privacy.	Identify.
STA-F-700	SPHINX shall provide customised cyber security reports.	Applications; Security/Privacy.	Identify; Detect; Protect.
STA-F-710	The SPHINX Dashboard shall display alerts generated by SPHINX components.	Applications.	Not applicable.
STA-F-720	The SPHINX Dashboard shall present spatiotemporal information about each generated alert.	Applications.	Not applicable.
STA-F-730	The SPHINX Dashboard shall display a menu bar with alert information and access to specific functions.	Applications.	Not applicable.
STA-F-740	The SPHINX Dashboard shall allow the selection of different statuses for each alert.	Applications.	Not applicable.
STA-F-750	The SPHINX Dashboard shall display the proposed action for each alert.	Applications.	Not applicable.
STA-F-760	The SPHINX Dashboard shall allow the creation user accounts with different roles.	Applications.	Not applicable.
STA-F-770	The SPHINX Dashboard shall allow the selection of different tools and services.	Applications.	Not applicable.
STA-F-780	The SPHINX Dashboard shall present data in visual and rich forms.	Applications.	Not applicable.
STA-F-790	The SPHINX Dashboard shall allow the user to export data into different file formats.	Applications.	Not applicable.
STA-F-800	The SPHINX Dashboard shall allow the user to customise the interface according to their needs.	Applications.	Not applicable.
STA-F-810	The SPHINX Dashboard shall provide searching and querying features.	Applications.	Not applicable.
STA-U-010	SPHINX shall be designed and implemented with a clear focus on usability.	Applications.	Not applicable.
STA-U-020	SPHINX shall provide interactive dashboards.	Applications.	Not applicable.
STA-U-030	SPHINX shall deliver a web-based dashboard aggregating information from SPHINX tools.	Applications; Security/Privacy.	Not applicable.
STA-U-040	SPHINX shall allow users to visualise the cyber security status related with the organisation's IT assets from a single location.	IT HW Infrastructure; Applications.	Not applicable.
STA-M-010	SPHINX shall be a modular, scalable and interoperable cyber security platform.	Applications.	Not applicable.





ID #	SPHINX Requirements and Guidelines	Categorisation per IT Domain	Categorisation per Function of the CSMC
STA-M-020	SPHINX shall be easily upgraded and maintained.	Applications.	Not applicable.
STA-M-030	The installation and operation of the SPHINX Platform shall be as transparent as possible to the existing IT network infrastructure.	Applications.	Not applicable.
STA-M-040	IT personnel should be notified of any upgrades to the SPHINX Platform and be able to install it.	Applications.	Not applicable.
STA-S-010	SPHINX shall implement information security mechanisms.	Security/Privacy.	Not applicable.
STA-S-020	SPHINX shall ensure that only authorised and authenticated users may access the system.	Security/Privacy.	Not applicable.
STA-S-030	SPHINX shall enforce secure management and storage of user credentials.	Security/Privacy.	Not applicable.
STA-S-040	SPHINX shall enable authorised and authenticated access to sensitive information produced by the system.	Security/Privacy.	Not applicable.
STA-S-050	SPHINX shall allow third-parties accessing the SPHINX functionalities to remove own personal and registration information from the system.	Security/Privacy.	Not applicable.
STA-S-060	SPHINX shall enable sessions management and re-authentication with single sign-on capabilities.	Security/Privacy.	Not applicable.
STA-S-070	SPHINX should be able to verify the authenticity and integrity of data produced within SPHINX.	Security/Privacy.	Not applicable.
STA-S-080	SPHINX shall establish and implement security rules to handle cyber-attacks and incidents.	Security/Privacy.	Not applicable.
STA-L-010	SPHINX shall adopt a behavioural and ethical design for its advanced security framework.	Security/Privacy.	Not applicable.
STA-L-020	SPHINX shall process data in compliance to applicable European and national legal requirements.	Security/Privacy.	Not applicable.
STA-L-030	SPHINX shall ensure that all collected sensitive information is encrypted and properly secured to avoid disclosure to unauthorised parties.	Security/Privacy.	Not applicable.
STA-L-040	SPHINX shall apply data protection mechanisms.	Security/Privacy.	Not applicable.
STA-L-050	SPHINX shall provide a data protection risk assessment.	Security/Privacy.	Not applicable.
STA-L-060	SPHINX shall provide GDPR compliance self-assessment procedures.	Security/Privacy.	Not applicable.

Table 2: SPHINX Requirements and Guidelines Matrix





4 Conclusion

The SPHINX requirements and guidelines consider the end-users' perspective in the generation of the next generation of cybersecurity tools, to face the specific cybersecurity challenges that mine and will continue mining healthcare organisations worldwide. The methodology for the elicitation of the users' requirements and guidelines has been based on the VOLERE model, adapted to the specifics of the SPHINX Project, and has considered not only the structuring of IT systems but also the teachings of NIST regarding the improvement of critical infrastructures' cybersecurity.

The eighty-five SPHINX requirements and guidelines will be revised and updated as part of *Task 2.3 – Stakeholders' Requirements*, considering the contributions from other relevant project outcomes, such as the SPHINX use cases, architecture and technical specifications, and delivering the final user requirements and guidelines for building the SPHINX System.





5 References

1. Robertson, J., & Robertson, S. (2017). *Volere Requirements Specification Template. Edition 10.1.*
2. National Institute of Standards and Technology (2018). *Framework for Improving Critical Infrastructure Cybersecurity.* Version 1.1. April 16, 2018. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.
3. ISO/IEC/IEEE (2015). 15288:2015 - Systems and software engineering — System life cycle processes. <https://www.iso.org/standard/63711.html>.
4. Lauesen, S. & Younessi, H. (1998). *Six Styles for Usability Requirements.* Proceedings of Fourth International Workshop on Requirements Engineering: Foundation for Software Quality. Presses Universitaires de Namur. June 8-9 1998. .

