
## Deliverable 2.2

# Technical Requirements

| Project ref. no. | H2020-SU-DS-2020 GA No 101019645 |
|---|---|
| **Project title** | SECurity And privacy protectioN in Internet of Things devices |
| **Duration of the project** | 1-09-2021 – 31-08-2024 (36 months) |
| **WP/Task:** | WP2/ T2.2 |
| **Dissemination level:** | PUBLIC |
| **Document due Date:** | 31/05/2022 (M09) |
| **Actual date of delivery** | 20/07/2022 (M11) |
| **Leader of this deliverable** | CLS |
| **Author (s)** | All partners |
| **Other Contributors** | All partners |
| **Version** | V2.0 |

# Document History

| Version | Date | Document history/approvals |
|---|---|---|
| **0.1** | 01/12/2021 | First draft of document structure, work assignments. |
| **0.2** | 28/03/2022 | Contribution to Section 1, 5 [CLS]. |
| **0.3** | 12/04/2022 | Contribution to Section 2.1, 2.2 [All partners]. |
| **0.4** | 27/04/2022 | Contribution to Section 4 [All partners]. |
| **0.5** | 15/05/2022 | Contribution to Section 3 [CLS]. |
| **0.6** | 20/05/2022 | Contribution to Section 2.3 [POLARIS, KI, THALES]. |
| **0.7** | 24/05/2022 | Final version sent for internal review. |
| **0.8** | 30/05/2022 | Version sent for PC review. |
| **0.9** | 30/05/2022 | Version sent for STC. |
| **1.0** | 31/05/2022 | Version ready for submission. |
| **1.1** | 20/06/2022 | Contributions from all partners to address comments made by NTTDES and CERTH |
| **1.2** | 04/07/2022 | Second round of contributions from all partners to address comments made by NTTDES and CERTH |
| **2.0** | 19/07/2022 | Final version ready for submission |

# Table of contents

# List of Figures



# List of Tables

# Abbreviations List

| Abbreviation | Meaning |
|---|---|
| **ABE** | Attribute-Based Encryption |
| **ABPRE** | Attribute-Based PRE |
| **APIs** | Application User Interfaces |
| **BFT** | Byzantine Fault-Tolerant |
| **BLS** | Boneh–Lynn–Shacham |
| **CERTs** | Computer Emergency Readiness Teams |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **CO-CRAE** | Connected Organisations Cyber Risk Assessment Engine |
| **COBIT** | Control Objectives for Information and Related Technologies |
| **CPE** | Common Platform Enumeration |
| **CPRE** | Conditional PRE |
| **CPS** | Cyber-Physical Systems |
| **CRL** | Cumulative Risk Level |
| **CRUD** | Create, Read, Update, and Delete |
| **CSIRTs** | Computer Security Incident Response Teams |
| **CSP** | Cloud Service Provider |
| **CSRAC** | Cyber Security Risk Assessment Companion |
| **CSTM** | Cyber Security Training Module |
| **CTI** | Cyber Threat Intelligence |
| **CVEs** | Common Vulnerabilities and Exposures |
| **CVSS** | Common Vulnerability Scoring System |
| **CybOX** | Cyber Observable eXpression |
| **DDoS** | Distributed Denial-of-Service |
| **DFS** | Depth-First Search |
| **DID** | Decentralized Identifiers |
| **DIM** | Decentralised Digital Identity Management |
| **DoA** | Description of Action |
| **DT** | Decision Trees |
| **FAIR** | Factor Analysis of Information Risk |
| **GDPR** | General Data Protection Regulation |
| **GUI** | Graphical User Interface |
| **HE** | Honey Encryption |

| Abbreviation | Meaning |
|---|---|
| **HVA** | Human Vulnerability Assessment |
| **IB-PRE** | Identity-Based PRE |
| **ICT** | Information and Communication Technologies |
| **IDS** | Intrusion Detection System |
| **IoT** | Internet of Things |
| **IP** | Internet Protocol |
| **IPL** | Interoperability Layer |
| **IPS** | Intrusion Prevention System |
| **IR** | Information Retrieval |
| **IRC** | Internet-Relay-Chat |
| **IRL** | Individual Risk Level |
| **MISP** | Malware Information Sharing Platform |
| **ML** | Machine Learning |
| **NLP** | Natural Language Processing |
| **NVD** | National Vulnerability Database |
| **OCR** | Organizational Cyber Range |
| **OCTAVE** | Operationally Critical Threat, Asset and Vulnerability Evaluation |
| **PBE** | Password-Based Encryption |
| **PEKS** | Public key Encryption with Keyword Search |
| **PRE** | Proxy Re-Encryption |
| **RFM** | Risk Management Framework |
| **SE** | Searchable Encryption |
| **SIEM** | Security Information and Event Management |
| **SSE** | Searchable Symmetric Encryption |
| **SSI** | Self-Sovereign Identity |
| **STIX** | Structured Threat Information eXpression |
| **TAM** | Trust and Accountability Module |
| **TARA** | Threat Assessment and Remediation Analysis |
| **TAXII** | Trusted Automated eXchange of Intelligence Information |
| **TIM** | Threat Intelligence Module |
| **TLS** | Transport Layer Security |
| **TPRE** | Time Based PRE |
| **TTPs** | Tactics, Techniques, and Procedures |
| **TVIA** | Technical Vulnerability and Impact Assessment |

| Abbreviation | Meaning |
|---|---|
| **URL** | Uniform Resource Locator |
| **W3C** | World Wide Web Consortium |

# Executive Summary

This deliverable reports the technical requirements of the SECANT solution. In particular, D2.2 Technical Requirements is eliciting the technical requirements that the SECANT must satisfy from the SECANT end-user/stakeholder requirements reported in *D2.1- End-user/stakeholder requirements* and the SECANT use cases as were defined under *D2.3 - Use cases analysis and application scenarios*. Initially, the context of the SECANT project is defined through a high-level presentation of its main objectives and key technological areas. Next, an initial threat portfolio is established to build the basis for the development of the Threat Intelligence Module. Finally, concepts relating to the elicitation, prioritisation and refinement of functional and non-functional requirements are introduced to further contextualise the work and define the scope of the analysis for the rest of the document.

The requirement elicitation methodology that was followed for the purposes of the activities described in this deliverable included the following:

- the interaction with technology providers via template documents for the description of their technological solutions and unstructured interviews for the refinement of their requirements
- the identification of relevant literature sources regarding the state-of-the-art of each SECANT component
- the process for the analysis, refinement, and categorisation of the elicited requirements

Finally, the document provides a list of up to 150 grouped and prioritised requirements that were identified by the contributors of this deliverable.

# 1. Introduction

## 1.1. Purpose of the Document

The goal of the SECANT project is to enhance the capabilities of an organization's stakeholders by implementing: (a) collaborative threat intelligence collection, analysis and sharing; (b) innovative risk analysis specifically designed for interconnected nodes of an industrial ecosystem; (c) cutting-edge trust and accountability mechanisms for data protection and (d) security awareness training for more informed security choices. SECANT contributes decisively towards improving the readiness and resilience of the organizations against the crippling modern cyber-threats, increasing privacy, data protection and accountability across the entire interconnected ICT ecosystem, and reducing the costs for security training in the European Single Market.

The present document is the result of the studies conducted during the first 9 months of the SECANT project as part of Task 2.2 - Technical requirements specification. Task 2.2 analyses the technical requirements that will drive the design and development of a proof-of-concept threat reporting and incident response system for CERTs/CSIRTs. Accordingly, the main purpose of this report is to provide a set of requirements for the specification of the technical solution of the project, to establish an initial threat portfolio to build the basis for the development of the threat intelligence module and finally, to present an overview of the core technologies and to discuss on how they will be improved beyond that in SECANT project [1].

## 1.2. Document Scope and Intended Audience

The focus of T2.2 and its subsequent output (D2.2) is to define the technical requirements of the SECANT components and platform. To that end, the methodology to gather the functional and non-functional requirements of the SECANT core technological groups is identified. This task involves interaction (interviews, template documents, workshops etc.) with SECANT's technology providers to gather necessary input. For this work, a multidisciplinary team has been established with specialists in Digital Security, Privacy by design, Risk & Vulnerability Assessment, Threat Intelligence & Taxonomies, Personal Data Protection, Trust & Accountability, Blockchain Technology, Security Awareness Training, Cyber Ranges, System Specifications and System Integration, that is responsible for considering the multiple dimensions of the SECANT project through a technical robust distributed architecture oriented towards incorporating the vision of all key stakeholders in a single design.

The output of T2.2, as reported in this deliverable, forms the baseline for the specification of the technical solution that will be offered by SECANT. Therefore, this deliverable provides input for the subsequent deliverables of WP2, especially the ones regarding the SECANT architecture (D2.4 and D2.5). It will also be used as a reference during the development of the individual SECANT components and the development and testing of the SECANT integrated solution within the project's technical and demonstration work packages.

## 1.3. Document Structure

The rest of this document is structured as follows:

- **Section 2** provides an overview of the SECANT project, its core technologies, and their state of the art. It also provides a high-level description of the threat portfolio of the digital landscape upon which SECANT will operate.
- **Section 3** presents the main concepts related to the specification of the functional and non-functional requirements of the technical solution of SECANT while also discusses the process for their elicitation, prioritisation, and refinement.
- **Section 4** presents the technical requirements of the SECANT solution grouped according to the specific group of technologies they apply to.

- **Section 5** concludes this deliverable by summarising its main outcomes and discussing their relevance towards the rest of the SECANT work plan.

# 2. SECANT Overview

## 2.1. SECANT in a Nutshell

SECANT envisages delivering a holistic framework for cyber security risk assessment to enhance digital security, privacy, and personal data protection in complex ICT infrastructures by employing state-of-the-art technologies and methodologies. SECANT rests on four major pillars. These are Digital Security and Privacy, Data Protection and Accountability, Collaborative Threat Intelligence, and Cyber Security Awareness Training.

SECANT introduces a unique architectural structure for best associating modern distributed ledger technologies with novel practices for digital security, privacy, data protection, and accountability to defend the industrial supply chain infrastructure against crippling modern cyber-threats.

## 2.2. SECANT Key Technological Areas

This section provides information about the state-of-the-art in key technical technological areas with the aim to establish their potential for integration at the SECANT platform. As identified in the DoA, these areas are:

1. Cyber threat intelligence collection and sharing
2. Cyber security risk management
3. Cyber security risk vulnerability and impact assessment
4. Social engineering vulnerability assessment
5. Data protection and accountability based on DLT
6. Privacy, data encryption, search and sharing
7. Decentralized digital identities
8. Cyber security training

The aim of the state-of-the-art is to provide guidance to the SECANT system co-design process of the Task 2.4 “Overall system design and functional architecture”.

### 2.2.1. Threat Intelligence Module

#### 2.2.1.1. Cyber Threat Intelligence – Current State of the Art

Over the past years, Cyber Threat Intelligence (CTI) has emerged as a critical component of an organisation’s security. For organisations to prevent, respond or mitigate the cybersecurity threats that affect their assets, they need to be informed about cyber threat trends and defend themselves against a wide range of adversaries. The content of CTI contains information that can help identify, assess, monitor, and respond to cyber-threats [2]. Among the provided information, Indicators and Tactics, Techniques, and Procedures (TTPs). The Cybersecurity and Infrastructure Security Agency (CISA) [3] maintains the ICS-CERT Alert [4] that provides timely notifications concerning critical infrastructure, including alerts affecting medical devices. Furthermore, most manufacturers of medical devices maintain a repository with CTI [3]. Additionally, CTI can be gathered from vulnerability databases including databases with exploits. The most well-known vulnerability databases include MITRE ATT&CK [5], OVAL [6], National Vulnerability Database (NVD) [7], and the Exploit Database [8].

While CTI gathering can be achieved by various approaches (e.g., Python scripts, APIs), web crawlers can be considered as the optimal approach due to the ability to gather CTI data from all web layers, namely Surface, Deep and Dark web. The basic concept regarding the data crawler functionality is that the crawler visits a URL address and downloads the webpage. Subsequently, it extracts the addresses found in the URL compares them with a list of visited URLs and adds the non-visited ones to its frontier list.

According to the literature, crawlers can be categorised based on features such as crawling applications, available hardware, the desired scalability properties, and the ability to scale/ expand the existing infrastructure [7]-[9]. Therefore, crawlers can be categorised as: Centralised, Hybrid, Parallel/Distributed or Peer-to-Peer.

CTI landscape comprises a wide range of sources which can be categorised according to different characteristics (e.g., interoperability semantic standards adopted by the parties, as well as the licensing options) [4]. An important categorisation of CTI sources can be made according to the web layer where the data source is located. Internet comprises three main layers: Surface Web, Deep Web, and Dark Web [5], [6], [10]. Surface web is the web in its simplest form. The content of the Surface Web can be accessed by search engine, and it consists of the web that the internet users use in daily basis. Deep Web is considered a special category of the Surface Web. The content of the Deep Web is not accessible from search engines and is available via other interfaces. Dark Web includes hidden content, intended mainly for illicit purposes and is typically accessible only with the use special software like the Tor browser [9][11].

While most CTI sources provide general information, they might also include information regarding threats that are domain specific (e.g., healthcare). Several Computer Emergency Readiness Teams (CERT) maintain sources that provide timely notification about various infrastructures, including medical devices, while also many manufacturers of medical devices maintain a repository of CTI data relevant to their products.

A significant difficulty emerges in cases where despite that a target website contains data relevant to the topic (e.g., healthcare), it has no actual information that can be leveraged to CTI (i.e., does not mention any related attack or vulnerability). Focused crawlers that leverage advanced language models are introduced as an effective approach to address this issue. Another critical issue that prevents the automated crawling is the use of authentication methods by the websites such as user login or CAPTCHA [5].

Deep Web constitutes the greater part of the internet. Consequently, more information is available in this layer. While this can be considered as an advantage, it poses various challenges such as filtering a significant amount of information to identify information that is relevant to a specific use case.

The terms Deep Web, Darknet and Dark Web are often mistaken for interchangeable. Dark web could be described as intentionally or cryptographically hidden content of the Deep web [10]. Darknet is defined as an overlay [11] network that is built over the regular internet like other overlay networks - peer-to-peer and client-server applications.

According to the authors in [12] there are four major hacker community platforms: (i) forums, (ii) DarkNet Marketplaces, (iii) Internet-Relay-Chat (IRC) channels, (iv) carding shops. Carding is defined as a fraud concerning the trafficking and unauthorised use of credit cards. Carding shops and IRC platforms do not provide the mechanisms for hackers to freely share threats, thus providing little information that can be used to extract CTI. On the other hand, Darknet markets and forums include vast amount of data including technical information of malware. Among other data, forums also provide rich metadata that can be utilised to extract useful CTI data.

Dark web CAPTCHA patterns are intentionally designed to have additional background noise and variable character length to prevent scripts bypass CAPTCHA [13]. An effective solution in automated CAPTCHA breaking is the use Machine Learning (ML) methods. Furthermore, another issue of sources from Dark web is content that is either written in poor English or in other languages.

The content of CTI contains information that can help identify, assess, monitor, and respond to cyber-threats [14]. Among the provided information, Indicators and TTPs. Indicators are defined as observables or technical artifacts which indicate either an ongoing attack or that the system has been already compromised. TTPs are defined as elements which provide an abstract description concerning the behaviour of the attacker.

Apart from the external sources, CTI data can also be retrieved from various sources within an organisation. These sources include both external as well as internal sources to the organisation. Internal sources are defined as sources that are internal to the organisation and include logs generated by servers, logs from databases, security monitoring tools (e.g., IDS, IPS), and various other services which operate within the organisation. Internal sources are especially useful for the collection of intelligence about threats and vulnerabilities that are currently not known to the public (zero-days). The structured representation of CTI according to a common standard is essential to maximise its usability potential. Furthermore, the use of protocols regarding the sharing of CTI is also critical. The most prevalent CTI standard is Structured Threat Information eXpression (STIX) [11]. Other well-known standards and protocols according to the literature are the Trusted Automated eXchange of Intelligence Information (TAXII), Cyber Observable eXpression (CybOX), and C3ISP.

Faced with the numerous architectures, products, and systems being used as sources of data for information sharing systems, there is a need for standardized and structured CTI platforms to allow a satisfying level of interoperability across the various stakeholders. Among the most used CTI sharing platform currently used are the MISP Threat Sharing Platform [12], OpenCTI [13], YETI [2], and CIF [14].

Web crawlers tend to specialise in a specific set of functionalities and thus, users should consider their needs/requirements before choosing to employ a crawler software. Among the popular state-of-the-art crawler solutions in both paid and free-to-use domains are the Dyno mapper [15], Screaming frog SEO spider [16], Deepcrawl [17], Apify [18], Oncrawl [19], Scrapy [20] and Apache Nutch [21].

Social media provide ways to stay informed about security vulnerabilities and availability of patches, providing dedicated channels that can be used to monitor for appearance of new vulnerabilities. These channels are scattered however, making automation of such monitoring rather difficult but not impossible, most notably on open publishing platforms such as Twitter and Telegram.

#### 2.2.1.2. Threat Intelligence Collection, Sharing and Reporting to CERTs/CSIRTs

The Threat Intelligence Module (TIM) will be adjusted to fit the needs of complex ICT infrastructures. The module will support the manual collection of threat intelligence through a user-friendly GUI as well as gathering of threat intelligence from logs and alerts of existing software and hardware security components (i.e., IDS/IPS) through relevant APIs.

SECANT's TIM will gather threat intelligence from different sources by utilising the MISP platform and CTI feeds which are maintained by manufacturers of medical devices and include CTI data relevant to their products. MISP is a threat intelligence platform for sharing, storing, and correlating Indicators of Compromise from targeted assaults, threat intelligence, financial fraud data, vulnerability data, and even counter-terrorism data. The basic MISP installation includes a large number of default feeds which consist of public OSINT feeds. Within the context of the development of TIM, more sources will be added which include valuable data to extract CTI. MISP platform will be modified to support more sources as well as to include more information to provide more insight regarding a cyber-attack.

Furthermore, TIM aims to utilise web crawlers with specific technical requirements such as scalability, transparency, reliability, and high-quality data collection. TIM will implement different crawler types which provide different advantages according to the source and the scope of crawling. Specifically, TIM will implement crawlers which will be able to gather information from all the layers of the Internet (i.e., Surface, Deep and Dark Web). Apart from these sources, TIM will also gather data by crawling and scraping online security-related sources, and feeds of CERTs/ CSIRTs which will be analysed to extract CTI.

#### 2.2.1.3. Dynamic Taxonomies for Cyber-attacks

Over the last year, cyber-attacks have been rapidly increasing in volume and sophistication and have evolved in both complexity and diversity, targeting organisations and individuals. Taxonomies that can assist in constructing novel defending procedures again cyber-attacks. Specifically, taxonomies help building a common language about cyber-attacks and better understanding their specific characteristics by transforming the information about an attack into explicit knowledge [22]. Taxonomies generally express this hierarchy in information inside taxonomies and help classify threats into well-defined categories [22]. In the past, various research efforts have tried to investigate the usage of taxonomies in the cyber-security domain [22], [23]. However, knowledge is a dynamic concept that changes over time [24]. Therefore, there is a need for updating the cyber-attack knowledge encapsulated inside taxonomies.

Among the most advanced and efficient methods of updating a taxonomy is the use of knowledge graphs. This method which is part of the general techniques of Artificial Intelligence (AI), can organise, manage, and utilise massive amounts of information and is applicable to the cyber-security domain [25]. Other general efforts (not explicitly towards cyber-security) include the use of Machine Learning (ML) methods such as Decision Trees (DT) [26] or pattern-based identification methods such as regular expressions [27]. In addition, some other researchers have used clustering methods using semantic proximity measures, set-theoretic methods [28] or Adaptive Term Embedding and hierarchical clustering techniques for automating taxonomy generation from text corpus [29]. Other research efforts are tolerated for the automatic expansion and completion of existing taxonomies using different ML methods [30], [31] or Taxonomy Enrichment with Self-Supervision [32]. In general, ML methods Information Retrieval (IR) [33] and sub-domains of Deep Learning, such as Natural Language Processing (NLP) [34], are at the core of the dynamic taxonomy adaptation techniques.

TIM will enable the taxonomies to be dynamically adjusted whenever new information is inserted into the database. Specifically, TIM will first provide suggestions for predicates and entries of the available taxonomies by trying to correlate that information with data already assigned to specific entries of the taxonomy, based on machine learning techniques (e.g., clustering) as well as on techniques that extract domain specific terms and relationships between the concepts that these terms represent.

Already existing cybersecurity-related taxonomies, such as the built-in taxonomies existing in the MISP platform, will be used as a starting point. The taxonomies will be automatically adjusted using, among others, machine learning-based techniques whenever new threat intelligence information is inserted to the platform.

#### 2.2.1.4. SECANT Interoperability Layer

The objectives of the Interoperability layer (IPL) are to filter heterogenous data from external sources and to ensure the retrieval of data from ICT ecosystems to internal components of SECANT Platform.

SECANT's Interoperability Layer (IPL) will complement TIM -Threat Intelligence Module and CO-CRAE – Risk Assessment, by developing a layer to allow both the integration with legacy security systems of the organizations' stakeholders and the collection of data. The IPL will have a database repository, in which it will store in a pseudonymized format the data collected from the systems, and it will provide access to the database repository through a backend service, exposing a message broker-based connection. The TIM services will interrogate the database using the message broker communication protocol to analyse and process the ICT ecosystem data. The IPL will ensure that data collected is in a common and valid format, not in a raw format. Another role of IPL is to establish communication between the ICT ecosystem and the SECANT high-level services. Also, the IPL must authenticate and authorize the data crossing the layer, integrating the DIM service.

### 2.2.2. Cyber Security Risk Assessment Companion

#### 2.2.2.1. Connected Cyber Risk Assessment

Several techniques have been proposed in the literature to provide solutions to businesses and organizations, so that they can identify and address the risks and vulnerabilities that may pose a threat to the operational security of individual devices, as well as their function and system as a whole. In the context of risk and vulnerability assessment of cyber-physical systems (CPS), a consistent vocabulary of terms is used throughout the relevant technical literature to denote various components and aspects of risk assessment methodologies:

- **Asset**: Any entity, which might be digital, physical, or even human, that provides value to an organization and needs to be protected.
- **Threat**: Any event or circumstance that can negatively impact organizational operations, assets, or individuals, through unauthorized access, destruction, modification or sharing of information.
- **Vulnerability**: A flaw or weakness in an information system that can be triggered or exploited by a threat source, resulting in a security breach or security policy violation.
- **Risk:** The level of impact on organizational operations, given the potential impact of a threat and the likelihood of the threat.
- **Control**: Any mitigation action that is applied to vulnerabilities and threats, to reduce the overall risk.

To quantify risk and to decide on mitigation actions to address threats and vulnerabilities, a risk assessment methodology needs to be applied. As previously mentioned, several risk assessment methodologies are available in the literature and may offer varying results, depending on the requirements of the system where they may be applied. Next, we provide a brief overview of such risk assessment methodologies available in the literature.

The Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) [35] is a framework developed at the Carnegie Mellon University, and it offers a comprehensive evaluation method that aims to identify and manage information security risks, based on a set of principles, attributes and outputs, defined as the OCTAVE criteria. There are also modified versions of the OCTAVE framework, namely OCTAVE-S and OCTAVE Allegro, which offer different functionalities depending on the needs of the target organization. The Threat Assessment and Remediation Analysis (TARA) methodology [36] aims to perform risk assessment methodology early in the development cycle, so that the operational cost to the organization is minimized. Another risk assessment methodology is the Factor Analysis of Information Risk (FAIR) framework, which takes into consideration interdependencies between factors that contribute to risk and can be used as a complementary framework to other methodologies. Another methodology that aims to ensure the quality, control, and reliability of information systems from a business perspective is the Control Objectives for Information and Related Technologies (COBIT) framework [37]. Finally, the NIST Risk Management Framework (RMF) aims to provide a risk assessment operation, that complies with federal laws, Executive orders, and regulations, regardless of the type and size of the organization.

The Connected cyber risk assessment to be developed within the SECANT will perform cybersecurity and information security impact assessment, based on the use of the Common Vulnerability Scoring System (CVSS) [38] to evaluate the severity of threats and vulnerabilities. It should be noted that, in the context of SECANT, the CVE methodology will be enhanced by using the latest version (3.1) of the CVSS score [39]. We will also consider the identification of the vulnerabilities that are defined by an attack path, so that each asset can be considered as an intrusion point.

The cyber risk assessment can assist in both the design-time and runtime risk assessment and can handle the cascading effects that a vulnerability may cause to the entire system, due to the interdependencies between the assets of the considered system. Moreover, cyber risk assessment will be constantly updated with the latest identified common vulnerabilities and exposures (CVEs) by

leveraging information from the US National Vulnerability Database, and it uses the CPE (Common Platform Enumeration) Dictionary naming convention for information technology systems, packages, and software.

The cyber risk assessment will be able to calculate risk levels throughout the entire operational environment of any system, including assets, processes, business elements and other organizational units, and will be used to perform the risk evaluation and calculate the risk graph in the context of the SECANT framework.

Next, we provide some details on the methodology employed by the risk assessment. The Assets are a key factor for a risk assessment methodology, as any risk quantification method is related to their exploitability. As previously mentioned, an asset is defined as any entity that is considered to be of value and needs to be protected. Each asset regardless of its nature or operational role, may entail several vulnerabilities. A potential adversary or attacker aims to exploit these vulnerabilities to achieve their goal of causing harm to an asset. Vulnerabilities may be present due to faulty configuration, or inherent weaknesses of the assets.

The risk assessment utilizes the concepts of the **Individual Risk Level (IRL)**, which quantifies the risk of an individual asset, taking into consideration its vulnerabilities, but ignoring all interdependencies and relationships with other assets, as well as the **Cumulative Risk Level (CRL)**, which refers to the risk level calculated at a particular asset, but taking into consideration the attack path followed to access this asset by an attacker. While the IRL can be calculated by only using knowledge of the particular asset, the CRL requires knowledge of the asset relationships. Regarding these relationships, the risk assessment metamodel includes the following:

1. **Classes**: Types of relationships, which may be physical, information, geospatial, etc.
2. **Dimensions**: Scope of the asset, including device characteristics, response and coupling behaviour, mode of operation.
3. **Characteristics**: Internal, upstream, and downstream dependencies.
4. **Direction**: Asset relationships can be either unidirectional or bidirectional. For example, given two assets A and B, it is possible that A s able to affect B, but B is not able to affect A, in which case the relationship is unidirectional. If both can affect each other, the relationship is bidirectional.

Relationships between assets have multiplicative effects the overall risk. If a threat affects or harms an asset, this can propagate to other assets and to the overall system, meaning that the asset interdependencies may cause amplification of the total consequences of an event. Therefore, we define the entry point of the attacker to the system as the single point of failure, which can eventually lead to generalized system failure.

To evaluate the CRL while taking into consideration the interdependencies between each individual asset, the knowledge of the relationship itself is not sufficient, but we also need the knowledge of how the exploitation of an asset can lead to the exploitation of a related asset. This knowledge is determined by the propagation rules, which are defined in the Propagation Rules Management component of the Risk Quantification Engine. For example, if an attacker successfully performs a Privilege Escalation Attack on a specific asset, they might act as a legitimate user, thus compromising the confidentiality and integrity of the asset. Through this asset, the attacker may gain access to other assets as well, which may cause harm to other assets that are accessible via the entry point, and therefore the entire system.

It is important to note that it is possible for an attack path to be cyclical, which means that it is possible for an attacker to return to an asset after having already accessed it, to obtain access to a different asset. This is because permissions and privileges might be needed, which may not be accessible through a direct path between two assets. Therefore, the direct path is not equivalent to a cyclical path between the entry and target points, so these two should be considered as two different paths.

The exhaustive calculation of all possible attack paths is performed by the **Attack Profiling** component.

#### 2.2.2.2. Technical Vulnerability and Impact Assessment

The process of defining, identifying and prioritizing vulnerabilities in computer systems alongside with network infrastructures is a vulnerability assessment. The importance of vulnerability assessment lies in the fact that it provides the knowledge and risk background so that administrators can act towards the threats that appear in their environment.

Even though various and promising tools exist in the vulnerability assessment area, few of them support standardized scoring of the assessment result and they mostly require human interaction.

Technical Vulnerability and Impact Assessment (TVIA) performs two functionalities: it assesses all devices and services against known vulnerabilities, and produces detailed reports based on the CVSS [40] scoring system.

The reports are provided in STIX 2.0 [41] format, in the essence of compatibility and according to the needs of each stakeholder.

The TVIA utilizes the standardized CVSS scoring system to score the overall vulnerability of the assessed entities, which is calculated based on three metric groups: Base, temporal and Environmental (Figure 1).

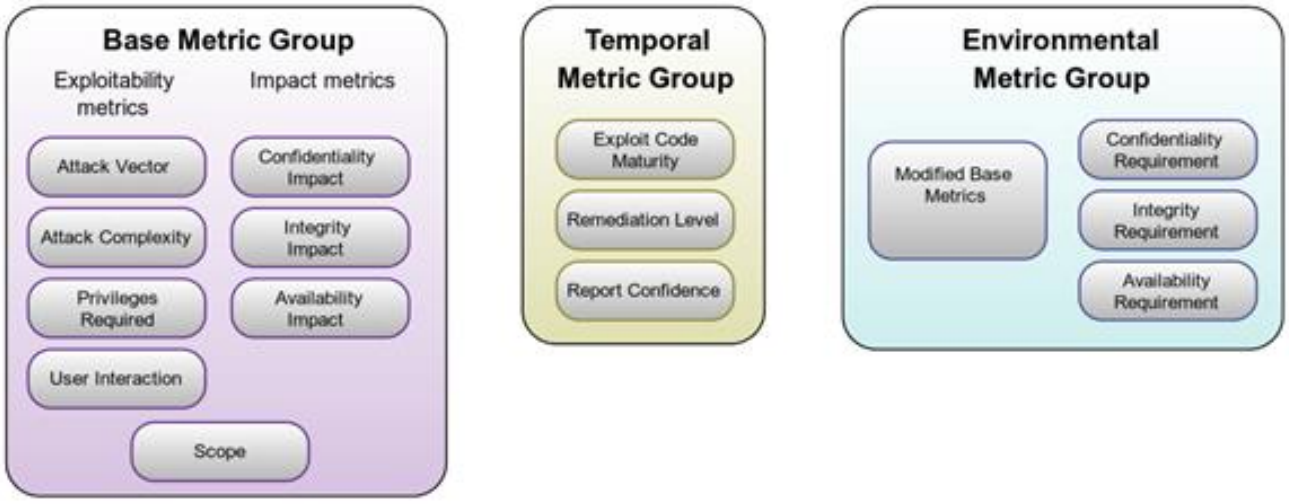


*Figure 1 - CVSS metric groups: Base, temporal and environmental*

The base metric group applies to vulnerabilities whose characteristics remain constant over time and across environments. The temporal metric group refers to vulnerabilities whose characteristics change over time but are not affected from other user environments. Finally, the environmental metric group refers to vulnerabilities whose characteristics are relevant and unique to user environments (Figure 2).

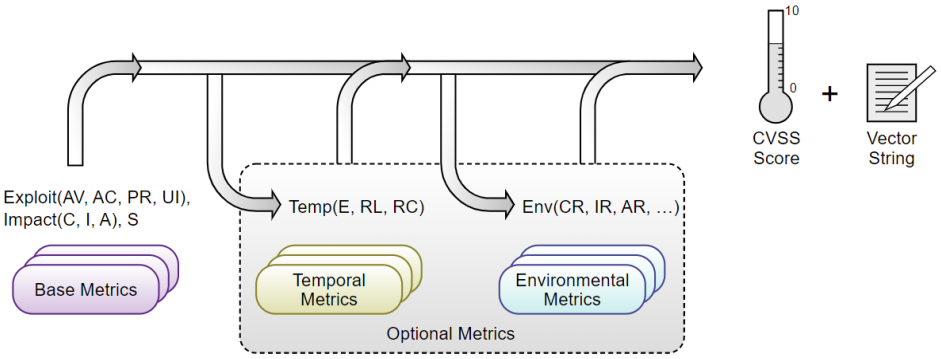


*Figure 2 - CVSS metrics categorized and explained*

The TVIA uses the Exploitability subscore of each detected vulnerability, in addition to the CVSS, to create a more comprehensive view of the impact of each issue.

The exploitability subscore is a metric supplied by NIST that measures how a vulnerability is accessed, the complexity of the attack, and the number of times an attacker must authenticate to exploit a vulnerability effectively. The urgency of resolving each issue is presented through this approach.

The scoring system is calculated with a series of equations, and it is a product of the equations from the base metrics group.

The score severity uses a Likert scale and is mapped to a five-level scale (Table 1).

*Table 1 - CVSS and exploitability scoring system to advisory severity levels*

| Rating | CVSS Score | Exploitability Score |
|---|---|---|
| **None** | 0.0 | 0.0 |
| **Low** | 0.1 – 3.9 | 0.1 - 3.9 |
| **Medium** | 4.0 – 6.9 | 4.0 - 6.9 |
| **High** | 7.0 – 8.9 | 7.0 - 8.9 |
| **Critical** | 9.0 – 10.0 | 9.0 - 10.0 |

**OpenUEBA**

OpenUEBA can identify a variety of threats, it's based on time-series behaviour analytics, and peer-based analytics. Having a defined baseline behaviour for either suspicious or legitimate behaviour can enable OpenUEBA to detect any threat related to the suspicious baseline behaviour which uses different IoCs and similar TTPs, likewise, understanding the legitimate baseline behaviour of an entity allows OpenUEBA to detect deviations and anomalies both from the entity itself and its peers, to detect unknown threats.

Using the IDS "alert triggers" and Monitoring agent "compliance events", we can pinpoint the moment where a threat occurred in the network and start a time-series analysis of the previous behaviour of the entity on the network, which will be assigned a suspicious baseline related to the threat associated with such initial trigger.

Using the data from the IDS, which collects network data (pcap/netflow) from the network, we can detect threats related to malware activity, and data leaks.

The OpenUEBA analysis establishes a behaviour model for each entity in the network, these models can be classified into groups based on multiple criteria, such as their functions, activities, criticality or risk level. When a risk is detected in the network, the OpenUEBA has the capability of correlating the behaviours of the affected entity with the rest of the network, detecting possible other vulnerable/affected entities.

OpenUEBA main functionalities are to:

- integrate security data with identity and entity context: User and Entity Behaviour Analytics compiles security data from event logs and outside threat intelligence. It attributes behaviours to the users and machines that carry them out, creating a master database containing interactions with systems, applications, and data. This database establishes a baseline of normal behaviour. With the baseline data, UEBA can pinpoint significant deviations in behaviour that identify malicious intent.
- UEBA offers robust behaviour analytics using machine learning: Machine learning algorithms analyse real-time security events and related data to detect threats that signature-based tools miss. Machine learning connects related events and compares them to threat models to detect specific types of slow and low attacks.

UEBA prioritizes threats for your security analysts. By taking care of the tedious work upfront, machine learning lets security analysts respond effectively to the top threats affecting the system.

- Analyses the context of user and entity behaviours and security events to reduce false positives: UEBA enriches security data within the context of business and user information. Context data typically includes the user's identity information, the geolocation of the user, the user's asset information, and external threat intelligence.
- UEBA builds profiles for each entity that it monitors and uses the context surrounding their behaviours to separate attacks from false positives.
- UEBA uses risk scores to determine when the behaviour and context rise to a threshold such that it is likely an attack. It connects the dots between related events to look at the entire chain of events, i.e., the attack chain.

#### 2.2.2.3. Human Vulnerability Assessment

Humans are in many cases identified as the weakest link in many cybersecurity architectures. Human errors can expose sensitive data, disrupt systems, or create exploitable access points for malicious software and attackers. Thus, HVA aims to assess the level of vulnerability that humans impose on the organization under which they operate. The HVA component utilizes specifically designed questionnaires to automatically extract personality characteristics and traits, which in turn illustrate the kinds of social engineering attacks the subject is more prone to sustain. The HVA results come to complement the overall risk assessment of an organization, along with the hardware and software assessments.

The Human Vulnerability Assessment (HVA) component utilizes existing frameworks to categorize and distinguish different personality traits and characteristics, such as:

- **Five Factor Model**: Which includes five unique personality traits Openness, Consciousness, Extraversion, Agreeableness, Neuroticism.
- **Myers – Briggs Type indicator**: Which is an inventory designed to identify a person's personality type, strengths, and preferences.
- **Dark Triad**: Which is a personality model with the tendency of exploring a darker side of the human personality and is focused on aspects of personality that can manipulate and deceive. The three traits mentioned in this model are Psychopathy, Narcissism, and Machiavellianism.

The HVA will take under consideration a wide range of parameters to identify the vulnerabilities. Factors that will be included are personality, decision-making, willingness for risk taking etc. The HVA component, following the GDPR guidelines [42] (Article 25, 32), will not store nor disseminate

individual vulnerability scores and results. It will produce reports that depict the cumulative vulnerability status of different departments (e.g., Accounting).

The HVA component will be based on personality traits as they are explored in the Five factor model, the Myers – Briggs type indicator, the dark trial, etc. Also, we will examine the HV, based on the demographics and personal characteristics.

### 2.2.3. Security awareness training for professionals and clients

#### 2.2.3.1. Cyber Range for Security Professionals

The Cyber Range is the tool dedicated to train security professionals in a safe and emulated environment. The Cyber Range tools rely on the virtualized environments components such as virtual machines to recreate an infrastructure as close to the real infrastructure. Cyber Ranges are defined as an interactive and simulated representation of a local network. They provide a safe environment to test and exercise cyber skills for product development and security posture testing.

From a technical point of view a Cyber Range is characterized by:

- A multi-level computer simulation environment.
- Network topologies: The environment makes it possible to reproduce network topologies made up of several thousand, or even tens of thousands of nodes. If based on a traditional virtualization system, the novelty lies in the fact that the administrators can easily create and configure network architectures and hosts.
- Security technologies such as firewalls, IPS/IDS, SIEM etc.
- Network traffic generators inject legitimate or malicious traffic into the environment to create the noise present in any network.

On the user side, Cyber Range revolves around two distinct teams:

- The "red team", responsible for attacking a system or a network. They reproduce targeted attacks to challenge the security mechanisms according to scope of the attack scenario
- The "blue team", responsible for the defence of networks and information systems, which is therefore made up of trainees participating in the training program.

A Cyber Range's purpose is utilized for 3 main targets: research, training, and exercises/competition in cybersecurity.

A Cyber Range can be categorized into 3 types: simulation, emulation and hybrid and they all rely on virtualization technologies. However, there are two kinds of virtualization. Conventional virtualization such as containers (Docker, lxc) and hypervisor (VMware, Gemu, VirtualBox, etc.) and Cloud virtualization such as Openstack, Terraform, AWS with both private and public clouds.

Different Cyber Ranges differ also by the kind of attacks/scenarios and network they can simulate. They all are focused on different areas. For that reason, the concept of Cyber Range collaboration emerges to cover a wide spectrum of situations.

Different manufacturers offer Cyber Ranges or simulation environments dedicated to cybersecurity such as Diateam (France), Thales (France), Cyber Test Systems (France), Airbus (France) Cyberbit (Israel), Ixia (United States), Ravello Systems (United States), Sypris (United States), IBM (United States), CybExer, Raytheon, Fujitsu etc.

Many Cyber Ranges come from universities and research institutes. The most used are listed in [57] and [58].

Finally, there is also a Cyber Range named Kypo from the Concordia European project [43].

In the context of the SECANT project, the development of the Cyber Range component is not focussed on internal function of the component itself but on the content of the Cyber Range, i.e., the attack and training scenarios that can be made available within in the Cyber Range's environment.

The healthcare infrastructure that will be simulated for the SECANT project is not currently available in any other available cyber range and is one of the core contributions to the SECANT's Cyber Range component.

Moreover, the SECANT components CSRAC and TIM will be simulated and included into the training scenarios. The usage of these components into a Cyber Range scenario is another core contribution part of the innovation the SECANT's Cyber Range component.

#### 2.2.3.2. Cyber Security Training Module

The Cyber Security Training Module (CSTM), when integrated with a chatbot application can act as a complete tool for the security awareness training of healthcare professionals and clients (patients). Chatbots are lightweight applications that can converse and interact with users through written and visual languages while at the same time they offer ease of use combined with an entertaining experience.

Every day we witness a constant increase in the amount of data that are generated, collected, and processed. The same is true for sensitive medical data which, due to their nature, must remain well protected while access to them must be very controlled. At the same time, modern platforms, like the web, facilitate access to these data from different places and at any time, shifting thus the data management tasks from few professionals to every involved individual. Therefore, as individuals have more control over their data, it becomes imperative to develop and maintain a satisfactory level of security awareness to minimize the risks of breaches or other types of misuse to their data by unauthorized actors. To this end a chatbot application provides a cost efficient and easily deployable solution that can significantly contribute to the increase of the security awareness level of clients, through the highly interactive and user-friendly conversational environment it offers.

The CSTM platform integrated with the Chatbot application will be accessible by any healthcare professionals and clients (patients) interested in taking a cybersecurity-relevant assessment. The assessment itself will be accessible through a link on the End User Application, that will redirect the user to a personalized session, held by the chatbot application. The assessment will comprise a configurable number of questions, for which the user's responses will be sought. At the end of the assessment session the chatbot application will be able to provide feedback to the user on his performance and depending on the responses, it may also provide references to material for improving the user's skills and enhancing the awareness of security topics.

The questions posed by the chatbot to the user will be randomly selected among a pool of questions categorized into 4 levels of difficulty [easy-medium-difficult-very difficult]. The different types of questions that are supported by the chatbot application are the following:

- Choosing one or multiple answers from a list of multiple-choice questions.
- Answering through free text.
- Multimedia content.

### 2.2.4. Trust and Accountability Module

The main role of the Trust and Accountability Module (TAM) is to register and verify decentralized devices identities and records devices' data transactions throughout different stakeholders' supply chains to ensure zero-error deliveries, adherence to standards and auditability. The SECANT will lay out an architecture for incorporating a decentralized security and privacy for data.

The current issue with the blockchain on the other hand, is its low scalability and a small number of transactions per second [44]. SECANT will address some of the most important problems with existing blockchain infrastructure such as being able to run on lightweight devices with constrained memory, eliminating transaction fees, and scalability.

TAM module core innovation is in its ability to verify devices and data integrity, on behalf of the data owner and provide access only to actors in the medical ecosystem that are authorized to access them.

The proposed approach will minimize the potential problem of losing control over the data, and it will increase the trust overall of the devices used in the medical ecosystem. To achieve this, the TAM module uses IOTA Tangle and IOTA streams.

The **IOTA Tangle** (i.e., a system of nodes used for confirming transactions) will be used for its lightweight and scalable nature that allows the integration of heterogenous datasets, as well as for its feeless consensus protocol. This highly reduces the barriers for adoption of this technology compared to conventional blockchain platforms. The Tangle is using different consensus mechanism from other blockchains.

The TAM Module integrates **IOTA Streams** – an encrypted channel that anchors the data in the blockchain (IOTA Tangle). IOTA Streams protects confidentiality of ledger data, while IOTA Identities will be integrated to remove unreliable centralized Identity Management Systems. The consensus mechanism is necessary to achieve agreement among the nodes of the network and ensure integrity of the data transactions.

Depending on the requirements of a particular application or use case, in each tangle the set of entities entitled to participate in the consensus algorithm (and, consequently, the algorithm used) can vary. For instance, an application may require that the validation of the transactions is performed by a single authority or a predefined set of multiple authorities. In contrast, other use cases may require that the validation is performed by the majority of a given community. For this reason, IOTA supports different configurations of the consensus mechanisms, and in SECANT we will use milestone consensus algorithm.

In milestone consensus, a special node acting as validator or coordinator is provided with an identity (a pair of ED25519 private and public keys). The validation takes place periodically (e.g., every 10 seconds) in the form of a special message called a ‘milestone’. Each milestone validates and confirms the set of messages and transactions it directly and indirectly references. Thus, the algorithm to select the set of parents of a milestone is optimized to maximize the number of messages confirmed by its past cone.

When a new milestone is broadcasted to the network, nodes in the network will first validate its signature against the known public key of the validator and then order the set of messages it confirms. A subset of the Tangle can be ordered depending on many of its properties (e.g., the alphanumeric sort of the message hashes); however, to compute the ledger state, a graph traversal must be done so it can be used to order the messages in a deterministic order with no extra overhead. This ordering is then defined as a topological ordering because it respects the dependency of messages, ensuring that parents of a message are applied before it. Since there are multiple valid topological orders for the same graph and to avoid conflicting ledger states, it is required that all nodes apply messages in the exact same order.

Thus, nodes apply the topological ordering generated by a post-order Depth-First Search (DFS) starting from a milestone message, going through its parents (in the order they appear in the message) and finally analysing the current message. Since only a subset of messages is considered, the stopping condition of this DFS is reaching messages that have been already confirmed by another milestone. If a conflict occurs in the set of messages confirmed by a milestone, nodes must apply the first (with regards to the order previously proposed) of the conflicting messages to the ledger and ignore all the others. Once a message is marked as ignored it is final and cannot be changed by a later milestone. Since the ledger state is maintained from one milestone to another, a message conflicting with a message already confirmed by a previous milestone would also be ignored.

Milestones can also be independently signed by multiple identities, acting as a prefixed committee of validators. Each member of the committee operates as a signature provider service and should run on an independent infrastructure element. This mitigates the risk of an attacker having access to all the key material necessary for forging milestones. The role of forming and proposing a milestone to

the rest of the committee can be assigned to one of the committee members both statically and dynamically. Such a role is dubbed 'coordinator'.

The coordinator collects signatures from the rest of the committee members acting as signature providers through an ad-hoc RPC connector. Mutual authentication should be enforced between the coordinator and the signature providers: a client-authenticated Transport Layer Security (TLS) handshake scheme is advisable. To increase the flexibility of the mechanism, nodes can be configured to require a quorum of valid signatures to consider a milestone as genuine.

If the application mandates for mission-critical grade requirements, the committee members can use a threshold signature scheme (e.g., "Boneh–Lynn–Shacham (BLS) under a Byzantine fault-tolerant (BFT) protocol in either a (weakly) synchronous (e.g., pBFT) or asynchronous assumption (e.g., HoneyBadgerBFT) to reach consensus on the creation of a new valid milestone.

The milestone-based consensus algorithm has three primary advantages over the approval weight-based one.

- First, it is more technically mature. While the approval weight variant is still under development, the milestone version is currently running live on the IOTA mainnet network.
- Second, it is securely permissioned. Although a network with approval weight can be permissioned too, particularly when mana is derived from a coin whose supply is limited to a few actors, the coordinator achieves a permissioned setup. The committee that runs the coordinator is cryptographically linked through their shared public key and changing any member of that committee requires all nodes to participate in a new distributed key generation phase, and thus the consent of the other committee members.
- Lastly, a network with a coordinator is much easier to anchor since finality is so easy to prove.

### 2.2.5. Privacy Toolkit

In this module, we will develop a backend and off-chain functionalities to define how the data owner can encrypt a decentralized sensitive data flow and further share it within the same supply chain or across different domains within the SECANT. This tool will be integrated with the IOTA Streams used in the TAM implementation for secure management and sharing of required encryption keys.

The privacy toolkit is designed for securing the patient and hospital records, achieving a fine-grained access control for hospital employers, and preventing a brute-force attack against the password or ciphertext. Specifically, the toolkit applies a hybrid combination of symmetric and asymmetric encryption technologies, which includes attributed-based encryption, proxy re-encryption, searchable encryption, password-based encryption, and honey encryption.

#### 2.2.5.1. Hybrid protection over data

**Attribute-Based Encryption (ABE)**: ABE is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes. In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext [45].

In ABE scheme, attributes play an especially important role. Attributes have been exploited to generate a public key for encrypting data and have been used as an access policy to control users' access. The access policy can be categorized as either a key-policy or ciphertext-policy. The key policy is the access structure on the user's private key, and the ciphertext-policy is the access structure on the ciphertext. The access structure can be categorized as either monotonic or non-monotonic one. Using ABE schemes can have the advantages: (1) to reduce the communication overhead of the Internet, and (2) to provide a fine-grained access control [46].

**Searchable encryption (SE)**: SE is a type of encryption that allows a party to outsource the storage of its data to a server in a private manner while maintaining the ability to selectively search over it. In such a scheme, users encrypt their files locally and send them encrypted to the cloud service provider

(CSP). Hence, the CSP who does not have access to the encryption key cannot learn anything about the content of users' data. Furthermore, whenever users wish to access their files, they can search directly over the encrypted data for specific keywords [47].

The two main branches of SE are Searchable Symmetric Encryption (SSE) and Public key Encryption with Keyword Search (PEKS). SSE allows only private key holders to produce ciphertexts and to create trapdoors for search, whereas PEKS enables several users who know the public key to produce ciphertexts but allows only the private key holder to create trapdoors [48].

**Proxy Re-Encryption (PRE)**: PRE is a type of encryption used for secure data sharing that enables a semi-trusted proxy to transform a ciphertext encrypted under the public key of a data owner into another ciphertext under the public key of another user without leaking the underlying encrypted messages or private keys of the data owner to the proxy [49].

PRE can be broadly classified into two categories: (1) Uni-Directional Schemes and (2) Bi-Directional Schemes.

The Uni-Directional Schemes are further classified as Identity-Based PRE, Attribute-Based PRE, Ciphertext-Policy Attribute based PRE, Conditional PRE, Time based PRE. The Bi-Directional Schemes are further classified as Type-Based PRE and Threshold-Based PRE [50].

Attribute-based PRE (ABPRE) combines the notions of PRE and ABE, allows a semi-trusted proxy to transform a ciphertext under a particular access-policy into a ciphertext under another access policy, without revealing any information about the underlying plaintext [50].

Conditional PRE (CPRE) is used to handle scenarios where a fine-grained delegation is demanded. In CPRE, only ciphertext satisfying a specific condition set by Alice can be transformed by the proxy and then decrypted by Bob [50].

Time Based PRE (TPRE) provides a scalable user revocation and reduces the workload of data owners. The main idea is to combine the concept of time together with ABE and PRE. In TPRE, the data is held with an attribute-based access structure and an access time. Each user is identified by a set of attributes and a set of eligible periods which denote the period of validity of the user's access right. The scheme allows every user's access right to be effectual in a pre-determined period and enables the cloud service provider to re-encrypt ciphertexts based on their own time [50].

Identity-Based PRE (IB-PRE) is an extended IBE scheme, which allows a proxy to translate an encryption under Alice's identity into one computed under Bob's identity. The proxy uses re-encryption keys to perform the translation without being able to learn the plaintext. No information on the secret keys of Alice and Bob can be deduced from the proxy keys [50].

#### 2.2.5.2. Protection over key, password & security-related information

**Password-Based Encryption (PBE)**: PBE is a type of encryption that generates a secret key based on a password provided by a user and a mixed-in salt. Then users can encrypt and decrypt their files with an easy to remember password and at the same time be confident that their files are secure [51].

**Honey Encryption (HE)**: HE is a type of encryption that provides resilience against brute-force attack by serving up plausible-looking but fake plaintext for every invalid key used by an intruder to decrypt a message [52].

### 2.2.6. Digital Identity Management Module

#### 2.2.6.1. Decentralized Identities

The traditional identity management system adopts the centralized approach, with a design already witnessed several limitations and weaknesses regarding security, privacy, and scalability. The negative side of centralized models is that identity providers have full control over individuals' identities, and the identity owners are incapable of preventing any misuse of their identities [53]. The sensitive data are exposed on daily basis in breach incidents caused by weak security of the

centralized databases. There are numerous weak points in the centralized approach, one of them being exchange of data when users register or access the services, when the data are shared or stored without following the best practice or standards.

SECANT decentralized identities will be based on the decentralized Identity or Self-Sovereign Identity (SSI) - a new method for identity management and authentication based on W3C Standard. It removes the centralized aspects and puts the Identity subject in full control over its own identity. Decentralized identity provides a solution for the increasing amount of database breaches, the lack of trust in any digital setting, and the increasingly difficult to comply to privacy legislation, such as GDPR. Another regulation to consider is eIDAS [54], compliance with which is not mandatory, but recommended. Complying with eIDAS provides interoperability of identities between the different EU Member States.

Self-Sovereign Identity is about returning autonomy and privacy to the individual, while controlling information flow. The user can create a single online profile, containing all personal information and decide who they share what information with, and a Verifier is able to verify the information to be correct, making the data trustworthy. This moves their online profile from a statistical estimation by corporate entities to an accurate and verifiable profile under their control.

The IOTA Identity framework goes beyond the scope of many other Self-Sovereign Identity frameworks and provides a fully secure environment for creating, storing, and sharing identities and verifiable credentials, based on several standards such as the W3C Decentralized Identifiers (DID) and Verifiable Credentials and the DIF DIDComm Messaging specifications alongside supporting methods. This framework can be used to create and authenticate digital identities, creating a trusted connection and sharing verifiable information, establishing trust in the digital world.

An identity solution contains many secrets, such as private keys and verifiable credentials. KayTrust's[1] credential management platform allows companies to issue verifiable credentials integrated with their information system, manage corporate and individual identities, issue, view, verify and revoke credentials, and manage received and issued credentials.

KayTrust will also provide a wallet that allows users to register their own identity on various Blockchain networks, as well as store and verify their credentials, which can be shared with other users or institutions, manage their identity and store, verify, and share credentials.

There are different ways to approach to the solution. One of them is using IOTA Tangle and 2nd layer IOTA Streams for sharing of encrypted information. However, for the Decentralized Digital Identity Management (DIM) module of this project, we will focus on a combination of the KayTrust and IOTA Identities solutions as the best solution.

#### 2.2.6.2. SECANT API

The main objective of SECANT API is to implement a service of collection of the metadata from the complex ICT infrastructures and from different type of data sources to transfer the required data into the SECANT platform and the metadata into the TAM module.

The API service has the role to collect and aggregate the crossing data and to change it in a commonly format accepted by the TAM Module. It also integrates the Decentralized Identity Management service to sign the data collected from ICT ecosystems.

### 2.2.7. SECANT Dashboard and End User Application

A Dashboard is an application built to display valuable information and critical, relevant data at a glance from a single point of access. The SECANT Dashboard acts as the main point of interaction between cybersecurity professionals and the SECANT platform. It will implement a Graphical User Interface (GUI) that supports the cyber security risk management teams interacting with the SECANT

[1] Asset provided by NTTDES, https://www.kaytrust.id

services. The Dashboard will offer access to the database of vulnerabilities collected by the SECANT Threat Intelligence module. Through the SECANT Dashboard, a cyber security professional shall be able to access the database of organization-specific, and general cyber security, and social engineering vulnerabilities collected by SECANT's Threat Intelligence module. The cybersecurity professional will be able to monitor the impact of the identified vulnerabilities as they propagate through the ICT ecosystem. Furthermore, the Dashboard will act as an integration point for the Organizational Cyber Range and the Connected ICT Cyber Risk Assessment Engine, providing access to the said services through the Dashboard's GUI.

Two significant challenges for the Dashboard are to provide advanced dashboard capabilities and to create a common UI/UX language for security experts. These features will act as an extra layer of information that will allow professionals not familiar with the complex ICT infrastructure specificities to access management tools to visually track, analyse, and display Key Performance Indicators (KPI).

The SECANT End User Application will allow health professionals and clients (patients) to access their sensitive data as well as raise their security awareness through training sessions. The health professionals and clients (patients) will be able to receive cybersecurity training concerning common online behaviours that can lead to cybersecurity pitfalls (e.g., social engineering), and learn ways to identify and remedy problematic situations to avoid compromising the security of the ICT ecosystem. The SECANT End User App interfaces with the CSTM for the cyber security assessment of the health professionals and clients (patients).

The monitoring capabilities will be offered by the End User Application that will allow its end users to easily identify how the information they received has been treated (e.g., who interacted with it, when and where was it created, which devices have been used) so their trust towards other stakeholders of the information chain can be increased.

The SECANT Dashboard and the SECANT End User Application will capitalize on well-established open-source frameworks for their implementation to overcome these challenges and fulfil the defined requirements.

## 2.3. Security Risk Identification and Threat Portfolio

This section depicts the initial threat portfolio that will form the basis of the CTI and the taxonomies that will be developed under WP3. Table 2 presents each threat, a short description and the impact of the threat in case of materialization. It is important to highlight that another significant threat is the threat against data but any of the following threats could harm data, based on the intentions of the malicious actors.

*Table 2 - Initial threat portfolio*

| Threat | Description | Impact |
|---|---|---|
| Cross-Site Scripting (XSS) | Cross-Site Scripting (XSS) attacks are a type of injection, in which the attacker inject data such as malicious scripts into trusted websites. The injection is achieved using a scripting language such as JavaScript. | Depending on the type of the XSS attack there are various impacts. Since the injected content originates from a trusted source which is the compromised website, the web browser of the user allows the content and the functionalities of the injected script. Therefore, the attacker can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. Furthermore, some XSS attacks are also able to modify the content of the HTML page. |

| Threat | Description | Impact |
|---|---|---|
| SQL Injection | SQL injection refers to an attack where the attacker injects SQL queries or procedures to the target application to gain unauthorised access to the application database or alter the stored data. | SQL injection targets mainly the confidentiality and the integrity of the data. In case the SQL Injection is successful, the attacker could read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. |
| Local File Inclusion (LFI) | LFI is an attack where the attacker tricks the web application into either exposing or running files on the web server. The most common reason for the success of such attacks is the lack of user input validation. | A successful LFI attack can result in exposure of sensitive data and in some cases, it can lead even in cross-site scripting (XSS). |
| Man-in-the-Middle (MitM) | MitM attack is a type of cyberattack in which the attacker secretly intercepts and relays messages between two communicating parties. | Unauthorised disclosure/exposure of data. |
| Man in the Browser (MitB) | MitB is very similar to a man-in-the-middle (MitM) attack. In a MitB attack the attacker installs a Trojan malware on the victim's computer which enables the modification the target user's web transactions. The Trojan is used to intercept and manipulate calls between the browser and the server. | The most common impact of MitB is financial fraud by manipulating transactions of Internet Banking systems. |
| DoS/DDoS | The Denial of Service (DoS) attack is focused on making a resource (site, application, server) unavailable. A distributed denial-of-service (DDoS) is performed by utilising several compromised machines which generate extensive internet traffic towards the target. The compromised machines can include computers as well as other networked assets such as IoT devices. | Renders the resources either temporary or permanently unavailable. If a service receives a very large number of requests, it may cease to be available to legitimate users. |
| Brute Force Attack | Brute force attacks can be realised following various approaches. The most common method is configuring predetermined values, making requests to the target server using those values, and subsequently analysing the response. Brute-force attacks are considered as a trial-and-error method which is used by the attackers to guess the password or encryption keys. | In case the attacker manages to guess the password of a user, the attacker could connect as the authorised user. Depending on the privilege level of the user, the attacker could access, modify, or even delete data. In case the attacker manages to guess the encryption keys then the encrypted data become susceptible to unauthorised disclosure/exposure. |
| Buffer Overflow Attack | Buffer overflow is an attack where the attacker attempts to write more data to a fixed-length block of memory, or buffer, than the buffer is allocated to hold. | Buffer overflow can result in crashing the target application, causing the target application to behave unpredictably and generate incorrect results, memory access errors, or crashes. |

| Threat | Description | Impact |
|---|---|---|
| Phishing | Phishing is considered as the most prevalent cybersecurity threat in healthcare. The most common phishing attack includes the practice of infecting a seemingly benign email which contains malicious links or attachments. | The attacker may gain access to the compromised machine which allows the attacker to perform further actions within the organisation's infrastructure. Most frequent actions include the use of the further spread of the malware and using the compromised machine as bot. Furthermore, the attacker could escalate privileges to gain unauthorised access to sensitive data. |
| pear-phishing | Spear-phishing is similar to a phishing attack with the difference that it targets a specific organisation or individual. Attackers gather as much information as they can through passive or active reconnaissance which is later used to craft targeted phishing emails. | The attacker may gain access to the compromised machine which allows the attacker to perform further actions within the organisation's infrastructure. Most frequent actions include the use of the further spread of the malware and using the compromised machine as bot. Furthermore, the attacker could escalate privileges to gain unauthorised access to sensitive data. |
| Scareware | Scareware attacks send extensive amount of false security alarms and alerts that indicate that the machine has been compromised. Therefore, users are deceived to think that their system has been compromised. The scareware is displaying a message which suggests installing a fake security software that could facilitate the delivery of a malware or is malware itself. | The attacker may gain access to the compromised machine which allows the attacker to perform further actions within the organisation's infrastructure. Most frequent actions include the use of the further spread of the malware and using the compromised machine as bot. Furthermore, the attacker could escalate privileges to gain unauthorised access to sensitive data. |
| Ransomware | Ransomware is a type of malware which encrypts an organisation’s data and demands payment (ransom) to restore access. The payment is usually done using cryptocurrency to avoid the detection of the attacker. | Encrypts all data and applications that is stored on the compromised machine to prevent the access to data and use of applications until the ransom is paid. More than 1 in 3 healthcare organizations globally fell victim to a ransomware attack in 2020. Concerning the healthcare domain, ransomware is considered the most common attack vector. |
| Spyware | Spyware is one of the most common threats to internet users. Spyware is a malware which aims at capturing sensitive data from a user’s computer and send it over the internet to adversaries without user acceptance. | Steal sensitive data and disclose/expose it to third parties. Data breach and misuse of private data. |
| Trojan Horse | Trojan is a type of malware which contains malicious code but is masquerade as a benign trusted software. The malicious code can be injected on benign applications, masqueraded in e-mail links leading to the download of a seemingly legitimate software and sometimes hidden in web pages as JavaScript code. There are 7 main types of Trojan Horse: Remote Access Trojan (RAT), Data Sending Trojan, Destructive Trojan, Proxy Trojan, FTP Trojan, Security software disabler Trojan, and Denial-of-Service attack Trojan. | Depending on the type of the Trojan, the impact includes among others abnormal behaviour of the compromised machine, unauthorised disclosure/exposure of data, modification of data or machine settings, deletion of data, use of the compromised machine as proxy for illicit purposes (e.g., banking fraud). With regards to the healthcare domain, the impact could also include steal payment information, re-route shipments, change prescriptions, or discover personal, confidential healthcare information. |

| Threat | Description | Impact |
|---|---|---|
| Worm | Worm is a malware that can propagate or self-replicate from one computer to another without human interaction. Worms spread across a network by replicating themselves. | Once the worm successfully infects a machine, it starts to self-replicate through the network. The impact varies based on the intentions of the coder/developer. On many occasions, it causes performance issues by draining the computer/network resources, it can delete files, steal data and more. |

# 3. Methodology

Common classification of requirements divides them into functional and non-functional requirements. Functional requirements capture the fundamental properties of the system at hand, describing its tangible processes, actions, and technical properties. Non-functional requirements capture properties that the system's functions must have such as performance, usability, GDPR compliance and security. In contrast with the functional requirements, non-functional requirements focus on the quality characteristics of the system.

The methodology followed for the elicitation, prioritisation, and refinement of functional and non-functional requirements of the SECANT platform consists of the following phases:

- Initially, a template was designed (ANNEX 1- Tool's Overview Template) and distributed to all SECANT technology providers. The template aimed to gather information about the SECANT tools or modules. In more detail, the template consists of two sections. Section 1 requests a detailed description of the tool (i.e., Name, Owner, Current TRL, Description, Input, Output, Dependencies, Tasks Involved, Innovation, and other information), while Section 2 refers to the key technological areas the tool or module it will contribute. Based on the input gathered via the form, we were able to identify the basic functionalities that each technological module will provide to the overall SECANT platform.
- Then, we examined and analysed D2.1, in which reported the end-user and stakeholder requirement classified as "NICE TO HAVE"; "SHOULD HAVE", and "MUST HAVE", to produce an initial draft of the technical requirements.
- Following, to be able to identify additional functionalities and aspects of the system that need to be satisfied by the technical solution offered by SECANT examined the Use cases as defined in the context of T2.3, namely: Protecting the Connected Ambulance of the Future, Cyber Security for Connected Medical Devices and Mobile Applications, Health Data Protection in the Healthcare Supply Chain and Cyber Security Training. The actors involved in the use cases can be categorised into two groups, namely (i) healthcare professionals and clients (patients); and (ii) ICT & Security professionals. The SECANT Use Cases will elaborate further in the deliverable (D2.3).
- Finally, to conclude the technical requirements with the collaboration of all technology providers brainstorming sessions, workshops, and dedicated telcos, produced the SECANT Technical Requirements Template (see Table 2) via which each SECANT tool or module owner identified and reported all functional and non-functional requirements. The prioritisation of the technical requirements followed the MoSCoW prioritisation approach, to define each requirement's criticality:
    - Must have: A label used for the most critical requirements which, if not delivered, could jeopardise the success of the whole project.
    - Should have: Denotes requirements that are important but not critical for the success of the implementation. Such requirements can be less time-critical than "Must have" requirements or there might be alternative ways to satisfy them.

- Could have: This category includes requirements that are desirable but not necessary. They usually include aspects relating to user experience or customer satisfaction which can be implemented if time and resources permit it.
- Won't have: Requirements in this category are the least critical and shall not be included or shall be reconsidered during later stages of the implementation.

*Table 3 - SECANT Technical Requirements Template*

| ID | <Unique string to identify each requirement> |
|---|---|
| **Name** | A brief name for the technical requirement |
| **Description** | A short description of the requirement |
| **Priority** | Following the MoSCoW method for the prioritisation of requirements one of the values. |
| **Relevant User Requirement(s)** | ID of related user requirements from D2.1 (if any) |
| **Dependency** | IDs of other related requirements (if any) |

# 4. SECANT Technical Requirements

## 4.1. Threat Intelligence Module

### Functional Requirements

| ID | TIM_FR_001 |
|---|---|
| **Name** | CTI Gathering via GUI |
| **Description** | Manually collect and retrieve threat information through an easy-to-use GUI (MISP). |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Collection and Extraction Module No. 2 |
| **Dependency** | - |

| ID | TIM_FR_002 |
|---|---|
| **Name** | Manual threat formulation |
| **Description** | User centric GUI design, to formulate a threat. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Collection and Extraction Module No. 6 (6.2) |
| **Dependency** | TIM_FR_001 |

| ID | TIM_FR_003 |
|---|---|
| **Name** | Input of Blacklisted IPs |
| **Description** | Provide functionality to specify blacklisted IPs from earlier attacks. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Collection and Extraction Module No. 6 (6.1) |
| **Dependency** | - |

| ID | TIM_FR_004 |
|---|---|
| **Name** | Data collection from Internal Sources |
| **Description** | Collect data from different internal sources (logs from IDS, IPS, Firewall etc.) |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Collection and Extraction Module No. 7, 8 (8.1 & 8.2), 10 |
| **Dependency** | - |

| ID | TIM_FR_005 |
|---|---|
| **Name** | Data collection from External Sources |
| **Description** | Collect data from different external sources (social media, surface and dark web, feeds from CERTs/CSIRTs etc). |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Collection and Extraction Module No. 1 (1.4), 7, 9 |
| **Dependency** | - |

| ID | TIM_FR_006 |
|---|---|
| **Name** | Data Correlation |
| **Description** | Correlate the different data that is received to create enhanced actionable CTI. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Collection and Extraction Module No. 4, 8, 9 |
| **Dependency** | TIM_FR_004, TIM_FR_005 |

| ID | TIM_FR_007 |
|---|---|
| **Name** | CTI Extraction |
| **Description** | Extract CTI in JSON, CSV, and PDF. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Collection and Extraction Module No. 5 (5.1, 5.2 & 5.3) |
| **Dependency** | TIM_FR_004, TIM_FR_005 |

| ID | TIM_FR_008 |
|---|---|
| **Name** | Support of CTI Standards |
| **Description** | Support extraction of CTI in standards such as STIX 2.X |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Collection and Extraction Module No. 1 (1.3) |
| **Dependency** | - |

| ID | TIM_FR_009 |
|---|---|
| **Name** | API Support |
| **Description** | Provide API which supports CRUD operations. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Collection and Extraction Module No. 1 (1.1), 3 (3.2), 6 (6.2) |
| **Dependency** | TIM_FR_001, TIM_FR_002 |

| ID | TIM_FR_010 |
|---|---|
| **Name** | API User Authentication |
| **Description** | Authenticate API user with their API Key to provide access only to specific data according to the user's role and access rights. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Correlation and Sharing Module No. 6 |
| **Dependency** | - |

| ID | TIM_FR_011 |
|---|---|
| **Name** | Crawler GUI |
| **Description** | User-friendly GUI that supports different configuration options (e.g., time intervals, crawling type, depth, etc.) |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Collection and Extraction Module No 1 (1.1), 6 (6.2), |
| **Dependency** | TIM_FR_001 |

| ID | TIM_FR_012 |
|---|---|
| **Name** | CTI Collection |
| **Description** | Provide the option to configure on MISP the time interval of CTI collection. |
| **Priority** | Should have |
| **Relevant User Requirement(s)** | CTI Correlation and Sharing Module No. 2 (2.1, 2.2, 2.3, 2.4) |
| **Dependency** | - |

| ID | TIM_FR_013 |
|---|---|
| **Name** | Filtering Options |
| **Description** | Provide filtering functionalities (e.g., date range) |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Correlation and Sharing Module No. 7 |
| **Dependency** | - |

| ID | TIM_FR_014 |
|---|---|
| **Name** | Simple and Advanced Correlation |
| **Description** | Provide both simple (e.g., MISP correlation) and advanced (e.g., ML-based) correlations of threats. Simple correlations will correlate threats based on similar values in different fields, while advanced correlations will correlate threats based on different features that are extracted from the identified threats. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Correlation and Sharing Module No. 9 |
| **Dependency** | TIM_FR_004, TIM_FR_005 |

| ID | TIM_FR_015 |
|---|---|
| **Name** | Search Engine |
| **Description** | Provide a search engine to narrow down searches within the available taxonomies. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Dynamic Taxonomies Creation Module No. 2 |
| **Dependency** | - |

| ID | TIM_FR_016 |
|---|---|
| **Name** | Description of Taxonomies |
| **Description** | Provide a functionality which explains the relevant terms regarding the included taxonomies on MISP. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Dynamic Taxonomies Creation Module No. 1, 3, 5 |
| **Dependency** | - |

| ID | TIM_FR_017 |
|---|---|
| **Name** | Automatic clustering of taxonomies |
| **Description** | Automatic clustering of taxonomies according to context through machine-learning and deep-learning based techniques. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Dynamic Taxonomies Creation Module No. 4 |
| **Dependency** | TIM_FR_014 |

## Non-Functional Requirements

| ID | TIM_NFR_001 |
|---|---|
| **Name** | TIM Availability |
| **Description** | Ensure availability of at least 97% uptime. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Correlation and Sharing Module No. 2 (2.1) |
| **Dependency** | - |

| ID | TIM_NFR_002 |
|---|---|
| **Name** | TIM CTI Data Reliability |
| **Description** | Ensure that all data is up to date according to the time interval that has been set. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Collection and Extraction Module No. 2, 3 (3.1)<br>CTI Correlation and Sharing Module 2 (2.1, 2.2, 2.3, 2.4) |
| **Dependency** | TIM_FR_012 |

| ID | TIM_NFR_003 |
|---|---|
| **Name** | TIM CTI Data Integrity |
| **Description** | Ensure that the data is consistent. Meaning that the data is not modified by unauthorised users and that all changes are logged. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Collection and Extraction Module No. 11<br>CTI Correlation and Sharing Module No. 10 |
| **Dependency** | - |

| ID | TIM_NFR_004 |
|---|---|
| **Name** | TIM CTI Standard Integrity |
| **Description** | Ensure that the content of TIM output that follow a specific CTI standard as STIX 2.X, is validated according to the standard specification. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Collection and Extraction Module No. 1 (1.3) |
| **Dependency** | TIM_FR_008 |

| ID | TIM_NFR_005 |
|---|---|
| **Name** | TIM CTI Data Confidentiality |
| **Description** | Ensure that the data is accessible only to authorised users with the appropriate access rights. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Collection and Extraction Module No. 11,<br>CTI Correlation and Sharing Module No. 3, 6, 10 |
| **Dependency** | TIM_NFR_003 |

| ID | TIM_NFR_006 |
|---|---|
| **Name** | TIM Security |
| **Description** | TIM shall be developed based on security requirements related to access control, personal data processing, and external attack risk reduction. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Collection and Extraction Module No. 11<br>CTI Correlation and Sharing Module No. 6, 10 |
| **Dependency** | TIM_NFR_003, TIM_NFR_005 |

| ID | TIM_NFR_007 |
|---|---|
| **Name** | TIM Portability |
| **Description** | TIM should be portable. Therefore, TIM can operate without any issues on different Operating Systems (OS). |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Collection and Extraction Module No. 4 (4.1, 4.2, 4.3, 4.4, 4.5) |
| **Dependency** | - |

| ID | TIM_NFR_008 |
|---|---|
| **Name** | TIM Response Time |
| **Description** | TIM GUI and API must respond within reasonable timeframe. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Collection and Extraction Module No. 1 (1.3), 2, 6 (6.2) |
| **Dependency** | - |

### 4.1.1. Interoperability Layer

#### Functional Requirements

| ID | SEIPL_FR_001 |
|---|---|
| **Name** | IPL TVIA data collection |
| **Description** | Secant platform offers an interoperability layer (IPL) to enable the communication channels for storing data collected by TVIA component. The data collected will be after used by the TIM, TAM and CO-CRAE components in order to be analysed. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - |

| ID | SEIPL_FR_002 |
|---|---|
| **Name** | IPL HVA data collection |
| **Description** | Secant platform offers interoperability layer (IPL) to enable the communication channels for storing data collected by HVA component. The data collected will be after used by the TIM, TAM and CO-CRAE components in order to be analysed. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - |

| ID | SEIPL_FR_003 |
|---|---|
| **Name** | IPL devices communication status collection |
| **Description** | The interoperability layer (IPL) will receive data collected by the pilot devices. The devices will inform the SECANT platform, through IPL about the communication healthy status between the mobile device from ambulance and the services from hospital. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - SEIPL_FR_006 |

| ID | SEIPL_FR_004 |
|---|---|
| **Name** | IPL repositories communication status collection |
| **Description** | The interoperability layer (IPL) will receive data collected by the pilot repositories. The repositories will inform the SECANT platform, through IPL about the communication healthy status between a repository service from a hospital and a different repository service from a different hospital. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - SEIPL_FR_006 |

| ID | SEIPL_FR_005 |
|---|---|
| **Name** | IPL data authentication, authorization, and validation |
| **Description** | The interoperability layer (IPL) will authenticate and authorize all the requests received from other components, using the DID integration. The IPL also will validate the payload content of the data received. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - Decentralized Digital Identity Management Module No. 1, 2 (2.4, 2.5) |
| **Dependency** | - |

| ID | SEIPL_FR_006 |
|---|---|
| **Name** | IPL main data storage |
| **Description** | The interoperability layer component will be the main storage component of the SECANT platform, using a database storage server. The stored data will be later consumed by the SECANT components. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | -SEIPL_FR_005 |

| ID | SEIPL_FR_007 |
|---|---|
| **Name** | IPL sharing stored data between components |
| **Description** | The interoperability layer component will provide a sharing mechanism of the collected and exported data between the SECANT components, through dedicated service that will expose appropriate endpoints. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | -SEIPL_FR_006 |

| ID | SEIPL_FR_008 |
|---|---|
| **Name** | IPL orchestrator |
| **Description** | It is possible that the IPL component to contain an orchestrator service, that will manage the intelligence and the policy engine. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | -SEIPL_FR_006 |

### Non-Functional Requirements

| ID | SEIPL_NFR_001 |
|---|---|
| **Name** | IPL must allow scalability and modularity |
| **Description** | Due to the management of many data are and devices, modularity and scalability of component integrations required so that the error rate is reduced, allowing the system to be efficient and available. |
| **Priority** | Should have |
| **Relevant User Requirement(s)** | |
| **Dependency** | - |

| ID | SEIPL_NFR_002 |
|---|---|
| **Name** | IPL sharing stored data through REST HTTP |
| **Description** | IPL repository service will provide sharing mechanism of collected and exported data, between the components by exporting HTTP REST endpoints |
| **Priority** | Should have |
| **Relevant User Requirement(s)** | |
| **Dependency** | - |

| ID | SEIPL_NFR_003 |
|---|---|
| **Name** | IPL sharing stored data through Pub/Sub |
| **Description** | IPL repository service will provide sharing mechanism of collected and exported data, between the components by exporting Pub/Sub connections |
| **Priority** | Should have |
| **Relevant User Requirement(s)** | |
| **Dependency** | - |

## 4.2. Cyber Security Risk Assessment Companion

### 4.2.1. Connected Organisations Cyber Risk Assessment Engine

#### Functional Requirements

| ID | CO-CRAE_FR_001 |
|---|---|
| **Name** | Real-time input on Vulnerabilities and Threats |
| **Description** | The cyber risk assessment should be able to receive real-time input on the identified threats, attacks, and vulnerabilities of the system from deployed vulnerability scanners, intrusion-detection systems, etc. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Connected Organizations Cyber Risk Assessment Engine (CO-CRAE) No. 1 (1.1, 1.4), 5 (5.5), 6 (6.2) |
| **Dependency** | - |

| ID | CO-CRAE_FR_002 |
|---|---|
| **Name** | CTI data and threat models |
| **Description** | The cyber risk assessment should be able to receive cyber-threat intelligence data and threat models based on the real-time assessment of the network |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Connected Organizations Cyber Risk Assessment Engine (CO-CRAE) No. 1 (1.1, 1.4), 3, 4, 5 (5.1, 5.2, 5.3, 5.4, 5.5) 6 (6.2) |
| **Dependency** | CO-CRAE_FR_001 |

| ID | CO-CRAE_FR_003 |
|---|---|
| **Name** | ICT ecosystem information |
| **Description** | The cyber risk assessment should be able to receive information on the ICT ecosystem information, including a catalogue of assets, their characteristics (operating system, version, etc.), the network cartography, topology, and the dependencies between them. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Connected Organizations Cyber Risk Assessment Engine (CO-CRAE) No.6 (6.2, 6.3) |
| **Dependency** | - |

| ID | CO-CRAE_FR_004 |
|---|---|
| **Name** | CVSS about known vulnerabilities |
| **Description** | The cyber risk assessment should be constantly updated with the latest identified CVEs by leveraging information from the US National Vulnerability Database, using the CPE Dictionary naming convention for information technology systems, packages, and software. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Connected Organizations Cyber Risk Assessment Engine (CO-CRAE) No. 1(1.1, 1.3), 3, 5 (5.1, 5.2, 5.3) 6(6.4) |
| **Dependency** | CO-CRAE_FR_002 |

| ID | CO-CRAE_FR_005 |
|---|---|
| **Name** | Asset interdependencies |
| **Description** | The SECANT risk assessment methodology should adequately address all the asset interdependencies comprising the envisioned use case ecosystems, so the possibility that a vulnerability of any particular asset does not compromise the security and overall trustworthiness of other assets that are defined by security relationships with the asset where the vulnerability is present, thus of the entire ecosystem. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Connected Organizations Cyber Risk Assessment Engine (CO-CRAE) No. 3, 4 |
| **Dependency** | CO-CRAE_FR_003 |

| ID | CO-CRAE_FR_006 |
|---|---|
| **Name** | User Authentication |
| **Description** | The risk assessment should be able to connect to the identity manager to enable the user authentication in a secure way. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Connected Organizations Cyber Risk Assessment Engine (CO-CRAE) No. 6 (6.4) |
| **Dependency** | CO-CRAE_FR_003 |

## Non-Functional Requirements

| ID | CO-CRAE_NFR_001 |
|---|---|
| **Name** | Rigorousness of risk assessment methodology |
| **Description** | The SECANT risk assessment methodology should be based on a rigorous, rational approach that produces high quality scientific and experimental based proofs and findings, indicators, and recommendations. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Connected Organizations Cyber Risk Assessment Engine (CO-CRAE) No. 1(1.1, 1.2, 1.3), 2, 3, 4, 5 (5.1, 5.2, 5.3) |
| **Dependency** | - |

| ID | CO-CRAE_NFR_002 |
|---|---|
| **Name** | Completeness and up-to-dateness of risk assessment methodology |
| **Description** | The SECANT risk assessment methodology should adequately address the cyber-threats dictated by the considered threat landscape, following the latest identified and most prominent threats [55], as the mapping and crawling functionality implemented in SECANT makes the consideration of the most up-to-date knowledge regarding cybersecurity of paramount importance. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Connected Organizations Cyber Risk Assessment Engine (CO-CRAE) No. 1 (1.1, 1.2, 1.3), 3, 4, 5 (5.1, 5.2, 5.3), 6 (6.3) |
| **Dependency** | CO-CRAE_NFR_001 |

| ID | CO-CRAE_NFR_003 |
|---|---|
| **Name** | Adaptability to use case requirements |
| **Description** | It should be ensured that the threats and vulnerabilities identified by the risk assessment methodology employed by SECANT accurately represent the risks and dangers that are most relevant to each use case, while ensuring the overall trustworthiness of the systems operated by the use case partners is not compromised. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Connected Organizations Cyber Risk Assessment Engine (CO-CRAE) No. 1 (1.1, 1.2), 2, 3, 4, 6(6.4) |
| **Dependency** | CO-CRAE_NFR_001 |

| ID | CO-CRAE_NFR_004 |
|---|---|
| **Name** | Privacy preservation |
| **Description** | The SECANT risk assessment system should not compromise the security and privacy requirements posed by the envisioned use cases and should not compromise the privacy guarantees provided by the components of the SECANT ecosystem, including the user privacy guarantees provided by the relevant employed methodologies. The system should guarantee compliance with GDPR. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Connected Organizations Cyber Risk Assessment Engine (CO-CRAE) No. 2, 3, 4, 6(6.4) |
| **Dependency** | CO-CRAE_NFR_001, CO-CRAE_NFR_003 |

| ID | CO-CRAE_NFR_005 |
|---|---|
| **Name** | Availability |
| **Description** | The SECANT risk assessment system shall ensure availability of at least 97% uptime. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | CO-CRAE_NFR_001 |

### 4.2.2. OpenUEBA: Open Source User and Entity Behaviour Analytics Engine

#### Functional Requirements

| ID | OpenUEBA_FR_001 |
|---|---|
| **Name** | Real-time input on Vulnerabilities and Threats |
| **Description** | The CSRAC should be able to receive real-time input on the identified threats, attacks, and vulnerabilities of the system from deployed vulnerability scanners, intrusion-detection systems, etc. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | OpenUEBA: Open Source User and Entity Behaviour Analytics Engine No. 1 |
| **Dependency** | - |

| ID | OpenUEBA_FR_002 |
|---|---|
| **Name** | CTI data and threat models |
| **Description** | The CSRAC should be able to receive cyber-threat intelligence data and threat models based on the real-time assessment of the network |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | OpenUAEBA_FR_001 |

| ID | OpenUEBA_FR_003 |
|---|---|
| **Name** | ICT ecosystem information |
| **Description** | The CSRAC should be able to receive information on the ICT ecosystem information, including a catalogue of assets, their characteristics (operating system, version, etc.), the network cartography, topology, and the dependencies between them. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | OpenUAEBA_FR_001, OpenUAEBA_FR_002 |

| ID | OpenUEBA_FR_004 |
|---|---|
| **Name** | CVSS about known vulnerabilities |
| **Description** | The CSRAC should be constantly updated with the latest identified CVEs by leveraging information from the US National Vulnerability Database, using the CPE Dictionary naming convention for information technology systems, packages, and software. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | OpenUAEBA_FR_002 |

| ID | OpenUEBA_FR_005 |
|---|---|
| **Name** | Asset interdependencies |
| **Description** | The CSRAC methodology should adequately address all the asset interdependencies comprising the envisioned use case ecosystems, so the possibility that a vulnerability of any particular asset does not compromise the security and overall trustworthiness of other assets that are defined by security relationships with the asset where the vulnerability is present, thus of the entire ecosystem. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | OpenUAEBA_FR_003 |

| ID | OpenUEBA_FR_006 |
|---|---|
| **Name** | User Authentication |
| **Description** | The CSRAC should be able to connect to the identity manager to enable the user authentication in a secure way. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | OpenUEBA: Open-Source User and Entity Behaviour Analytics Engine 2, 4, 5 |
| **Dependency** | OpenUAEBA_FR_003 |

#### Non-Functional Requirements

| ID | OpenUEBA_NFR_001 |
|---|---|
| **Name** | Availability |
| **Description** | The SECANT risk assessment system shall ensure availability of at least 97% uptime. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | CO-CRAE_NFR_001 |

| ID | OpenUEBA_NFR_002 |
|---|---|
| **Name** | Usability |
| **Description** | The risk assessment system shall ensure availability of at least 97% uptime. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | CO-CRAE_NFR-001 |

### 4.2.3. Technical and Impact Vulnerability Assessment

#### Functional Requirements

| ID | TVIA_FR_001 |
|---|---|
| **Name** | TVIA shall retrieve the list of connected entities from a discovery service. |
| **Description** | The TVIA performs assessment on network entities. For that, it needs to know which entities are connected. For this purpose, the TVIA module queries a discovery service to retrieve the list of connected network entities. |
| **Priority** | Must Have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - |

| ID | TVIA_FR_002 |
|---|---|
| **Name** | TVIA shall perform a vulnerability assessment in networked entities. |
| **Description** | The TVIA assesses non-assessed network entities the moment they are discovered, and periodically re-assesses existing ones against cyber security vulnerabilities, to determine their CVSS score and compile a detailed list of discovered vulnerabilities. |
| **Priority** | Must Have |
| **Relevant User Requirement(s)** | Technical and Impact Vulnerability Assessment & Human Vulnerability Assessment tools 3 (3.2) |
| **Dependency** | TVIA_FR_001 |

| ID | TVIA_FR_003 |
|---|---|
| **Name** | TVIA shall produce a CVSS score and a report depicting the entities' vulnerability status. |
| **Description** | As a result of the assessment operation, the TVIA outputs a score depicting the entity's vulnerability status, based on a standardized scoring system (CVSS v3 [56]). TVIA also produces a detailed assessment report in a structured format (e.g., JSON). |
| **Priority** | Must Have |
| **Relevant User Requirement(s)** | Technical and Impact Vulnerability Assessment & Human Vulnerability Assessment tools 1(1.5, 1.6) |
| **Dependency** | TVIA_FR_002 |

| ID | TVIA_FR_004 |
|---|---|
| **Name** | TVIA should retrieve threat intelligence from a Threat Intelligence Module |
| **Description** | TVIA should retrieve threat intelligence information, to enrich its assessment results. This information should be retrieved from an external component (e.g., TIM). |
| **Priority** | Should Have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - |

### Non-Functional Requirements

| ID | TVIA_NFR_001 |
|---|---|
| **Name** | Availability |
| **Description** | The TVIA shall ensure availability of at least 97% uptime. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - |

## 4.2.4. Human Vulnerability Assessment tools

### Functional Requirements

| ID | HVA_FR_001 |
|---|---|
| **Name** | HVA shall retrieve SECANT users' information |
| **Description** | The HVA component shall retrieve the list of users and their relevant information (e.g., email, department, etc.) from an external component (e.g., Identity Manager) |
| **Priority** | Should Have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - |

| ID | HVA_FR_002 |
|---|---|
| **Name** | HVA shall send specific questionnaires to users |
| **Description** | The HVA component shall send specific weighted questionnaires in a digital form (e.g., google forms) to users, to assess their vulnerability status |
| **Priority** | Must Have |
| **Relevant User Requirement(s)** | Technical and Impact Vulnerability Assessment & Human Vulnerability Assessment tools 3 (3.1) |
| **Dependency** | - |

| ID | HVA_FR_003 |
|---|---|
| **Name** | HVA shall produce Human Vulnerability Assessment reports |
| **Description** | The HVA component shall produce vulnerability assessment reports periodically, based on the derived results of the acquired questionnaires. |
| **Priority** | Must Have |
| **Relevant User Requirement(s)** | Technical and Impact Vulnerability Assessment & Human Vulnerability Assessment tools 3 (3.1) |
| **Dependency** | HVA_FR_002 |

## Non-Functional Requirements

| ID | HVA_NFR_001 |
|---|---|
| **Name** | Availability |
| **Description** | The HVA shall ensure availability of at least 97% uptime. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - |

| ID | HVA_NFR_002 |
|---|---|
| **Name** | Theoretical background |
| **Description** | The HVA should build upon robust theoretical background |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Technical and Impact Vulnerability Assessment & Human Vulnerability Assessment tools 2 (2.1) |
| **Dependency** | - |

| ID | HVA_NFR_003 |
|---|---|
| **Name** | GDPR compliant |
| **Description** | The HVA should have GDPR compliant data management and reporting |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Technical and Impact Vulnerability Assessment & Human Vulnerability Assessment tools 2 (2.2) |
| **Dependency** | - |

## 4.3. Cyber Security Training Module

### 4.3.1. Cyber Range

#### Functional Requirements

| ID | CR_FR_001 |
|---|---|
| **Name** | Infrastructure configuration |
| **Description** | The Cyber Range must be able to precisely define the topology and to enforce the configuration files in any devices of the simulated infrastructure. It must be able to precisely define the network parameters of the links and switches. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Cyber range No 1 |
| **Dependency** | - |

| ID | CR_FR_002 |
|---|---|
| **Name** | Training visualisation |
| **Description** | The Cyber Range must have the capability to show what is happening during a training session by showing the traffic exchanged between the nodes and giving access to any devices of the simulated infrastructure. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Cyber range No 3 |
| **Dependency** | - |

| ID | CR_FR_003 |
|---|---|
| **Name** | Scenario creation and run |
| **Description** | The Cyber Range must have the capability to define and create scenarios and run it to simulate a complex malicious activity. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Cyber range No 3 |
| **Dependency** | - |

#### Non-Functional Requirements

| ID | CR_NFR_001 |
|---|---|
| **Name** | Cyber range security |
| **Description** | The Cyber Range must restrict the cyber activities inside the Cyber Range and not propagate the malicious activities outside the Cyber Range, i.e., in the stakeholder infrastructure. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - |

| ID | CR-NFR-002 |
|---|---|
| **Name** | Cyber range reliability |
| **Description** | The Cyber range should be able to handle an intensive activity to recreate malicious activity relying on intensive request like DDoS. |
| **Priority** | Should have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - |

| ID | CR-NFR-003 |
|---|---|
| **Name** | Cyber range scalability |
| **Description** | The cyber range must be able to simulate topology for up to one hundred nodes. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - |

### 4.3.2. Cyber Security Training Module with Chatbot

#### Functional Requirements

| ID | CSTM_FR_001 |
|---|---|
| **Name** | Security training initiation |
| **Description** | The health professional/client (patient) should be able to start a new security training assessment, to assess their security awareness. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Cyber Security Training Module with Chatbot No. 2 (2.5) |
| **Dependency** | - |

| ID | CSTM_FR_002 |
|---|---|
| **Name** | Chatbot response |
| **Description** | The chatbot should be able to accept the users' answers to the question asked and handle different types of answers. In case the user answers correctly the flow continues to the next question. In any other case the chatbot should repeat the question and prompt the user for a new answer. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Cyber Security Training Module with Chatbot No. 2 (2.4) |
| **Dependency** | - |

| ID | CSTM_FR_003 |
|---|---|
| **Name** | Chatbot question retrieval |
| **Description** | The chatbot should be able to receive all the security training assessment questions from a JSON file. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Cyber Security Training Module with Chatbot No. 2 (2.3) |
| **Dependency** | CSTM_FR_002 |

| ID | CSTM_FR_004 |
|---|---|
| **Name** | Chatbot question selection |
| **Description** | The chatbot should be able to randomly select up to 10 questions from the training assessment questions and serve them to the health professional/ client (patient). [easy-medium-difficult-very difficult ranking on the questions] |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Cyber Security Training Module with Chatbot No. 1, 2 (2.3, 2.4, 2.5, 2.6) |
| **Dependency** | CSTM_FR_003 |

| ID | CSTM_FR_005 |
|---|---|
| **Name** | Chatbot question delivery |
| **Description** | The chatbot should be able to display the following types of questions:<br>1. The question can be sent as a rich text message<br>2. The question can be sent as an image having accompanying text<br>3. The question can be sent as a message in a select button. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Cyber Security Training Module with Chatbot No. 2 (2.4) |
| **Dependency** | CSTM_FR_003, CSTM_FR_004 |

| ID | CSTM_FR_006 |
|---|---|
| **Name** | Chatbot answer selection |
| **Description** | The health professional/ client(patient) should be able to respond to the chatbot's questions by:<br>• Uploading multimedia files<br>• Choosing one or multiple answers from a multiple-choice question served as buttons<br>• Typing comma separated keywords |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Cyber Security Training Module with Chatbot No. 2 (2.4) |
| **Dependency** | CSTM_FR_005 |

| ID | CSTM_FR_007 |
|---|---|
| **Name** | Chatbot answer validation |
| **Description** | The chatbot should be able to provide the health professional/ client(patient) with feedback according to their answer to the questions.<br>• For questions answered by buttons, assessment should be automated<br>• For other types of question assessment should be manual |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Cyber Security Training Module with Chatbot No. 2 (2.4) |
| **Dependency** | CSTM_FR_006 |

| ID | CSTM_FR_008 |
|---|---|
| **Name** | Chatbot wrong answer feedback |
| **Description** | In case of false answers, the chatbot should be able to provide the health professional/ client (patient) with a link to additional training material. |
| **Priority** | Should have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | CSTM_FR_007 |

| ID | CSTM_FR_009 |
|---|---|
| **Name** | Chatbot assessment scoring |
| **Description** | The chatbot should be able to score the health professional/client (patient) based on their assessment results. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | CSTM_FR_007 |

| ID | CSTM_FR_010 |
|---|---|
| **Name** | Chatbot result communication |
| **Description** | The chatbot should be able to send the scores of the health professional's/client's (patient's) assessment, to the SECANT End-User Application, via a REST API. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | SECANT End-User Application No. 1 (1.5) |
| **Dependency** | CSTM_FR_009 |

| ID | CSTM_FR_011 |
|---|---|
| **Name** | Chatbot training suggestions |
| **Description** | The chatbot should be able to communicate training topics based on the health professional's/client's (patient's) assessment score, by providing links to the SECANT End-User Application. |
| **Priority** | Should have |
| **Relevant User Requirement(s)** | SECANT End-User Application No. 1 (1.6) |
| **Dependency** | CSTM_FR_009 |

## Non-Functional Requirements

| ID | CSTM_NFR_001 |
|---|---|
| **Name** | CSTM with chatbot availability |
| **Description** | The CSTM with Chatbot shall ensure availability of at least 97% uptime. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - |

| ID | CSTM_NFR_002 |
|---|---|
| **Name** | CSTM with chatbot security |
| **Description** | The CSTM with Chatbot app should respect security requirements related to access control, personal data processing, and external attack risk reduction. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Cyber Security Training Module with Chatbot No. 2 (2.2) |
| **Dependency** | - |

| ID | CSTM_NFR_003 |
|---|---|
| **Name** | CSTM with chatbot privacy |
| **Description** | The CSTM with Chatbot should guarantee GDPR compliance. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Cyber Security Training Module with Chatbot No. 2 (2.1) |
| **Dependency** | - |

| ID | CSTM_NFR_004 |
|---|---|
| **Name** | CSTM with chatbot usability |
| **Description** | The CSTM with Chatbot should support accessibility features, allowing the health professional/client (patient) with accessibility needs to seamlessly interact with it. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Cyber Security Training Module with Chatbot No. 1 |
| **Dependency** | - |

## 4.4. Privacy, Accountability, and Identity Management

### 4.4.1. Trust and Accountability Module

**Functional Requirements**

| ID | TAM_FR_001 |
|---|---|
| **Name** | Encryption streams to control the ownership of the data |
| **Description** | Data streams kept on the encrypted channels with only specific Identities holding the right secret key able to decrypt and access it |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Trust and Accountability Module No.1, 3, 4, 7<br>Advance Privacy Toolkit No 1, 2 |
| **Dependency** | DIM_FR_012, PT_FR_002 |

| ID | TAM_FR_002 |
|---|---|
| **Name** | Mechanisms to provide data immutability with hashes from data streams kept on the blockchain |
| **Description** | Data integrity must be ensured with the blockchain but ensuring that hash (from metadata) of the data kept in the Stream is successfully kept on the blockchain (Tangle) |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Trust and Accountability Module No.1, 4, 5, 7<br>Advance Privacy Toolkit No. 1 |
| **Dependency** | *TAM_FR_001* |

| ID | TAM_FR_003 |
|---|---|
| **Name** | Create secure decentralized identities with data anchored on the blockchain (Tangle) |
| **Description** | Creation of identities for the devices, components, and other entities for secure identification in the SECANT |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Trust and Accountability Module No.1, 3, 4, 7<br>Decentralized Identity Module No. 1, 2.3 |
| **Dependency** | DIM_FR_007, DIM_FR_008, DIM_FR_009, DIM_FR_010 |

| ID | TAM_FR_004 |
|---|---|
| **Name** | Create anonymous credentials for users to preserve privacy of personal data (attributes) by allowing sequential access to the data |
| **Description** | Creation of verifiable credentials mechanisms based on zero-knowledge proof and encryption mechanisms that will ensure only access to the part of verifiable credentials |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Trust and Accountability Module No.1, 3, 4, 7<br>Decentralized Identity Module No. 2 (2.2) |
| **Dependency** | DIM_FR_007, DIM_FR_008, DIM_FR_009, DIM_FR_010 |

**Non-Functional Requirements**

| ID | TAM_NFR_001 |
|---|---|
| **Name** | GDPR compliance of the data |
| **Description** | Data added in the TAM module must follow GDPR relevant technological procedures to make all data saved compliant:<br>- Hash of the data in the blockchain which are made from non-anonymized data must not contain personal data<br>- Permissioned blockchain should be used to avoid having the hash on the public ledger |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Trust and Accountability Module No.1, 3, 4, 7 |
| **Dependency** | TAM_FR_001, TAM_FR_002, TAM_FR_003 |

### 4.4.2. Advance Privacy Toolkit

**Functional Requirements**

| ID | PT_FR_001 |
|---|---|
| **Name** | Fine-grained data access control |
| **Description** | The privacy toolkit should be able to define access policies for healthcare data so that it could be only accessed by authorized parties. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Advanced Privacy Toolkit No. 1, 2 (2.1, 2.2, 2.6, 2.7, 2.8) |
| **Dependency** | PT_FR_002, TAM_FR_001, TAM_FR_002 |

| ID | PT_FR_002 |
|---|---|
| **Name** | Searchability over encrypted data |
| **Description** | The privacy toolkit should be able to allow data users to search over healthcare data in an encrypted form by keywords |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Advanced Privacy Toolkit No. 1, 2 (2.1, 2.2, 2.3, 2.6) |
| **Dependency** | PT_FR_001, TAM_FR_001, TAM_FR_002 |

| ID | PT_FR_003 |
|---|---|
| **Name** | Password protection |
| **Description** | The privacy toolkit should be able to protect the security of the login passwords, especially against brute-force attacks. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Advanced Privacy Toolkit No. 1, 2 (2.1, 2.2, 2.3, 2.6) |
| **Dependency** | PT_FR_001, PT_FR_002, TAM_FR_001, TAM_FR_002 |

#### Non-Functional Requirements

| ID | PT_NFR_001 |
|---|---|
| **Name** | GDPR compliance of the data |
| **Description** | Data used in the Privacy Toolkit must follow GDPR relevant technological procedures:<br>• The data used for the advanced hybrid encryption schemes must not contain personal data.<br>• The data used for the password authentication and honey encryption must not contain personal data. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Advanced Privacy Toolkit No. 1, 2 (2.1, 2.2, 2.3, 2.6) |
| **Dependency** | PT_FR_001, PT_FR_002, PT_FR_003 |

### 4.4.3. Decentralized Digital Identity Management Module

#### Functional Requirements

| ID | DIM_FR_001 |
|---|---|
| **Name** | Identity Provider |
| **Description** | The DIM module must include a digitalized portal, this will be the regulatory entity in which will provide and manage identities. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 1 |
| **Dependency** | - |

| ID | DIM_FR_002 |
|---|---|
| **Name** | Wallet |
| **Description** | The DIM module wants to give users the ability to access and manage their credentials through a wallet. The Wallet will be the access point and main communication trail for the users. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 2 (2.1) |
| **Dependency** | DIM_FR_001 |

| ID | DIM_FR_003 |
|---|---|
| **Name** | Connection Wallet- Identity provider |
| **Description** | The DIM module must implement a function to insure the communication between the wallet, in our case the Wallet, and the identity provider. In this function we must manage the ability to send and receive credentials. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 2 (2.1) |
| **Dependency** | DIM_FR_002 |

| ID | DIM_FR_004 |
|---|---|
| **Name** | Connection Identity Provider-Tangle |
| **Description** | The DIM module must have a secure connection between the Identity Provider and the Tangle. This must provide the users with a secure communication route to send and receive DID between these two modules. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 2 (2.3) |
| **Dependency** | DIM_FR_001 |

| ID | DIM_FR_005 |
|---|---|
| **Name** | Connection TAM-DIM |
| **Description** | The DIM module will contain two different modules, Trust, and Accountability Module (TAM) and Decentralized Digital Identity Management Module, which will have to communicate with a secure and proper procedure |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 2 (2.4) |
| **Dependency** | - |

| ID | DIM_FR_006 |
|---|---|
| **Name** | DIM Interconnection |
| **Description** | The DIM module will ensure interoperability between different tools. We must guarantee that communication between the DIM and the other components is done correctly and in a secure way. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 2 (2.4) |
| **Dependency** | - |

| ID | DIM_FR_007 |
|---|---|
| **Name** | Creation and management of credentials |
| **Description** | The DIM module must implement a function to properly register and administrate the credentials in the Tangle |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 2 (2.2) |
| **Dependency** | DIM_FR_002 |

| ID | DIM_FR_008 |
|---|---|
| **Name** | Revoke of credentials |
| **Description** | The DIM module needs to have the ability to update specific credentials already inside the Tangle, and be able to revise the information in it without tempering with the credential history |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 2 (2.5) |
| **Dependency** | DIM_FR_002 |

| ID | DIM_FR_009 |
|---|---|
| **Name** | Verification of credentials |
| **Description** | The DIM module must have a function in which we can corroborate the credentials, ensuring the integrity and validity of this information with the Tangle. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 2 (2.6) |
| **Dependency** | DIM_FR_002 |

| ID | DIM_FR_010 |
|---|---|
| **Name** | Share credentials |
| **Description** | The DIM module must implement a method of sharing credentials through the Tangle, also granting access to the recipient. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 2 (2.3) |
| **Dependency** | DIM_FR_002 |

| ID | DIM_FR_011 |
|---|---|
| **Name** | Identity traceability |
| **Description** | The DIM module wants to ensure that users can track their information inside the Tangle. We want to provide a way of checking set history and follow all changes of our identity. |
| **Priority** | Should have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 2 (2.7) |
| **Dependency** | DIM_FR_001, DIM_FR_002, DIM_FR_003 |

| ID | DIM_FR_012 |
|---|---|
| **Name** | Role management |
| **Description** | The DIM module needs to manage the different roles of actors that we have on the system, giving authorization to manage the permissions only to certain actors. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 1 |
| **Dependency** | - |

| ID | DIM_FR_013 |
|---|---|
| **Name** | Permission management |
| **Description** | The DIM module integrates sharing credentials, this implies that the identity must have attributes that will come in play when giving other actors authorization to check certain information. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 2 (2.5) |
| **Dependency** | - |

| ID | DIM_FR_014 |
|---|---|
| **Name** | DIM module availability |
| **Description** | The DIM module Have the capability to handle and process the data produced by many devices and services, maintaining adequate quality of service (this capability cannot affect the normal operations of devices and services). |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 2 (2.4) |
| **Dependency** | DIM_FR_001, DIM_FR_002 |

| ID | DIM_FR_015 |
|---|---|
| **Name** | Authentication function |
| **Description** | The DIM module must have a function in which we verify the identity of the respective actor who wants to have access to the Tangle, giving them permission to communicate with the Tangle. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 1 |
| **Dependency** | DIM_FR_001 |

| ID | DIM_FR_016 |
|---|---|
| **Name** | Credential storage |
| **Description** | The DIM module will manage credentials and identities from an unknown number of users, this means that we need a storage solution with proper and plentiful capacity for storing credential in the DID document. |
| **Priority** | Should have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 2 (2.1) |
| **Dependency** | - |

## Non-Functional Requirements

| ID | DIM_NFR_001 |
|---|---|
| **Name** | GDPR compliance |
| **Description** | The DIM module must follow the GDPR regulation, meaning that the identity structures must comply with the GDPR regulation |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 1, 2 (2.1, 2.5, 2.6) |
| **Dependency** | - |

| ID | DIM_NFR_002 |
|---|---|
| **Name** | W3C compliance |
| **Description** | The DIM module must follow the W3C Standard, meaning that the identity structures must comply with the W3C Standard |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 2 (2.2) |
| **Dependency** | - |

| ID | DIM_NFR_003 |
|---|---|
| **Name** | eIDAS compliance |
| **Description** | The DIM module could follow the eIDAS regulation, meaning that the identity structures should comply with the eIDAS regulation |
| **Priority** | Could have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 2 (2.1) |
| **Dependency** | - |

| ID | DIM_NFR_004 |
|---|---|
| **Name** | Identity persistence |
| **Description** | In the DIM module the information must be persistent, unable to be deleted or tampered with by no authorized actors. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 2 (2.5) |
| **Dependency** | DIM_FR_001, DIM_FR_003 |

| ID | DIM_NFR_005 |
|---|---|
| **Name** | Identity integrity |
| **Description** | The DIM module's main objective is to security manage credentials and identities; therefore, we need to ensure that unauthorized actors cannot access or manipulate information of other users |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 2 (2.1) |
| **Dependency** | DIM_FR_001, DIM_FR_003 |

| ID | DIM_NFR_006 |
|---|---|
| **Name** | User Privacy |
| **Description** | In the DIM module, the privacy of all users must be ensured as sensitive data is being processed. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 2 (2.6) |
| **Dependency** | DIM_FR_001, DIM_FR_003 |

### 4.4.4. SECANT API

#### Functional Requirements

| ID | SEAPI_FR_001 |
|---|---|
| **Name** | The API must allow the distribution of data through communication channels in a secure format. |
| **Description** | To communicate effectively, components require a secure, account-based communication path with access roles through which data can be transmitted in well-defined formats. This will make data integrity and error prevention possible. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Trust and Accountability Module No. 7<br>Advanced Privacy Toolkit No. 1, 2 (2.1, 2.2, 2.6)<br>Decentralized Digital Identity Management Module No. 1, 2 (2.4, 2.5) |
| **Dependency** | SEAPI_FR_002 |

| ID | SEAPI_FR_002 |
|---|---|
| **Name** | The API must enable data access through an authentication system. |
| **Description** | To access the data, a component needs a set of credentials and certifications that authorize both access to the platform and to communicate with other components and devices. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Advanced Privacy Toolkit No. 2 (2.4)<br>Decentralized Digital Identity Management Module No. 1, 2 (2.2, 2.6) |
| **Dependency** | - |

| ID | SEAPI_FR_003 |
|---|---|
| **Name** | The API must allow retrieval of information access to services. |
| **Description** | The API must allow role-based access so that each role has certain services or features that can be used. Based on this, the API must be able to inform the user about the roles and information associated with the account. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Advanced Privacy Toolkit No. 2 (2.2, 2.4) |
| **Dependency** | SEAPI_FR_002 |

**Non-Functional Requirements**

| ID | SEAPI_NFR_001 |
|---|---|
| **Name** | The API shall present the imported data in an expressive metadata format. |
| **Description** | Imported data must be presented in a rigorous and clear format, which can be accessed from a single place through modern mechanisms that can help document the endpoints. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Collection and Extraction Module No. 1 (1.4), 5 (5.1) |
| **Dependency** | - |

## 4.5. Dashboard, End-User Application

### 4.5.1. SECANT Dashboard for Security Professionals

**Functional Requirements**

| ID | SDSP_FR_001 |
|---|---|
| **Name** | SECANT Dashboard registration |
| **Description** | The SECANT Dashboard must provide user registration functionalities to security professionals. The registration requests will be reviewed by the platform administrator. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | SECANT Dashboard No. 3 (3.4) |
| **Dependency** | - |

| ID | SDSP_FR_002 |
|---|---|
| **Name** | SECANT Dashboard sign in |
| **Description** | The SECANT Dashboard must provide user and admin sign-in functionalities. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | SECANT Dashboard No. 3 (3.4) |
| **Dependency** | SDSP_FR_001 |

| ID | SDSP_FR_003 |
|---|---|
| **Name** | SECANT Dashboard Role-Based Access Policy |
| **Description** | The SECANT Dashboard must provide and ensure Role-Based Access to the SECANT backbone services. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | SECANT Dashboard No. 3 (3.4) |
| **Dependency** | SDSP_FR_002 |

| ID | SDSP_FR_004 |
|---|---|
| **Name** | List with identified threats and vulnerabilities |
| **Description** | The SECANT Dashboard must be able to interact with the Threat Intelligent Module to retrieve and present a complete list of identified threats and vulnerabilities. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | SECANT Dashboard No. 3 (3.1, 3.2) |
| **Dependency** | - |

| ID | SDSP_FR_005 |
|---|---|
| **Name** | Inspect identified threats and vulnerabilities |
| **Description** | The SECANT Dashboard must be able to allow users to select and inspect specific threats/vulnerabilities, retrieving details about their impact as they propagate through the ICT ecosystem. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | SECANT Dashboard No. 1, 2, 3 (3.1, 3.2) |
| **Dependency** | SDSP_FR_004 |

| ID | SDSP_FR_006 |
|---|---|
| **Name** | Access to the Organizational Cyber Range |
| **Description** | The SECANT Dashboard must be able to explore and interact with the Organizational Cyber Range (OCR). |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - |

| ID | SDSP_FR_007 |
|---|---|
| **Name** | SECANT Dashboard Visualizations |
| **Description** | The SECANT Dashboard should be able to create and provide multiple visualizations based on the collected information from the SECANT backbone services. |
| **Priority** | Should have |
| **Relevant User Requirement(s)** | SECANT Dashboard No. 1, 2, 3 (3.3) |
| **Dependency** | SDSP_FR_004 |

| ID | SDSP_FR_008 |
|---|---|
| **Name** | SECANT Dashboard Alerts |
| **Description** | The SECANT Dashboard should support pop-up notifications about aggregated alerts coming from the SECANT backbone services. |
| **Priority** | Should have |
| **Relevant User Requirement(s)** | SECANT Dashboard No. 3 (3.1, 3.2) |
| **Dependency** | SDSP_FR_004 |

| ID | SDSP_FR_009 |
|---|---|
| **Name** | SECANT Dashboard Subscriptions |
| **Description** | The SECANT Dashboard should allow security professionals to subscribe to incoming notifications and alerts. |
| **Priority** | Should have |
| **Relevant User Requirement(s)** | SECANT Dashboard No. 3 (3.4) |
| **Dependency** | SDSP_FR_001, SDSP_FR_002, SDSP_FR_003 |

| ID | SDSP_FR_010 |
|---|---|
| **Name** | SECANT Dashboard Encrypted and Trusted Communication |
| **Description** | The SECANT Dashboard must support encrypted and trusted communication with security professionals, using HTTPS/TLS protocol and trusted certificates. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - |

### Non-Functional Requirements

| ID | SDSP_NFR_001 |
|---|---|
| **Name** | SECANT Dashboard common UI/UX Language |
| **Description** | The SECANT Dashboard should be able to create and provide a common UI/UX language for security experts (CERTs/ CSIRTs) that are not familiar with the complex ICT infrastructure specificities. |
| **Priority** | Should have |
| **Relevant User Requirement(s)** | SECANT Dashboard No. 3(3.5) |
| **Dependency** | - |

| ID | SDSP_NFR_002 |
|---|---|
| **Name** | SECANT Dashboard availability |
| **Description** | The SECANT Dashboard must ensure availability of at least 99% uptime. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - |

| ID | SDSP_NFR_003 |
|---|---|
| **Name** | SECANT Dashboard privacy |
| **Description** | The SECANT Dashboard must ensure GDPR compliance. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | SDSP_FR_010 |

| ID | SDSP_NFR_004 |
|---|---|
| **Name** | SECANT Dashboard usability |
| **Description** | The SECANT Dashboard must provide a user-friendly and easily accessible graphical user interface. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | SECANT Dashboard No. 1, 2, 3 (3.3) |
| **Dependency** | SDSP_FR_007 |

| ID | SDSP_NFR_005 |
|---|---|
| **Name** | SECANT Dashboard guidance |
| **Description** | The SECANT Dashboard SHOULD provide a guidance/documentation page to assist security professionals interacting with it. |
| **Priority** | Should have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - |

### 4.5.2. SECANT End-User Application

#### Functional Requirements

| ID | SEUA_FR_001 |
|---|---|
| **Name** | SECANT End User Application sign up |
| **Description** | The health professional/ client(patient) should be able to sign up for the SECANT End User Application. |
| **Priority** | Should have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - |

| ID | SEUA_FR_002 |
|---|---|
| **Name** | SECANT End User Application log in |
| **Description** | The health professional/ client(patient) should be able to log in to the SECANT End User Application. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - |

| ID | SEUA_FR_003 |
|---|---|
| **Name** | SECANT End User Application personal information |
| **Description** | The health professional/ client(patient) should be able to view their personal information. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | SEUA_FR_002 |

| ID | SEUA_FR_004 |
|---|---|
| **Name** | SECANT End User Application log out |
| **Description** | The health professional/ client(patient) should be able to log out from the SECANT End User Application. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | SEUA_FR_002 |

| ID | SEUA_FR_005 |
|---|---|
| **Name** | SECANT End User Application account deletion |
| **Description** | The health professional/ client(patient) should be able to delete their account on the SECANT End User Application. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | SEUA_FR_001 |

| ID | SEUA_FR_006 |
|---|---|
| **Name** | SECANT End User Application sensitive data access |
| **Description** | The health professional/ client(patient) should be able to view their sensitive data coming from TAM. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - |

| ID | SEUA_FR_007 |
|---|---|
| **Name** | SECANT End User Application training access |
| **Description** | The health professional/ client(patient) should be able to be trained to raise their security awareness. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | SECANT End-User Application No. 1 (1.3, 1.4, 1.5, 1.6) |
| **Dependency** | - |

| ID | SEUA_FR_008 |
|---|---|
| **Name** | SECANT End User Application training score monitoring |
| **Description** | The health professional/ client(patient) should be able to view their score history from the cyber security training assessments via Chatbot to monitor their progress. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | SECANT End-User Application No. 1 (1.2) |
| **Dependency** | SEUA_FR_007, CSTM_FR_011 |

| ID | SEUA_FR_009 |
|---|---|
| **Name** | SECANT End User Application training assessment score ranking |
| **Description** | The health professional/ client(patient) should be able to view their security training assessment score rank in their organization. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | SECANT End-User Application No. 1 (1.5) |
| **Dependency** | SEUA_FR_008 |

## Non-Functional Requirements

| ID | SEUA_NFR_001 |
|---|---|
| **Name** | SECANT End User Application availability |
| **Description** | The SECANT End User Application shall ensure availability of at least 97% uptime. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - |

| ID | SEUA_NFR_002 |
|---|---|
| **Name** | SECANT End User Application security |
| **Description** | The SECANT End User Application shall be developed based on security requirements related to access control, personal data processing, and external attack risk reduction. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | SEUA_FR_001, SEUA_FR_002, SEUA_FR_003, SEUA_FR_004, SEUA_FR_005, SEUA_FR_006 |

| ID | SEUA_NFR_003 |
|---|---|
| **Name** | SECANT End User Application security |
| **Description** | The SECANT End User Application shall be developed based on security requirements related to access control, personal data processing, and external attack risk reduction. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | SEUA_FR_001, SEUA_FR_002, SEUA_FR_003, SEUA_FR_004, SEUA_FR_005, SEUA_FR_006 |

| ID | SEUA_NFR_004 |
|---|---|
| **Name** | SECANT End User Application privacy |
| **Description** | The SECANT End User Application shall guarantee GDPR compliance. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | SEUA_FR_006, SEUA_NFR_003 |

## 4.6. SECANT Platform

### Functional Requirements

| ID | SEPLT_FR_001 |
|---|---|
| **Name** | Provides support for cyber security risks |
| **Description** | The SECANT Platform shall identify possible attacks and threats, promoting the importance of cybersecurity awareness among users. It plays a decisive role in the resilience and readiness of organizations against infectious content and cyber threats to prevent future intrusions and data loss. The platform helps to share the information that has been collected from network traffic and transmit it to a database. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Collection and Extraction Module No. 1 (1.2)<br>CTI Correlation and Sharing Module No. 2 (2.1), 8<br>Connected Organizations Cyber Risk Assessment Engine (CO-CRAE) No. 4 |
| **Dependency** | TIM_FR_012 |

| ID | SEPLT_FR_002 |
|---|---|
| **Name** | Detection of advanced and modern cyber threats |
| **Description** | The SECANT Platform shall continuously monitor network traffic to detect the latest, most advanced, and modern cyber threats to protect data and increase privacy throughout the cyber ecosystem. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | CTI Collection and Extraction Module No. 1 (1.2), 9, 10<br>CTI Correlation and Sharing Module No. 1 (1.1)<br>Cyber Range No. 2 |
| **Dependency** | TIM_FR_006 |

| ID | SEPLT_FR_003 |
|---|---|
| **Name** | Platform authentication and authorization |
| **Description** | The SECANT Platform must prevent unauthorized access of users and clients by implementing an authorization and authentication mechanism. To establish that, SECANT services must integrate DIM services. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Decentralized Digital Identity Management Module No. 3 (3.4) |
| **Dependency** | DIM_FR_001 |

| ID | SEPLT_FR_004 |
|---|---|
| **Name** | Platform common point of access and navigation |
| **Description** | The SECANT Platform should have a common point of access and a navigation menu from where users can choose to be redirected to the desired front end. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - |

## Non-Functional Requirements

| ID | SEPLT_NFR_001 |
|---|---|
| **Name** | Platform usability |
| **Description** | The SECANT Platform will be implemented in the simplest way possible for ease of use when used by users or IT administrators. Interfaces should allow easy navigation and be intuitive, to help the user to learn and remember easily minimizing cognitive load, warning of human errors, facilitating the execution of operations and tasks. Each front end should be user-friendly, have an internationalization pilot language and become easy to navigate. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | SDSP_NFR_004 |

| ID | SEPLT_NFR_002 |
|---|---|
| **Name** | Easy to maintain and upgrade |
| **Description** | The SECANT Platform should allow for upgrades, bug fixes, and IT staff should receive both notifications and a way to install new upgrades. Applying upgrades and fixing possible bugs in a timely manner is an important part of a cybersecurity program. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | - |
| **Dependency** | - |

| ID | SEPLT_NFR_003 |
|---|---|
| **Name** | GDPR compliance |
| **Description** | Within the system, the SECANT platform allows access to sensitive data only to users who are authorized and authenticated, according to the GDPR guidelines. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Technical and Impact Vulnerability Assessment & Human Vulnerability Assessment tools 2 (2.2)<br>Advanced Privacy Toolkit 2 (2.2) |
| **Dependency** | HVA_NFR_003, PT_FR_001 |

| ID | SEPLT_NFR_004 |
|---|---|
| **Name** | The data are processed according to the applicable national and European legal requirements |
| **Description** | Regarding the data processing the platform will be designed to consider the applicable legal requirements, at European and national level, but also the nature of the data collected. |
| **Priority** | Must have |
| **Relevant User Requirement(s)** | Technical and Impact Vulnerability Assessment & Human Vulnerability Assessment tools 2 (2.2) |
| **Dependency** | HVA_NFR_003 |

# 5. Conclusions

This deliverable has identified the technical requirements of the SECANT solution. Overall, 103 functional and 47 non-fictional requirements have been elicited, analysed, and prioritised because of the activities performed under T2.2 of the SECANT work plan and captured in this deliverable (D2.2). More specifically, the analysis and prioritisation resulted in 131 requirements capturing high-priority (i.e., must have), 18 capturing medium-priority (i.e., should have) and 1 capturing low-priority (i.e., could have) user needs. These requirements provide the framework upon which the specification of the SECANT architecture is being constructed.

Section 2 of this document provided an overview of SECANT in terms of its main objectives, its core technologies, their state-of-the-art and an initial assessment of the SECANT threat portfolio to build the basis for the development of the Threat Intelligence Module. This overview provided useful context regarding the inner workings of the project at a level of abstraction appropriate for the definition of its technical requirements in its later stages.

In Section 3 the main concepts necessary for the identification and definition of the SECANT technical requirements were introduced. This section also presented the methodology followed for the elicitation of requirements by discussing the overall requirements engineering process including the collection, analysis, and prioritisation activities. Different template documents used for the collection of input from the project's technology providers and the synthesis of the information collected via such documents. The template documents can be found in Appendix 0.

Finally, Section 4 provided an exhaustive list of all the functional and non-functional requirements of each group of technologies represented in SECANT. As the specification and implementation of the SECANT solution is a dynamic and ever-evolving process, the requirements extracted in this document can also evolve during the project's lifecycle. More specifically, subsequent activities of WP2 will use the requirements listed in this deliverable as the basis for the specification of the SECANT architecture. Finally, the implementation of the project's use cases during WP7 'Demonstration and Evaluation', will validate the implementation of the identified requirements of SECANT solution through the tracking of relevant KPIs.

# References

[1] Grant Agreement Number 101019645-SECANT

[2] YETI. YETI. (2022). Retrieved 24 May 2022, from https://yeti-platform.github.io/.

[3] ABOUT CISA | CISA. Cisa.gov. (2022). Retrieved 24 May 2022, from https://www.cisa.gov/about-cisa.

[4] ICS-CERT Alerts | CISA. Cisa.gov. (2022). Retrieved 24 May 2022, from https://www.cisa.gov/uscert/ics/alerts.

[5] MITRE ATT&CK®. Attack.mitre.org. (2022). Retrieved 24 May 2022, from https://attack.mitre.org/.

[6] OVAL - Open Vulnerability and Assessment Language. Oval.mitre.org. (2022). Retrieved 24 May 2022, from https://oval.mitre.org.

[7] Nvd.nist.gov. (2022). Retrieved 24 May 2022, from https://nvd.nist.gov/.

[8] Offensive Security's Exploit Database Archive. Exploit-db.com. (2022). Retrieved 24 May 2022, from https://www.exploit-db.com/.

[9] The Tor Project | Privacy & Freedom Online. Torproject.org. (2022). Retrieved 24 May 2022, from https://www.torproject.org/.

[10] What is overlay network? - Definition from WhatIs.com. SearchNetworking. (2022). Retrieved 24 May 2022, from https://www.techtarget.com/searchnetworking/definition/overlay-network.

[11] Introduction to STIX. Oasis-open.github.io. (2022). Retrieved 24 May 2022, from https://oasis-open.github.io/cti-documentation/stix/intro.html.

[12] MISP Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing. MISP Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing. (2022). Retrieved 24 May 2022, from https://www.misp-project.org/.

[13] OpenCTI - Open platform for cyber threat intelligence. OpenCTI - Open platform for cyber threat intelligence. (2022). Retrieved 24 May 2022, from https://www.opencti.io/en/.

[14] Collective Intelligence Framework — CSIRT Gadgets, LLC. CSIRT Gadgets, LLC. (2022). Retrieved 24 May 2022, from https://csirtgadgets.com/collective-intelligence-framework.

[15] Create Sitemaps - Sitemap Generator - Visual Sitemap Generator. Dynomapper.com. (2022). Retrieved 24 May 2022, from https://dynomapper.com/.

[16] Screaming Frog SEO Spider Website Crawler. Screaming Frog. (2022). Retrieved 24 May 2022, from https://www.screamingfrog.co.uk/seo-spider/.

[17] Deepcrawl | The #1 Technical SEO Platform. Deepcrawl. (2022). Retrieved 24 May 2022, from https://www.deepcrawl.com/.

[18] Web Scraping, Data Extraction and Automation · Apify. Apify. (2022). Retrieved 24 May 2022, from https://apify.com/.

[19] Oncrawl | Enterprise Technical & Data SEO Platform for Smarter SEO. Oncrawl. (2022). Retrieved 24 May 2022, from https://www.oncrawl.com/.

[20] Scrapy | A Fast and Powerful Scraping and Web Crawling Framework. Scrapy.org. (2022). Retrieved 24 May 2022, from https://scrapy.org/.

[21] Committee, A. (2022). Apache Nutch™. Nutch.apache.org. Retrieved 24 May 2022, from https://nutch.apache.org/.

[22] Abrek, N. (2015). Attack taxonomies and ontologies. In Seminar Future Internet SS2014, Network Architectures and Services. Munich, Germany: Technical University of Munich.

[23] Rosa, F. D. F., Bonacin, R., & Jino, M. (2017). The security assessment domain: a survey of taxonomies and ontologies. arXiv preprint arXiv:1706.09772.

[24] Nonaka, I., Toyama, R., & Konno, N. (2000). SECI, Ba and Leadership: a Unified Model of Dynamic Knowledge Creation. Long Range Planning, 33(1), 5-34. https://doi.org/10.1016/s0024-6301(99)00115-6

[25] Zhang, K., & Liu, J. (2020). Review on the Application of Knowledge Graph in Cyber Security Assessment. IOP Conference Series: Materials Science And Engineering, 768(5), 052103. https://doi.org/10.1088/1757-899x/768/5/052103

[26] Hsieh, J. M., Gribble, S. D., & Levy, H. M. (2010). The Architecture and Implementation of an Extensible Web Crawler. NSDI, 10, 28-30.

[27] Witschel, H. F. (2005). Using decision trees and text mining techniques for extending taxonomies. In Proceedings of the Workshop on learning and extending lexical ontologies by using machine learning methods, 8.

[28] Marchenko, O. (2016). A Method for Automatic Construction of Ontological Knowledge Bases. III. Automatic Generation of Taxonomy as the Basis for Ontology*. Cybernetics And Systems Analysis, 52(3), 365-370. https://doi.org/10.1007/s10559-016-9836-z

[29] Zhang, C., Tao, F., Chen, X., Shen, J., Jiang, M., Sadler, B., ... & Han, J. (2018). Taxogen: Unsupervised topic taxonomy construction by adaptive term embedding and clustering. In Proceedings of the 24th ACM SIGKDD Int. Conf., 2701-2709.

[30] Manzoor, E., Li, R., Shrouty, D., & Leskovec, J. (2020). Expanding Taxonomies with Implicit Edge Semantics. Proceedings Of The Web Conference 2020. https://doi.org/10.1145/3366423.3380271

[31] Shen, J., Shen, Z., Xiong, C., Wang, C., Wang, K., & Han, J. (2020). TaxoExpan: Self-supervised Taxonomy Expansion with Position-Enhanced Graph Neural Network. Proceedings Of The Web Conference 2020, 486-497. https://doi.org/10.1145/3366423.3380132

[32] Mao, Y., Zhao, T., Kan, A., Zhang, C., Dong, X., Faloutsos, C., & Han, J. (2020). Octet. Proceedings Of The 26Th ACM SIGKDD International Conference On Knowledge Discovery &Amp; Data Mining, 2247-2257. https://doi.org/10.1145/3394486.3403274

[33] Manning, C., Raghavan, P., & Schütze, H. (2010). Introduction to information retrieval. Natural Language Engineering, 16(1), 100-103.

[34] Manning, C., & Schutze, H. (1999). Foundations of statistical natural language processing. MIT press.

[35] Christopher J. A., Audrey J. D. (2001). OCTAVE Criteria, Version 2.0. Software Engineering Institute

[36] MITRE (2011). Threat Assessment & Remediation Analysis. MITRE technical report

[37] ISACA (2013). Understanding the Core Concepts in COBIT 5. ISACA JOURNAL, 5.

[38] Common Vulnerability Scoring System SIG. FIRST — Forum of Incident Response and Security Teams. (2022). Retrieved 24 May 2022, from https://www.first.org/cvss/.

[39] Common Vulnerability Scoring System. FIRST — Forum of Incident Response and Security Teams. (2022). Retrieved 24 May 2022, from https://www.first.org/cvss/v3-1/.

[40] Common Vulnerability Scoring System SIG. FIRST — Forum of Incident Response and Security Teams. (2022). Retrieved 24 May 2022, from https://www.first.org/cvss/.

[41] Introduction to STIX. Oasis-open.github.io. (2022). Retrieved 24 May 2022, from https://oasis-open.github.io/cti-documentation/stix/intro.html.

[42] (2022). Retrieved 24 May 2022, from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EL.

[43] Kypo Cyber Range: CONCORDIA. CONCORDIA. (2022). Retrieved 24 May 2022, from https://www.concordia-h2020.eu/kypo-cyber-range/.

[44] Shabandri, B., & Maheshwari, P. (2019). Enhancing IoT Security and Privacy Using Distributed Ledgers with IOTA and the Tangle. 2019 6Th International Conference On Signal Processing And Integrated Networks (SPIN). https://doi.org/10.1109/spin.2019.8711591

[45] Attribute-based encryption - Wikipedia. En.wikipedia.org. (2022). Retrieved 24 May 2022, from https://en.wikipedia.org/wiki/Attribute-based_encryption.

[46] Lee, C., Chung, P., & Hwang, M. (2013). A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments. Int. J. Netw. Secur., 15, 231-240.

[47] Searchable symmetric encryption - Wikipedia. En.wikipedia.org. (2022). Retrieved 24 May 2022, from https://en.wikipedia.org/wiki/Searchable_symmetric_encryption.

[48] Wang, Y., Wang, J., & Chen, X. (2016). Secure searchable encryption: a survey. Journal Of Communications And Information Networks, 1(4), 52-65. https://doi.org/10.1007/bf03391580

[49] Qin, Z., Xiong, H., Wu, S., & Batamuliza, J. (2016). A Survey of Proxy Re-Encryption for Secure Data Sharing in Cloud Computing. IEEE Transactions On Services Computing, 1-1. https://doi.org/10.1109/tsc.2016.2551238

[50] Roy R, Mathai PP. (2017). Proxy re-encryption schemes for secure cloud data and applications: a survey. Int J Comput Appl, 164(5): 1-6.

[51] Kaliski B. (2002). PKCS# 5: Password-based cryptography specification version 2.0.

[52] Abiodun, E., Jantan, A., Abiodun, I., & Poston, H. (2022). A comprehensive review of honey encryption scheme. Retrieved 24 May 2022, from.

[53] Bouras, M., Lu, Q., Zhang, F., Wan, Y., Zhang, T., & Ning, H. (2020). Distributed Ledger Technology for eHealth Identity Privacy: State of The Art and Future Perspective. Sensors, 20(2), 483. https://doi.org/10.3390/s20020483

[54] eIDAS Regulation. Shaping Europe's digital future. (2022). Retrieved 24 May 2022, from https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation.

[55] Enisa.europa.eu. (2022). Retrieved on 24 May 2022, from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

[56] Common Vulnerability Scoring System SIG. FIRST — Forum of Incident Response and Security Teams. (2022). Retrieved on 24 May 2022, from https://www.first.org/cvss/v3.0/specification-document.

[57] Chouliaras, N., Kittes, G., Kantzavelou, I., Maglaras, L., Pantziou, G., & Ferrag, M. (2021). Cyber Ranges and TestBeds for Education, Training, and Research. Applied Sciences, 11(4), 1809. https://doi.org/10.3390/app11041809

[58] Ukwandu, E., Farah, M., Hindy, H., Brosset, D., Kavallieros, D., & Atkinson, R. et al. (2020). A Review of Cyber-Ranges and Test-Beds: Current and Future Trends. Sensors, 20(24), 7148. https://doi.org/10.3390/s20247148

# Appendix 1- Tool's Overview Template


**[Partner Acronym]**

# Technology Providers Input

## Tool Overview

| Features | Description |
|---|---|
| **Name** | *Provide the name of the tool or module.* |
| **Owner** | *Provide the name of the organisation(s) owning the tool or module.* |
| **Current TRL** | *Indicate the current technology readiness level (TRL) of the tool or module (1-9).* |
| **Target TRL** | *Indicate the target TRL of the tool or module at the end of the project (1-9).* |
| **Description** | *Provide a brief description (2-3 sentences) of the tool or module (e.g., main functionalities, expected role in SECANT platform).* |
| **Input** | *Briefly describe the input required by the tool or module (e.g., patient data) and the source of this input (e.g., hospital records).* |
| **Output** | *Briefly describe the output produced by the tool or module and the consumer of this output, if known.* |
| **Dependencies** | *Briefly describe any dependencies of the tool or module.* |
| **Licensing model** | *Indicate the licensing model of the tool or module (e.g., proprietary, commercially available, open source)* |
| **Tasks Involved** | *Indicate the WP(s) and specific tasks the tool or module is involved.* |
| **Innovation** | *Provide a brief description (3-4 sentences) of the main innovations of the tool or module compared to the state-of-the-art. If available, provide references describing the state-of-the-art of the specific technological area.* |
| **Other Information** | *Provide any other information relevant to the tool or module, if available (e.g., figure(s), flow diagram(s), links to website, documentation)* |

*Please create a copy of the above table and place it here in case your organisation contributes more than one tools or modules to the project.*

## Key Technological Areas

Please add the name of your tool or module at the last column to indicate the technological area(s) to which it will contribute.

| Key Technological Area | Sub-Topic | Involved Module |
|---|---|---|
| **Threat Intelligence Module** | Threat intelligence collection, sharing and reporting to CERTs/CSIRTs | |
| | Dynamic taxonomies for cyber-attacks | |
| **Cyber Security Risk Assessment Companion** | Connected cyber risk assessment | |
| | Human vulnerability assessment | |
| | Technical vulnerability assessment | |
| | Impact assessment | |
| **Cyber Security Training Module** | Cyber range for security professionals | |
| | Security awareness training for other professionals and clients | |
| | Chatbot | |
| **Trust and Accountability Module** | - | |
| **Privacy Toolkit** | Hybrid protection over data | |
| | Protection over key, password & security-related information | |
| **Digital Identity Management Module** | - | |
| **SECANT Dashboard and End-User Application** | - | |