D3.1 Distributed Situational Awareness Framework v1

WP3 – Cyber security risk assessment & Beyond – Sphinx Intelligence

Version: 1.00

SPHINX

A Universal Cyber Security Toolkit for Health-Care Industry

Disclaimer

Copyright message

Document information

Grant Agreement Number	826183	Acronym	SPHINX
Full Title	A Universal Cyber Security Toolkit for Health-Care Industry		
Topic	SU-TDS-02-2018 Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures		
Funding scheme	RIA - Research and Innovation action		
Start Date	1st January 2019	**Duration**	36 months
Project URL	http://sphinx-project.eu/		
EU Project Officer	Reza RAZAVI (CNECT/H/03)		
Project Coordinator	National Technical University of Athens - NTUA		
Deliverable	D3.1 Distributed Situational Awareness Framework v1		
Work Package	WP3 – Cyber security risk assessment & Beyond – Sphinx Intelligence		
Date of Delivery	**Contractual** M18	**Actual**	M18
Nature	R - Report	**Dissemination Level**	P - Public
Lead Beneficiary	NTUA		
Responsible Author	George Doukas	**Email**	gdoukas@epu.ntua.gr
		Phone	
Reviewer(s):	Dimitris Apostolakis and Argiris Sideris [FINT], Bárbara Guerra and Marco Manso [EDGE]		
Keywords	Situational Awareness		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Document History

Version	Issue Date	Stage	Changes	Contributor
0.10	10/02/2020	Draft	ToC	George Doukas (NTUA)
0.20	12/06/2020	Draft	Contributions to Sections 2, 5 & 6	George Doukas (NTUA), Michael Kontoulis (NTUA)
0.30	16/06/2020	Draft	Contributions to Sections 1, 2, 5, 6 and 7	George Doukas (NTUA), Michael Kontoulis (NTUA)
0.40	18/06/2020	Draft	Contribution to Section 4	Panagiotis Panagiotidis (KT)
0.50	19/06/2020	Draft	Contribution to Section 3	Erkuden Rios (TECNALIA)
0.60	21/06/2020	Draft	Draft for internal review	George Doukas (NTUA), Michael Kontoulis (NTUA)
0.70	24/06/2020	Pre-final	Review 1	Bárbara Guerra (EDGE), Marco Manso (EDGE)
0.80	25/06/2020	Pre-final	Review 2	Dimitris Apostolakis (FINT), Argiris Sideris (FINT)
0.90	26/06/2020	Pre-final	Incorporation of Review comments	George Doukas (NTUA)
0.95	29/06/2020	Pre-final	Quality Control	George Doukas (NTUA) , Michael Kontoulis (NTUA)
1.00	29/06/2020	Final	Final	Christos Ntanos (NTUA)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Executive Summary

This document provides the specifications of the SPHINX's Cyber Situational Awareness (SA) Framework. Given that currently all tools and methodologies are under the design and development phase, the degree of coverage of the target cannot be assessed; however, the broad description of this Framework can encapstulate the outcome of all SPHINX's tools. In the second version of this deliverable (D3.7 due to M30) the capabilities of each tool shall have been adequately defined, supporting a better assessment of the achieved degree of Cyber SA in SPHINX.

Several techniques, mechanisms, and tools shall be involved in automating many of the capabilities that have traditionally required a significant involvement of human analysts. The goal is to promote the *distributed perspective* of SA by combining human and technological agents' intelligence. Cyber SA by necessity involves both technical and cognitive challenges in that the basic data used for developing situational awareness consists of some kind of underlying estimate of the state of the environment which, in turn, is the result of some kind of data processing. To go beyond rudimentary assessments of security posture and attack response, the Sphinx toolkit needs to merge isolated data into higher-level knowledge of network-wide attack vulnerability and mission readiness in the face of cyber threats.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Table of Figures

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Table of Abbreviations

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

SA : Situational Awareness

NIST : National Institute of Standards and Technology

ISO : International Organization for Standardization

NVD : National Vulnerability Database

CVE : Common Vulnerabilities and Exposures

CWE : Common Weakness Enumeration

CAPEC : Common Attack Pattern Enumeration and Classification

OWASP : Open Source Foundation for Application Security

AI : Artificial Intelligence

DTM : Data Traffic Monitoring

RCRA : Real-time Cyber Risk Assessment

SIEM : Security Information and Event Management

HP : Artificial Intelligence Honeypot

FDCE : Forensic Data Collection Engine

HE : Homomorphic Encryption

AP : Anonymisation and Privacy

ID : Interactive Dashboards

VAaaS : Vulnerability Assessment as a Service

MLID : Machine Learning-empowered Intrusion Detection

DSS : Decision Support System

BBTR : Blockchain-based Threat Registry

SB : Sandbox

CIP : Common Integration Platform

SM : Service Manager

JSON : JavaScript Object Notation

CVSS : Common Vulnerability Scoring System

WMI : Windows Management Instrumentation

JDBC : Java Database Connectivity

SNMP : Simple Network Management Protocol

LEA : Log Export API

IT : Information Technology

WHID : Web Hacking Incidents Database

VCDB : VERIS Community Database

DOS : Denial of Service

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

LSTM : Long short-term memory

KPIs : Key performance indicators

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

1 Introduction

1.1 Purpose & Scope

This document, named "Distributed Situational Awareness Framework v1", part of Task 3.3 - SPHINX Distributed Cyber Situational Awareness Framework & Real Time Risk Assessment Module, presents a detailed description of the Situation Awareness Framework, its role and purpose in the SPHINX scope of the project and finally describes its actual implementation, relying on several SPHINX components.

SA is described as knowing what is going on around you and within that knowledge of your surroundings, knowing what is important. A situation is a collection of objects that have relationships with one another and the environment, and an object is a physical entity: something that is within the grasp of the senses. Hence, SA can be described as ''the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future'' (Endsley M. , 1995).

Indeed, the Situational Awareness Framework relies heavily on SPHINX tools, described in section 3, since it combines their output in order to provide prompt and actionable information. Given that currently all tools and methodologies are under the design and development phase, the degree of coverage of the target of Cyber SA cannot be assessed; however, the broad description of this Framework can encapstulate the outcome of all SPHINX's tools. In the second version of this deliverable (D3.7 due to M30) the capabilities of each tool shall have been adequately defined, supporting a better assessment of the achieved degree of Cyber SA in SPHINX.

1.2 Structure of the deliverable

This document is structured as follows: section 2 describes the concept of situational awareness and the design specification that will be followed in SPHINX; section 3 mainly describes the different tools and available data sources that provide information to the SA; section 4 highlights the importance of data aggregation and analysis to extend the SA within SPHINX, section 5 mainly describes risk management approach as part of the overall decision support procedure, section 6 describes the contribution of visualisations to SA and section 7 presents the conclusions.

In addition, Annex I presents all the states of threat-related factors utilized in Risk assessment process. As already mentioned, SPHINX utilises the OWASP factors in order to calculate the likelihoods in the threat exposure node. SPHINX further enriches the original factors, as to better characterise the threats. All the factors have different states that are used to correspond to specific semi-quantitative and qualitative values. Those states are presented in detail the Annex I of this document.

1.3 Relation to other WPs & Tasks

The document, and by extension the Situational Awareness Framework, are intrinsically linked to WP2 and specifically the stakeholder's requirements as outlined in Task 2.3, and the SPHINX use cases defined in Task 2.4, which form much of its specification and design philosophy. Additionally, the SA Framework considers the outputs of Task 2.5, which addressed the whole architecture of the SPHINX Toolkit, its comprising components or tools and how they interact with each other.

Being the link between many different SPHINX components, developed within Work Packages 3, 4 and 5, the Situational Awareness Framework depends on the output and input of the tools designed and developed in the tasks pertaining to those work packages.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

2 Overview of Cyber Situational Awareness

2.1 Scope of Cyber Situational Awareness

Situational Awareness (SA) is an important design objective for a wide variety of domains, which can be approached from several different perspectives. From a technical viewpoint, situational awareness comes down to compiling, processing, and fusing data. Such data processing includes the need to be able to assess data fragments as well as fused information and provide a rational estimate of its information quality (Arnborg S, 2000). With this approach it is feasible to technically relate and evaluate pieces of information relative to each other. In contrast, the cognitive side of situational awareness concerns the human capacity of being able to comprehend the technical implications and draw conclusions in order to develop informed decisions.

SA is described as knowing what is going on around you and within that knowledge of your surroundings, knowing what is important (A. D'Amico, 2005). A situation is a collection of objects that have relationships with one another and the environment, and an object is a physical entity: something that is within the grasp of the senses. Hence, SA can be described as ‘‘the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future’’ (Endsley M. , 1995). This SA model, based on its role in dynamic human decision making, follows a chain of information processing from perception, through interpretation, to projection. In dynamic environments, many decisions are required across a fairly narrow space of time, and tasks are dependent on ongoing, up-to-date analysis of the environment.

From the lowest to the highest, the levels of SA are as follows:

- Level l SA: Perception of the Elements in the Environment to perceive the status, attributes, and dynamics of relevant elements in the environment.
- Level 2 SA: Comprehension of the Current Situation
- Level 3 SA: Projection of Future Status: This is achieved through knowledge of the status and dynamics of the elements and comprehension of the situation (both Level I and Level 2 SA).

In 2001, (Endsley M. , 2001) defined Situation Awareness as the key to providing information, because the problem is no longer lack of information, but finding what is needed when it is needed. Cognitively it is therefore interesting to measure to what extent a human decision-maker is aware of the situation, i.e., has reached a certain level of situational awareness, and how well he/she manages to maintain and develop this awareness as time progresses.

Over the years, SA has been defined in a number of complementary ways, most focusing on the application of SA to specific domains. Cumiford (D.Cumiford, 2006) defines SA in Cyber Defense as *the ability to rapidly and effectively address incoming stimuli with appropriate response*; Figure 1 is adapted from Endsley's SA reference model, which presents three levels of situation awareness, perception, comprehension and projection. McGuinness and Foy extension of Endsley's SA model (B. McGuinness, 2000) introduced an additional fourth level (resolution).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

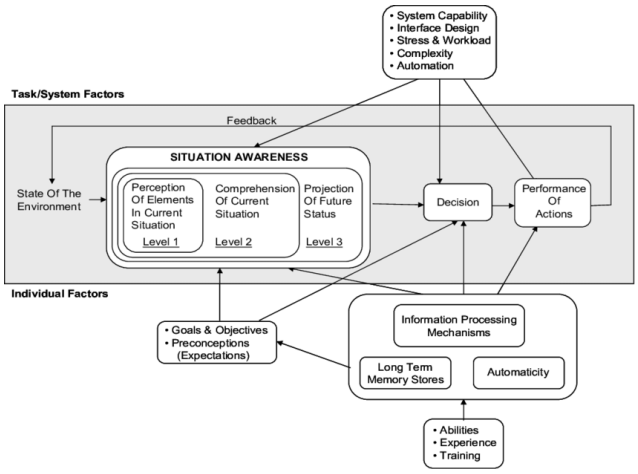

Figure 1: Endsley's Situation Awareness Model

In Cyber SA all cases require the understanding of a number of different situations, an awareness of, comprehension thereof, projection of current situation, and the estimation of escalations of current situations to impending future situations, and resolution of both the current situations and the impending ones. People are an integral aspect of Cyber SA because the understanding and/or resolution of these situations could not happen without analysts, administrator, operators. In general, Cyber SA encompasses people, process and technology required to gain awareness of historic, current and future situations in cyber, and the enablement of controls to protect the systems from future projected incidents.

According to Cyril Onwubiko (C. Onwubiko, 2011), the four levels (added Resolution level) of Situational Awareness in Computer Network Security is described as follows:

- *Perception* deals with evidence gathering of cyber situations (knowledge of the elements in the network such as alerts reported by intrusion detection systems, firewall logs, scan reports, as well as the time they occurred; classification of information into meaningful representations that offers the underlying for comprehension, projection and resolution.).
- *Comprehension* is related to understanding of the exact situation, which may be derived from analysis of the set of evidence gathered or perceived of the current cyber situation, and also involves the understanding of the exact threat level, identification of attack types, and of the associated or interdependent risks.
- *Projection* deals with predictive measures to forecast future incidents, situations or states using the current state of the situation, and understanding how current situations could escalate. In addition, it relates to the estimation of, and what the current situation could become in the nearest future considering the perceived current tension, escalations and evolution that might happen over time.
- *Resolution* deals with controls to repair, recover, remedy and resolve the perceived cyber situations.

Cyber SA can be seen as a subset of an organisation's overall SA (Endsley M. , Measurement of situation awareness in dynamic systems, 1995). Although cyber SA concerns awareness regarding cyber issues, these need to be combined with other information to obtain full understanding regarding the situation. Hence, cyber events offer additional insight about the overall situation, not about a disjointed cyber situation.

Improving a decision maker's situational awareness within the cyber domain is similar to other domains. Situational awareness requires working with processes capable of identifying domain specific activities as well those which cross domains. These processes depend on the context of the environment, the domains, the goals and the interests of the decision maker, but they can be defined to support any domain (G. Tadda, 2010).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

2.1.1 Design Principles

Despite the significant attention being given to the critical problems of cyber security, the ability to keep up with the increasing volume and sophistication of network attacks is seriously lagging.

Cyber SA by necessity involves both technical and cognitive challenges in that the basic data used for developing situational awareness consists of some kind of underlying estimate of the state of the environment that, in turn, is the result of some kind of data processing. To go beyond rudimentary assessments of security posture and attack response, organizations need to merge isolated data into higher-level knowledge of network-wide attack vulnerability and mission readiness in the face of cyber threats. Network environments are always changing, with devices being added and removed, patches applied (or not), applications (un)installed, firewall rules changed, all with potential impact on security posture. Intrusion alerts and anti-virus warnings need attention, and even seemingly benign events such as logins, service connections and file share accesses could be associated with adversary activity.

The transformation of large amounts of data into comprehensible information, accompanied by a technical decision support system that ultimately serve to help a decision-maker gain and further develop a high degree of situational awareness. The problem is not lack of information, but rather the ability to assemble disparate pieces of information into an overall analytic picture, easily comprehensible in order to support optimal courses of action and concurrently maintaining mission readiness.

According to (S. Jajodia, 2010), a full cyber SA for cyber defence requires the integration of at least the following seven aspects:

1. Be aware of the current situation (which may include network security and the wider cyber influence)

   Current situation: Situation perception includes both situation recognition and identification. Situation identification can include identifying the type of attack, the source of attack, the target, etc. Situation perception is beyond intrusion detection. Intrusion detection is a very primitive element of this aspect.

2. Be aware of the impact of the attack

   Impact: Impact assessment refers to the assessment of current impact (damage from occurring events) and the assessment of future impact (projection to the future). Vulnerability analysis and threat assessment are two significant factors of future impact assessment.

3. Be aware of how situations evolve

   Evolution: Situation tracking is a major component of this aspect.

4. Be aware of adversary behaviour

   Behaviour: A major component of this aspect is attack trend and intent analysis, which are more oriented towards the behaviors of an adversary or actor(s) within a situation than with the situation itself.

5. Be aware of why and how the current situation is caused

   Chain of evidence: This aspect includes causality analysis and forensics.

6. Be aware of the quality and trustworthiness of the situational awareness information

   Information: Collected information and the deriving knowledge-intelligence delimit the quality of decision process.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

7. Assess plausible features of the current situation

   Prediction: This involves a multitude of technologies for projecting future possible actions/activities of an adversary, paths the adversary might take, and then constraining the possible futures into those that are plausible. This constraint requires an understanding of adversary intent, opportunity, and capability (knowledge of them) as well as an understanding of blue vulnerabilities. (knowledge of "us").

Endsley's model can be related with these seven aspects as: recognition (1, 6, and 7), comprehension (2, 4, and 5), and finally projection (3). This approach is by nature, human-centric, especially since its goal is to minimize human error and strengthen the first line of defence. However, in practice, cyber SA involves several additional factors such as threat detection and management, network management, incident reporting, threat intelligence sharing and risk management. All the above should be incorporated into the organizations' cybersecurity protocols. Information flows are by default bi-directional (top-down, bottom-up) to ensure that the right information is available to the right person at the right time. Human comprehension plays a significant role to proactive mitigation and reduction of response and dwell detection time. In fact, incident reporting is key to breaking a cyber kill chain.

Cyber SA is a subset of situational awareness, i.e., cyber situational awareness is the part of situational awareness which concerns the "cyber" environment. Cyber SA can be reached by the use of data from IT sensors (intrusion detection systems, among others) that can be used from a data analysis process or be directly presented to the decision-maker. SA can also be reached by more abstract sensors, such as an external source about an imminent cyber-attack. It is important to note that cyber SA cannot be treated in isolation but is intertwined with and a part of the overall situational awareness.

Although cyber SA is directly linked with cyber issues, these cyber issues need to be combined with other information to obtain a full understanding regarding the situation in total. Hence, cyber events can offer additional insight of the overall situation, not only of a disjoint cyber situation. Similarly, events outside the "digital" world can offer additional insight regarding a cyber situation. For instance, the combination of information from an intrusion detection system and of information stemming from human activities contribute jointly to enhancing the overall cyber situational awareness.

Cyber SA is studied from the perspective that situational awareness serves to enhance sensemaking, i.e., the perspective taken is that new cyber sensors can contribute to situational awareness for the purpose of understanding what needs to be done in terms of the desired effects and the actions that ought to be undertaken to achieve these effects (K.E. Weick, 2005). From this point of view, the information infrastructures that cyber situational awareness targets can be related to two distinguishing contexts, namely the daily operation in an organization, and the reaction to a specific situation. At this point the extension (Resolution level) to Endsley's model comes into play. Resolution deals with controls to repair, recover, remedy and resolve the perceived cyber situations. The biggest challenge in cyber security is the emerging new risks and methods of attack. Due to the constant evolution of attacks and risks, cyber security cannot rely on static procedures. It requires constant maintenance, consistent updating, continuous monitoring and proactive planning.

The ultimate outcome of cyber SA can be summarized as the implementation of procedures/algorithms that will greatly enhance machines' intelligence that shall assist human decision maker's through the automation of cognitive SA processes. While data from all levels should be taken into consideration, this huge amount of information needs to be combined and transformed into a more concise and meaningful form. Indeed, a level of abstraction at least of collected "raw data", otherwise, data collected at the lowest levels can easily overwhelm the cognitive capacity of human decision makers. Situation awareness based solely on low level data is clearly insufficient and this is where artificial intelligence (AI) is needed.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

In general, all aspects of SA are interdependent and play a vital role in ensuring that an organisation is comprehensively informed about the health of its networks, the status of its offensive and defensive strategies and identifying the risks associated with a potential attack.

2.1.2 Human Factor

Situation awareness is gained by a system, which is usually the (cyber-physical) system being threatened by random or organized cyber-attacks. Although the ultimate system is one that can gain self-awareness without involving any humans in the loop, this vision is still very distant from the current reality, and there is still no tangible roadmap to achieve this vision. Decision-makers are an indispensable “component” of the system gaining situation awareness. Cyber SA systems benefit from advanced hardware sensors and “intelligent” components, but human comprehension is the most decisive factor in making advanced decisions.

In addition, securing human endpoints requires a comprehensive strategy that focuses on training, cyber situational awareness (Cyber SA is continuous and integral to daily learnings and is different from training.), and prompt incident reporting. Humans are the most significant factor in building a culture of security awareness. If cyber SA is properly communicated to everyone, the foundations towards perimeter security have been achieved. Moreover, humans hold a vital role in real- time identification and reporting of suspicious activity, thus supporting any automated process in place. Artificial intelligence is a very promising field in cybersecurity, but human intelligence is irreplaceable. Clearly, human-computer interaction is essential for achieving cyber situational awareness.

2.1.3 Time Aspects

Time plays a vital role in the definition of SA. The time aspect enables us to capture the dynamics of the environment. The SA definitions that represent the process approach address the time aspect naturally. The three-level definition covers the time aspect by the "within a volume of time" statement. This statement contained in the definition pertains to the fact that operators need to capture the environment not only in terms of volume (where, how many elements are present) but also in time (i.e., how will the environment evolve and what impact it will it have on the operator’s goal and tasks). Time is a substantial part of Levels 2 and 3 of the three-level definition.

The SA is not necessarily a product/process that is acquired/finished instantaneously. It is built over time. Thus, it is essential to take into account, that some aspects of the SA can be acquired only over time. Such a piece of knowledge could then be used for better environment perception or more accurate projection of future status. In this context, Endsley (Endsley M. , 1995) introduced the following two terms: working memory and long-term memory.

Working memory stores the perceived information from the environment. In case an operator does not have any previous information on the environment, the majority of information is stored in working memory. Apart from the perceived information, the working memory contains all necessary information needed for actual SA - mental models recalled from long-term memory, subsequent decisions, or current goals. All information is processed there and a picture of the current situation is generated, including the prediction of the future environment status. It requires the maintenance of present conditions, rules used for prediction, and actions resulting from the predictions. All these tasks impose a heavy load on the working memory that might be considered as a bottleneck for SA.

Long-term memory contains schemata and mental models which aids the working memory with obtaining SA. Schemata represent coherent frameworks for capturing highly complex systems including their components, states, and functioning. Several details of the situation are lost during the capture of a situation to a schema. Still, the schema can serve to capture a coherent picture of a given situation and may be efficiently recalled to

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

aid the working memory. Mental models represent a generalization mechanism for the generation of general descriptions of systems (e.g., explanations of functions, goals). An expert operator would have developed numerous mental models that shift a situation representation to prototypical abstract codes. A mental model can then be understood as a schema for a particular situation.

2.1.4 Decision-Making

Situation Awareness should be strictly separated from the process of decision making. SA provides an operator's internal model of the situation that serves as input for his/her decision process. Even with a correct SA of the actual state, an operator may come to a wrong decision. The decision process involves assumptions, restrictions and conditions, e.g., level of risk aversion, and it should not be directly related to SA. However, decision may impact SA through the implemented controls and actions.

2.2 Background

In literature (N.A. Stanton, 2009) three main theoretical perspectives have been identified: (a) the cognitive perspective; (b) the technological perspective, and (c) the distributed perspective.

- The *cognitive perspective* is the most widely adopted theoretical perspective in SA research. It considers SA as a human internal cognitive state comprised of perception, comprehension, and projection. The analytical focus of the *cognitive perspective* is on the human operator's understanding of the environment at a particular point in time.
- The *technological perspective* advocates that SA is instantiated through the presentation of information by a technological agent. Implicit in this view is that SA resides within the agent itself, typically in the form of information. The analytical focus of the *technological perspective* is the design and configuration of information presentations to most effectively convey the SA contained within the agent.
- The *distributed perspective* of SA is a hybrid theory that considers both human and technological agents influence SA (distributed throughout a socio-technical system (N.A. Stanton et al., 2006)). Within the broader system, different agents may have different SA, and the degree to which agents within the system share SA is a function of the extent to which their goals overlap. The analytical focus of the *distributed perspective* is the socio-cognitive system and interactions between agents within the system and the system, and agents and the environment.

Each theoretical perspective has its strengths and weaknesses, particularly in their application to the cyber SA. Much of the research on cyber SA, has primarily taken an algorithmic perspective, focusing primarily on the automation and the development of new defensive tools for protection, detection and response (E. McMillan, 2012). Examples of this work include data visualizations (A.D'Amico, 2001), data fusion methods for tracking cyber-attacks (A. Stotz, 2007) (S. J. Yang, 2009), identification of internal and external threats using intelligent agents (J. F. Buford, 2008) (J. Yen, 2010), and the use of probabilistic models to assess network vulnerability (X. Peng, 2010). Although valuable, this body of work overlooks perhaps the most crucial component of cyber defence analysis: the human component (M.W.Boyce, 2011). In these attempts, little attention was paid to how operators perform with existing technologies let alone whether these new technologies actually improve SA in human operators.

2.3 Situational Awareness in Sphinx

SA model in SPHINX relays to Endsley's modified model, as shown in Figure 2.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

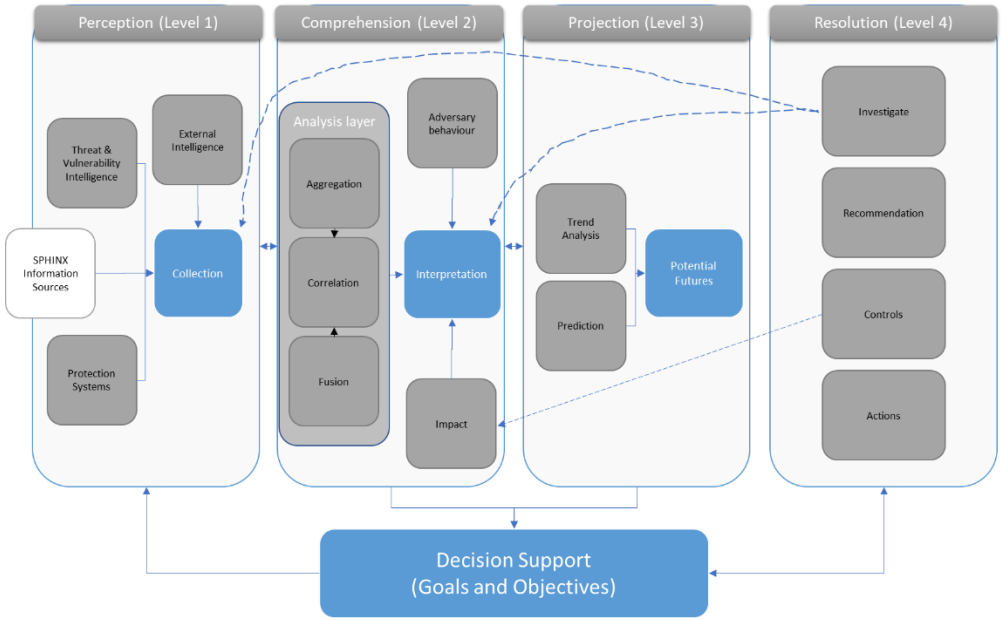

Figure 2: Cyber Situation Awareness Model

In order to make informed decisions, security officers need to be aware of the current situation, the impact and evolution of an attack, the behaviour of the attackers, the quality of available information and models, and the potential futures of the current situation. The SA model consists of the following four levels:

Level 1

Four general sources provide information in this model.

- The first is classified as sources generating information from their operation status. These sources (systems, subsystems, devices) provide logs as a result of their activity or interaction with other (sub)systems. This type of information may contain pieces of evidence symptomatic of an attack.
- The second is classified as sources generating information through their role as detection and security tools supervising the network (may include firewalls, intrusion detection systems, antivirus servers). These systems capture additional information of the state of the network segment they monitor.
- The third is classified as sources able to bring Vulnerability and Threat intelligence within the SPHINX Toolkit. These might be external data-sources (like NVD[1], CVE[2]) vendor vulnerability intelligence, threat information (e.g. CAPEC[3]) which can provide complementary enrichment of the already existing awareness and hence complement a current SA 'picture' to enable improved comprehension.
- The fourth is classified as other external sources of intelligence. External intelligence can be gained through mechanisms such as social media intelligence, government or agency intelligence.

Collection is the central mechanism that will allow all disparate pieces of evidence to be collected, gathered, and available for the scope of analysis of Level 2.

Level 2

Comprehension comprises of analysis tools and techniques to better understand situations that occur in Cyber. Analysis is an on-going process that incorporates technology to perform automated, swift and repetitive tasks aimed at providing actionable insights of the current or impending future situations (Level 3). Analysis techniques must result a meaningful "reasoning" of the situation, especially when information is missing or is

[1] National Vulnerability Database https://nvd.nist.gov/
[2] Common Vulnerabilities and Exposures https://cve.mitre.org/
[3] Common Attack Pattern Enumeration and Classification https://capec.mitre.org/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

not complete, or even seems to be contradicting among agents. Aggregation allows information from relevant resources to be group together into a more "abstract" and meaningful intelligence. Fusion of information for 'better' understanding of the situation shall support analysis. Fusion allows disparate and somewhat unrelated events or activities to be combined in order to understand the 'bigger' picture. Correlation allows the analysis of all sources in order to understand the type of relationships and how they might interact each other. Adversary behaviour and Impact blocks provide a better understanding of the occurring situations and their potential impact. The synthesis of analysis intelligence with the information from those two blocks shall highlight, among others, the conditions that led to a specific situation in order to support decision making.

The *Interpretation* mechanism provides the outcome of analysis that will allow all pieces of evidence to be well understood and available for the scope of Level 3 and in parallel support decision making.

Level 3

Projection takes advantage of the "analysed intelligence" from Level 2 to predict future states or situations. It shall be an on-going process to allow the situation's understanding to be updated when new and current intelligence becomes available. Trend Analysis allows the current situation to be monitored in order to track when the current situation changes so as to update the overall picture. Prediction uses tools and technics to provide an estimation about the near-future situation, by using all available information from Level 2, hence notify any foreseen change.

The *Potential Futures* mechanism provides information regarding future states or situations. This process shall provide information to the decision-making level for risk management, the implementation of proactive actions or the design of a mitigation strategy.

Level 4

Resolution focuses on what needs to be done in order to remedy, recover and resolve situations or respond to future situations observed through security monitoring, threat intelligence, tracking and external intelligence. Investigation and Actions blocks act as a forensics mechanism that gather incident-related evidences and any action taken in order to provide additional information to *Collection (L1) & Interpretation (L2).* Controls are the implemented safeguards or countermeasures to avoid, detect, counteract, or minimize security risks involving information, computer systems, or any other type of assets used to support Level 2. Finally, the Recommendations block includes any additional information stemming from decision support suggestions that is not incorporated into a control.

In summary, the model prescribes the basic concept to enhance situational awareness. A specific array of techniques and automated tools with the objective of drastically enhancing Cyber SA is presented in the following Sections 3, 4 and 6. Several techniques, mechanisms, and tools shall be involved in automating many of the capabilities that have traditionally required a significant involvement of human analysts. The goal is to promote the *distributed perspective* of SA by combining human and technological agents' intelligence. Section 3 covers Levels 1 (*Collection*) and part of Level 2 (*Interpretation*). Section 4 in conjunction with Section 5 contribute to Levels 2 to 4, while section 6 supports horizontally the overall cognitive prossesses.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

3 Perimeter security management and data collection

3.1 Data Management

Data acquisition in SPHINX is performed by the **Data Traffic Monitoring (DTM)** component, that is able to capture network traffic data from multiple protocols of the communications between system assets. The component performs a first analysis of traffic packets and files in different formats to identify users and sources of traffic. In case abnormal communication or activity is detected, or any suspicious packet, the component would rise an event. The DTM can also provide statistics of traffic flows that support the intelligence of other components in SPHINX (Deliverable 2.6, 2020).

Being the main point of traffic data capturing, the DTM does have interfaces with all the other components in charge of analysing the data in SPHINX, including the following SPHINX components relevant for situational awareness:

- Anomaly Detection (AD) -> identifies “abnormal” behaviours concerning the infrastructure (system) and the users;
- Real-time Cyber Risk Assessment (RCRA) -> evaluates the risks of the system according to identified threats and value of the system assets. See Section 5 for further details;
- Security Information and Event Management (SIEM) -> see Section 3.5;
- Artificial Intelligence Honeypot (HP) -> see Section 3.6;
- Forensic Data Collection Engine (FDCE) -> produces a timeline of cyber security incidents and enables the reconstruction of incidents;
- Homomorphic Encryption (HE) -> this component is not directly related to perimeter security management but implements a security-by-design and privacy-by-design technique to enable advanced confidentiality and integrity of healthcare data. Traffic data is not expected to undergo such a protection;
- Anonymisation and Privacy (AP) -> this component is able to identify and anonymise any personal data that might exist in collected traffic information (including data packets, Universal Resource Locators or URLs, IPs and timestamps);
- Interactive Dashboards (ID) -> this component supports the visualisation and notification features of the SPHINX Tookit. The ID panels inform on high-level decisions, planned suggestions, trends and forecasts related to cybersecurity threats and protections about the system under analysis. This information, fed from multiple SPHINX components’ output, is displayed to system operators in a user-friendly manner to allow a rapid situational awareness and understanding. See Section 6 for further details.

As part of the SPHINX Common Integration Platform (CIP), the SPHINX **Service Manager (SM)** allows all actors and systems to exchange data through various data exchange protocols, such as RESTful web services. The CIP incorporates also mechanisms to effectively support advanced big data analytics that are relevant, such as risk assessments. To this aim, the CIP includes a data sandboxing-based Master Data Management framework that acts as a single integration layer between all the necessary data sources and data provision services, so they can be shared across all SPHINX components and applications.

The SPHINX Master Data Management framework relies on Hadoop Data Lake approach to offer a large storage repository of all raw data and supports data from different sources and in different types and formats. To achieve fast and big data processing, the infrastructure is coupled with Apache Spark analytics engine.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

3.2 Asset Management

As part of the RCRA tool, SPHINX offers an Asset Inventory module that is able to discover dynamically the entities connected to the network (in conjunction with DTM tool) and update their attributes. The asset inventory characterises the system assets by multiple attributes such as their description, IP address, communication protocols and, most importantly, it stores the value assigned by system administrator to the asset. The asset value will be a key attribute when assessing the risks over the assets, as the highest the value the more severe the risks of threats against the asset.

3.3 Vulnerability & Patch Management

The identification of vulnerabilities in system assets is done in SPHINX through the Vulnerability Assessment as a Service (VAaaS) component. This component continuously monitors the network entities through an embedded discovery service and dynamically scans them for vulnerabilities. The identified vulnerabilities are listed in the output vulnerability report (e.g. in JavaScript Object Notation or JSON format). The assessed network entities are also assigned a vulnerability score that represents the overall level of security of the entity and its vulnerabilities. The asset score is computed from the scores of individual vulnerabilities identified in the asset. The scoring system used is the Common Vulnerability Scoring System (CVSS)[4].

The information about the patches applied in the system entities is not directly managed by SPHINX, but the Vulnerability identification service (VAaaS) and Certification module service (see below in Section 3.7) produce reports that enable to identify whether specific vulnerabilities or flaws do exist still in the componententity. In case a particular vulnerability cannot be found it would mean that the corresponding patch solving it is already applied and working properly in the component.

3.4 Network & Configuration Management

The Data Traffic Monitoring (DTM) module in SPHINX is continuously capturing network data and is in charge of providing it together with network flow statistics to other platform components. With regards to configuration management and change control, good practices promote to the execution of perform testing on updated and patched components before being their deploymented into a production environment. The Testing component module in SPHINX could definitively help in this task.

3.5 Security Information & Event Management (SIEM)

The **Security Information & Event Management (SIEM**) component is a central component in the SPHINX Toolkit to manage security and event information and therefore plays a very relevant role in situational awareness. The SIEM implements data search and visualisation services to empower the human operator in discovering attacks and their causes.

The tool provides a dashboard offering insights on detected security incidents. The tool enables the user to acquire a global view of network information and security incidents and events in the system, having the ability to search, report and analyse data of different components. The search interface of the SIEM allows other components or users to search through its events and supports these functionalities: time-based queries, row and column filtering, statistical aggregations, event correlation and event enrichment.

[4] https://www.first.org/cvss/v3.0/specification-document.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

The SIEM relies on the Anomaly Detection (AD) component to identify disturbances and suspicious events, activities or observations that differ from the normal infrastructure/component/user behaviour.

The interface with the DTM component allows the SIEM to collect information on abnormal and suspicious traffic activity (including data packets) so as to obtain the complete view of the system's security information and events. Furthermore, the SPHINX SIEM supports industry-based log collection methods (syslog, WMI, JDBC, SNMP, Checkpoint LEA) to further exchange the logs to other SPHINX components such as the Forensic Data Collection Engine (FDCE).

3.6 Threat Detection & Incident Management

The **Machine Learning-empowered Intrusion Detection (MLID)** component in SPHINX is capable of detecting existing threats and even learning new uncategorised threats. The module applies advanced statistics and pattern recognition techniques to avoid intruders teaching the system to consider its attacks as normal data.

MLID operates in conjunction with SPHINX honeypots to collect interaction data generated by attackers (logs/attacker data and signatures) for early intrusion detection. Supervised learning is used to flag and classify in near real-time traffic generated from honeypot interactions, while eliminating the need of manual and continuous updates of databases and detection rules required in traditional intrusion detection systems.

A very important component of perimeter security management in SPHINX comes in form of **Honeypots** that emulate system assets. Production Honeypots deployed in the same network as system components would allow to lure attackers, track all their activities and gain insights on their behaviour and the tactics used. This is very valuable information when trying to understand how to best protect the system perimeter from external attacks. The Artificial Intelligence-based Honeypot (HP) component in SPHINX would therefore play a very important role to identify which preventive and reactive measures could be applied to counter the attacks.

Whenever the HP detects incidents and attacks, it generates notification messages to inform SPHINX components, such as the SIEM, the DSS and the ID for further analysis and notifications. Furthermore, HP provides logged data to the MLID that performs a meta-analysis on these data. The incidents and attacks detected by the Honeypots would appear in the ID to inform the SPHINX Platform's users that an action might be needed.

SPHINX support to **incident forensics** is materialised in the Forensic Data Collection Engine (FDCE) component which correlates, analyses and stores in a privacy-respectful manner all incident-related information and data from different levels and contexts of the system.

The FDCE is able to discover the relationships between devices and the related evidence and produce a timeline of cyber security incidents, including a record of incident related information, a map of involved assets (system components) and a set of meaningful chain of evidence. This component connects to an online cyber threats taxonomy base that is part of a knowledge base of formal and uniform representations of digital evidence, along with their relationships that encapsulates all concepts of the forensic field.

The Blockchain-based Threat Registry (BBTR) provides a de-centralised secure and trusted mechanism to record and share **threat information** to be stored and distributed across blockchain nodes hosted by healthcare organisations using SPHINX. This enables all connected organisations to build a trusted channel of communication about threat information and a synchronised threat registry that is updated whenever a node is attacked. Any authorised SPHINX blockchain user could retrieve information and historical data on suffered attacks registered in the BBTR ledger.

Four main SPHINX components interact with the BBTR: i) The SIEM that generates logs of new threats detected and inserts them in the BBTR, ii) the FDCE that identifies new threats and inserts forensics information on them

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

in the BBTR, iii) the DSS that is informed on new threats logged in the BBTR, and finally iv) the Interactive Dashboard (ID) component which retrieves information on new threats that will be shown to the user in the control panel.

3.7 Compliance Management

Compliance Management in SPHINX is supported mainly by the **Sandbox (SB)** component which supports cyber certification and assessment of component's compatibility with the certification used by the Health and care domain under consideration. Therefore, the SB tool checks the system component's compliance with standards such as ISO/IEC 27001 and NIST SP 800 series. The tool supports the analysis of threats and the protection of sensitive data as part of the cyber security certification model.

The SB considers vulnerability assessment results to isolate any unsupervised processes. To this aim, SB retrieves the VAaaS's vulnerability assessments that provide intelligence on the level of security of particular entities (CVSS report), i.e. identifies all the possible exploits related to the particular IT infrastructure's vulnerabilities. The module also collects up-to-date cyber threat intelligence (new malware, zero-day attacks, vulnerabilities) from the SPHINX Knowledge Base and from external threat intelligence repositories to be considered in the analysis. As a result of this analysis, the SB component produces a certification report that identifies the result of the certification process according to the certification criteria from the standard under consideration.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

4 Data aggregation and analysis

4.1 Overview

Data aggregation processes (e.g. decision support and Internet of Things systems) are essential in many cases for data management. To improve the design of the system, it is necessary to understand the data aggregation processes and their dependencies to time-related properties (A. Bar, 2014). Additionally, data aggregation became a very important topic for collecting enormous amounts of data in real-time from different services and also, for further analysis. Different data aggregation approaches exist along with various requirements, e.g., it is possible that one aggregation receives data passively and another may receive data actively. These differences are increasing the difficulty of design a holistic solution with multiple aggregations. Also, for effective analysis, the data should be aggregated on the time that is needed, whereas, in other cases, the analysis is ineffective and useless.

The data aggregation approach that is more closely to SPHINX's purpose is the aggregation from multiple data sources at different time intervals. There are some basic steps in data aggregation processes (D.J.Abadi, 2003):

1. Preparation of the raw data: This step includes the locating, extraction, transportation and normalization of raw data, if it is useful.
2. Aggregation of raw data: In this step the raw data are transformed into aggregated data by using an aggregation function.
3. The aggregated data: In this step the data are stored (e.g. in a database) and used for other purposes (e.g. analysis).

4.2 Correlation and further exploitation of available data

There are various types of correlations between the data attributes in most domains. All these correlations can be efficiently utilized to give optimized solutions to different problems. Particularly, there are two categories of data correlations, the hard and soft ones. The hard correlations should hold for all data tuples but for the soft ones it is sufficient to apply to the majority of the data tuples. An example of soft correlation could be the case of online shopping, where the duration for the products' delivery can be 3 or 4 days. However, in the case of the SPHINX project, we have to deal with many hard correlations, e.g., we have the IP address of the affected asset, the time that the threat occurs, a description of the threat and additional attributes.

In general, a correlation indicates that the values among the two variables are not independent. In this case, a variable indicates some knowledge for the other variable. For the relational database systems, the definition of these correlations has many advantages such as data integrity and query optimization. In many cases, unfortunately, the data integrity is bypassed. The reasons for bypassing the data integrity are many, such as the data size that makes it very difficult to scan for integrity issues. Also, in the case of big data the correlations are not confirmed at all, due to complexity issues.

Although, data integrity is not an easy task, it is very important for query optimization. In this case, data integrity is very useful for big data infrastructures that use structured and/or semi-structured data. Another issue regarding data integrity is that experts may provide their opinion for possible correlations, but it is very difficult to identify if these correlations are useful. Although the hard correlations are ready for exploitation, the soft correlations need specific handling and strategies for correct query execution. Also, this handling has a storage cost. Finally, the system may pay the cost of handling the correlations, which lead to a waste of resources. It is important to deal with a cost-benefit model that will select the correlations by their costs and benefits (J. Baulier, 1998).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

All available data received from the SPHINX components will be stored in a database (e.g. MongoDB) for further analysis. Visualizations, such as bar and pie plots, will provide an overview for example for the number of attacks and the attack types that occur in an organization e.g. the previous week. Also, these data will be used to re-train SPHINX's models for the prediction of an upcoming attack.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

5 Decision Support

5.1 Overview

The Decision Support process in SPHINX is monitored through the Decision Support System (DSS). The DSS has two main functionalities, the proactive and the active functionality. The proactive functionality refers to the pre-incident actions and the active functionality to the post-incident actions. At the proactive stage, the DSS uses Machine Learning models to predict upcoming cyber-attacks (e.g. prediction of 10 packets ahead). In this case, the prediction of an attack could help the users by alerting them and increasing the situational awareness. In more detail, this functionality may help defenders to perceive, comprehend and project an emergent cyber-attack situation in the network (M.R. Endsley, 2012).

However, the Machine Learning algorithms are not 100% accurate in detecting threats and may predict an attack that does not exist and vice versa. In this case, it is up to the defender's judgment to decide how to handle these alerts. The defender has the ability to block the IP of the possible attacker or not. To help the defenders to take the correct decision, the maximization of the accuracy of the models is needed to minimize false alarms (predict an attack when there is none) and misses (not predict an attack when there is one). To achieve this, the models will be retrained in predefined time intervals.

Dutt, Moisan, and Gonzalez (V. Dutt, 2016) made an experiment to investigate the impact of an intrusion prevention system, in the decision-making progress. This experiment shows that the presence of this system with accuracies of 10% or 90% reduce the proportion of defending actions. Many researchers have mentioned the influences of the intrusion prevention systems on the defender's actions, although there is not so much effort on how such systems influence the cyber situational awareness. Finally, such systems could be a very effective way of creating situational awareness among the defenders.

At the active stage, the DSS uses the inputs from the other modules to identify and to evaluate the threats. In this case, the inputs are used in a rule-based system that uses not only simple IF – THEN rules, but a fuzzy-logic approach (A.F. Baba, 2009). This approach is more similar to human thinking than the traditional rule-based approaches. A fuzzy-logic approach could be more appropriate for situational awareness. In this case, all the input variables and fuzzy logic are combined to decide if a particular defence action should be triggered.

Regarding the fuzzy-logic, the variables could be both binaries (e.g 0,1) and values in ranges (e.g. 0-10). Additionally, linguistic variables could be used, which in the SPHINX's case are defined from the modules that give input to the DSS. The major advantage of this approach is that it could be adjusted to a particular infrastructure with its requirements, policies and variables. To understand the way that this system operates, a specific example is given: "IF MLID IS 1 AND SIEM Output IS Alert THEN Critical Infrastructure Status IS High". In this case, the MLID module indicates that an attack has occurred and the SIEM module raised an alarm. This state indicates a High critical infrastructure status and suggests a high level of situational awareness.

5.2 Risk Management

Cyber risk is traditionally considered as part of operational risk in corporation risk management. The approach of seeing cyber risk only applicable to the operational level was limiting the effectiveness of risk management, mostly because it was not taking into consideration several factors that play a significant role in the core value generation process of business. In today's business context, it is increasingly evident that cyber risk should be embedded into all parts of critical business risk. Moreover, the rapid pace of increasing complexity and the potential impact levels of cyber threats demand better prioritisation, availability of resources and prompt reaction than any other type of risk corporations face today.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

5.2.1 Risk assessment

Risk assessment is the initial step of risk management and constitutes the most critical and difficult phase. In order to assess the scenarios that compose the threats, a risk assessment model needs to be structured. Using a simplified interpretation, a risk assessment model can be seen as a set of rules to predict the future performance of a system from a risk perspective. Threat modelling, combined with risk management, should give answers to the question of who will attack your own systems, and how or where the attack will originate from.

Risk assessment involves all the processes that help the identification of the different risks that can have adverse effects on data integrity availability, confidentiality and in general the security of systems. This identification is heavily reliant on available data, which were described in the previous sections. These data, sent by the components like the VAaaS and SIEM along with threat detection information, provide a trove of information about cybersecurity threats. This information is multidimensional since it can provide information regarding the threats more likely to appear and materialise, but also for those that have already leveraged existing vulnerabilities. This data shall be appended by information regarding the general topology of the network. This shall enrich and contextualise the information concerning the detected threats by correlating it with information about which specific assets it will potentially affect and how it will affect them.

The main goal of any risk assessment model is to provide a relative or absolute quantification of risks in a comprehensible structure. Risk assessment and risk analysis explore the different possibilities and all the different factors that can affect them in order to quantify how likely each scenario is. In SPHINX the General Model for Incident Risk Analysis (GIRA) model will be used as the basis for both risk assessment and risk analysis and, whenever needed, adjustments shall be made (Aitor Couce-Vieira, 2017). This is an overview of the model and its nodes.

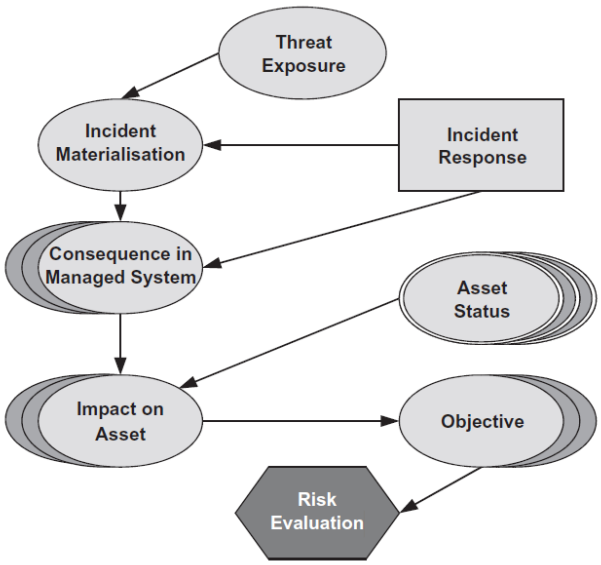

Figure 3: GIRA fundamental Model (Adopted from Aitor Couce-Vieira, 2017)

Aitor Couce-Vieira (2017) points out that most existing risk analysis methods focus on analysing risks that a system might face throughout its life. However, there is no explicit method for risk analysis during incidents. Approaches such as bow-ties and attack trees provide reliable information about triggers and escalation of incidents, but do not cover risk evaluation. Risk matrices include the entire risk analysis process; however, their risk evaluation approach is oversimplified. In the scope of SPHINX, the GIRA fundamental Model shall be

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

adopted and appropriately adapted to the needs and limitations of the project. The GIRA model, formalises the incident risk analysis process through an influence diagram, which does not rely on traditional frequentistic statistics, since they cannot easily represent the conditions of the model. Instead, Bayesian statistics and Bayesian inference are utilized, for they can more accurately reflect the various causes of modeling, allowing multi-objective optimization.

Additionally, GIRA, can support both quantitative and qualitative approaches and semi-quantitative ones. By using information gathered from the SPHINX tools and external databases, SPHINX has enough data regarding incoming threats and it is possible to utilise a semi-quantitative approach, at least during the initial threat assessment and threat exposure phases. Regarding the rest of the phases, expert opinion and the magnitude of historical data and all other required data shall be assessed in order to support a quantitative approach. The desired outcome is to deliver decision support with reliable risk information.

5.2.1.1 Threat Exposure, Vulnerabilities and Controls

The threat exposure node is responsible for presenting the likelihood of a threat appearing. Each threat exposure node instance represents a different threat. OWASP methodology shall be used for estimating likelihood through several factors. These factors are applied to CAPEC instances that form the different threats taken into account and are calculated through the data acquired from the different SPHINX tools or/and the end-users. Figure 4 depicts how these factors are interconnected in order to be estimated the Incident Materialisation likelihood.

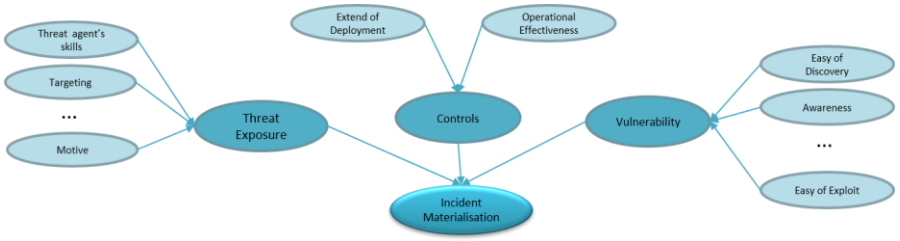

Figure 4: Likelihood estimation factors

Threat Factors

As already mentioned, SPHINX utilises the OWASP factors in order to calculate the likelihoods in the threat exposure node. SPHINX further enriches the original factors, as to better characterise the threats. All the factors have different states that are used to correspond to specific semi-quantitative and qualitative values. Those states are presented in detail the Annex I of this document. Concisely, those factors are:

- Threat Agent Factors:
  - Required adversary Skills;
  - Adversary Motive;
  - Adversary Targeting;
  - Opportunity;
  - Population Size;
  - Non-Adversarial.

To provide an initial ranking for each factor, the CAPEC's attack pattern shall be used.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

- Vulnerability Factors:
  - Easy of Discovery;
  - Ease of Exploit;
  - Awareness;
  - Intrusion Detection.

Data originating from the vulnerability assessment modules contains in its metadata information about which specific CVE affects the system. These values shall provide the relation of identified vulnerabilities with the CAPEC enumeration database.

- Controls:
  - Extend of Deployment;
  - Operational Effectiveness.

Provided the vulnerabilities any control in place shall be related. The ranking is anticipated to be inserted by the users.

5.2.2 Risk Analysis

While the risk assessment focus is on recognising different threats, risk analysis on the other hand aims to give insight on the different possible negative scenarios, their likelihood and the various mitigating measures that can be taken. Those measures contain both measures that try to avoid the materialisation of an incident all together and those that aim to lessen the negative consequences of a threat after it has materialised in the system. In Figure 5, the procedure of assessing the potential impact is presented.

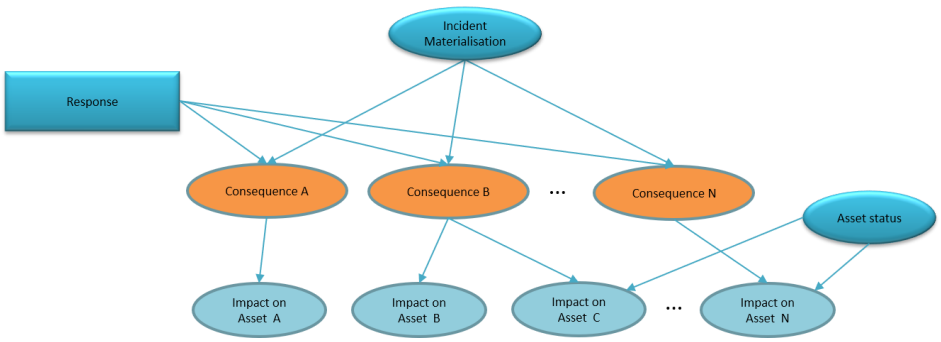

Figure 5: Impact Assessment

Risk analysis in order to be effective needs to take into account several elements.

- Risk analysis is essentially a subjective analysis, done from the point of view of the administrators of an organization. Risk assessment provides an objective view of the threats and the analysis correlates these facts with the administrators' preferences, targets and risk thresholds. Models providing that and alsosupporting this subjective view are relatively rare since most tend to focus on objectively describing the threats only.
- Many, if not most, threats that exist in cybersecurity in particular are adversarial. When dealing with this kind of threats merely characterising them by calculating the probability of them being realised is not enough. Those threats need to be modeled in attacker – defender relationships, where the reactions of attackers are taken into account. (Rios Insua, 2009).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

- In reality, whether a threat manifests itself and has negative impacts depends on many factors. Factors like mitigating actions, specific impacts and triggering events play a significant role when researching potential threats. Those factors are what give meaning to the SPHINX model, providing specific context and explaining what the results represent. Simply assigning numbers when describing a risk like it is often done when presenting a risk matrix, can prove meaningless since they are merely generalized abstractions and cannot give actionable information. (Fenton, 2012) Models should try to take into account those factors.
- It is a fact that estimating likelihoods is a hard process that may not be possible to do or often depends on subjective input from experts or has results that are not consistent when repeated. Having a robust methodology that aims to alleviate these issues is necessary. Automation can aid this process considerably, since it is often one of the most time consuming parts of the risk assessment process, although to effectively automate it, the problem needs to be well defined first. (Chapman, 2000)
- The various threats that can be detected are all significantly different from each other. As such, in order to effectively compare them and effectively communicate their effect in the system, they need to be compared to specific objectives. The usual solution in traditional risk analysis involves comparing the effects to their monetary impact, which by its own usually is not enough to accurately present the effects of a threat.

5.2.2.1 Incident Response

Each state of the incident response node represents a different proactive or reactive action that can prevent a threat from appearing all together or just mitigating some of the damage. In this case, all actions are considered disjoint among them. This node must include all relevant possible combinations of actions, including doing nothing.

In SPHINX implementation those instances will be constructed through the different solutions gathered during the risk assessment phase.

5.2.2.2 Incident Materialisation

The incident materialisation node represents the possibility that an instance of the threat exposure node, despite any controls employed in the incident response node, will escalate into an actual incident. Similar to the incident response node, events here-in can be disjoint from each other and happen simultaneously, but, in this case, these events usually modelled as consequence nodes, as outlined in the original methodology.

In SPHINX implementation, the probabilities depend on the previous probabilities produced during the threat exposure node and the modifiers in the incident materialisation node.

5.2.2.3 Consequence in the main system

The consequence node describes the likelihood that an incident will cause negative effects in the system. These consequences are linked by nature to the incident that causes them. Each incident can cause different consequences, and each one is a different instance. Each instance has different states that describe the effect of the consequence. The likelihood of a consequence materialising, is affected both by the incident materialisation, the incident response that may contain controls to mitigate certain consequences and, finally, the nature of the consequence itself.

In SPHINX's implementation, the consequences of a threat as described in the CAPEC and CWE databases will be utilised, but additional consequences shall also be introduced from the user' perspective. SPHINX also take advantage of the data structures constructed in the risk assessment phase. Using those structures, we can model, exactly what part of the system is affected by each consequence. This is useful because it allows us to immediately and easily link the consequence nodes to the impact on asset nodes.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

5.2.2.4 Asset Nodes

Asset nodes are responsible for describing the various assets in the system, with each node instance representing a single asset or a group of them. The word asset does not necessarily refer to specific physical assets. It can refer to actions and processes too. For example, an asset node can represent the capacity to perform blood tests on patients. The assets represented by those nodes depend on the granularity choosen. It is possible to focus on specific aspects of the network, like specific devices but that would make it exceedingly hard to connect the asset nodes to the business logic in further steps. That is why assets will focus on processes more closely related to the business logic, like the capability to service patients, patient status and doctor's status.

The different nodes and their states will be decided in conjunction with the SPHINX users, who have the best possible knowledge of their own processes and functionalities.

5.2.2.5 Impact on Assets

Impact on asset nodes is responsible for representing the actual impact of a consequence on an asset, depending on its state at the time of an incident. Different impacts are directly correlated with the consequences found in the previous nodes. While this will require a significant effort on their part, the list of the various consequences isn't infinite. They are directly correlated with the acquired consequences from CAPEC or/and CWE[5] or/and user additions. Furthermore, the effect of a consequence on an asset is always the same, regardless of the threat that causes it. The final likelihood depends on both the previously computed likelihood on the consequence nodes and the static nature of the relationship between a consequence and an asset status.

Finally, the synthesis of all impact levels in a small number of objectives relevant to stakeholders shall be conducted. The states each instance of the objective nodes has, typically represents its typical potential states. For example, the operational status of a clinic or the cost in money. To determine the likelihood, users need to take into account whether an impact automatically translates to a specific level and if not, how likely each objective status is, depending on the impact.

The objectives node output shall be provided to the SPHINX DSS module.

5.3 Forecasting

Recent data breaches, such as those at Target[6], JP Morgan[7], and Home Depot (SIDEL, 2014) highlight the increasing social and economic impact of such cyber incidents. For example, the JP Morgan Chase attack was believed to be one of the largest in history, affecting nearly 76 million households. Often, by the time a breach is detected, it is already too late, and the damage has already occurred. As a result, such events call into the question whether these breaches could have been predicted and the damage avoided. In this context, by performing a statistical analysis on the well-known VCDB[8] (Veris Community Database), one concludes that the majority of cybersecurity incidents that occurred in the time frame between 2000 and 2019 targeted the health sector as shown in Figure 6. And this is normal, given the great importance, sensitivity and value of healthcare and patient data. Hence, a risk forecasting module constitutes a necessary ingredient of the SPHINX risk assessment component in order to mitigate and possibly prevent such events.

[5] https://cwe.mitre.org/index.html
[6] KREBS, B. The target breach, by the numbers. http://krebsonsecurity.com/2014/05/thetarget-breach-by-the-numbers/ , May 2014.
[7] AGRAWAL, T., HENRY, D., AND FINKLE, J. JPMorgan hack exposed data of 83 million, among biggest breaches in history. http://www.reuters.com/article/2014/10/03/usjpmorgan-cybersecurity-idUSKCN0HR23T20141003, October 2014.
[8] VERIS. VERIS Community Database (VCDB). http://veriscommunity.net/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

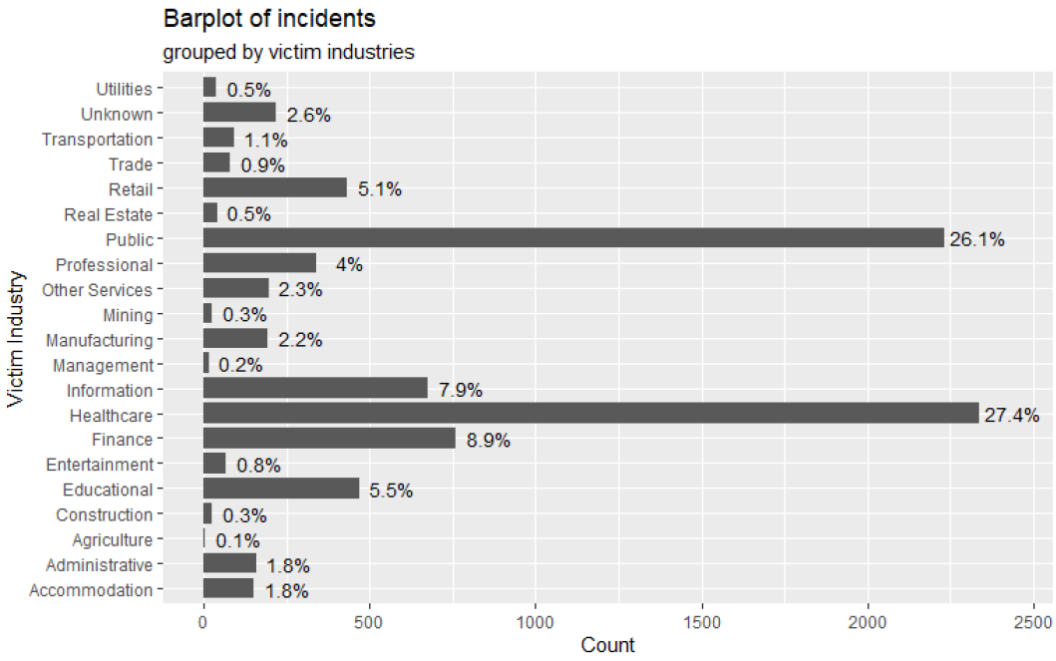

Figure 6: Veris Community Database

As already mentioned, the SPHINX Toolkit consists of components responsible for gathering data in near real time, specifically the vulnerability assessment, the honeypot and the anomaly detection components. It is of the uttermost importance that this data are collected either from the respective components or indirectly through the SIEM in order to perform statistical analysis and useful aggregations that will lead to the extraction of valuable information concerning the security posture of the system. Such information could be web mismanagement symptoms (e.g. server misconfigurations, vulnerabilities reported from the VAaaS), the rates of malicious activity inside the SPHINX network (e.g. spam, scanning and phishing activities). Thus, the Risk Forecasting submodule will combine this aggregated and internally collected data, deriving from the rest of components in conjunction with public available data on cybersecurity incidents and data breaches. Such data are available in online databases such as the ones presented below:

- VERIS Community Database (VCDB): This dataset represents a broad ranging public effort to gather cyber security incident reports in a common format. The collection is maintained by the Verizon RISK Team and is used by Verizon in its highly publicized annual Data Breach Investigations Reports (DBIR)[9]. The current repository contains more than 5,000 incident reports, that cover a variety of different types of events such as server breach, website defacements, and physically stolen assets. It is necessary to highlight that higher importance will be assigned to reported incidents that refer to the healthcare sector.
- Hackmageddon[10]: This is an independently maintained cyber incident blog that aggregates and documents various public reports of cyber security incidents on a monthly basis.
- The Web Hacking Incidents Database (WHID)[11]: This is an actively maintained cyber security incident repository; its goal is to raise awareness of cyber security issues and to provide information for statistical analysis.

The key to SPHINX's prediction framework is the construction classifiers. These classifiers are going to work either in a rule-based manner or alternatively based on machine learning and deep learning algorithms trained on features deriving from the aggregation and fusion of the aforementioned data. Hence the Risk forecasting submodule will be able to extract a vector of probabilities of future exposure to possible data breaches and

[9] VERIZON. Data Breach Investigations Reports (DBIR). http://www.verizonenterprise.com/DBIR/.
[10] PASSERI, P. Hackmageddon.com. https://www.hackmageddon.com/
[11] http://projects.webappsec.org/w/page/13246995/Web-Hacking-Incident-Database

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

specific cyber security incidents (e.g. Errors, DOS, Crimeware, Cyber Espionage). What is most important in the cyber risk forecasting framework is the continuous update on the current situation of the system and its combination with previous ones of various timeframes in order to provide valuable predictions about the future. The deployment of recurrent neural network architectures (such as LSTMs) will be seriously considered for this task.

5.4 Risk Treatment

The DSS shall evaluate the different scenarios from risk analysis. In conjunction with the inputs from other components, the DSS shall evaluate the threats. All the input variables and fuzzy logic shall be combined to decide if a particular defence action should be triggered, thus, Risk Treatment is an integrated part of the SPHINX DSS module, which shall be analytically discussed in Task 5.1.

5.5 Technical Specifications of Real-Time Risk Assessment module

In order to achieve the highest degree of interoperability with other SPHINX tools the following frameworks are selected to be used for the implementation of the Real-Time Risk Assessment component.

5.5.1 Python/Flask

Python is one of the most commonly used programming languages and as such supports a great number of plugins, ready implementations and frameworks. One of those frameworks is Flask, a web-based microframework that is incredibly versatile and lightweight since it does not require any specific tools or libraries initially and does not even have a database abstraction layer. This allows us to use only the absolute necessary libraries and packets, significantly reducing the final size of the tool and the resource usage.

In order to communicate with other SPHINX components as outlined in the SPHINX architecture (Deliverable 2.6, 2020), the innate capabilities of Flask will be utilised to create a Rest API, capable of providing data when requested. This data will mainly encompass the detailed reports produced and any alerts or notifications, that occur when certain thresholds are passed.

5.5.2 SQLite

As Flask, does not intrinsically use a specific database, this give the freedom to use any database as long as the relevant flask plugins shall be in place to resolve any compatibility issues. In SPHINX implementation SQLite database is selected.

The SQLite is often used as a test database or learning database due to its simplicity and to the lacking of capabilities that make it suitable for large scale commercial web sites. In SPHINX, those lacking capabilities do not matter, since SPHINX is essentially used as a desktop application (SQLite Consortium, n.d.). There is a possibility that the data handled by SPHINX, cross a certain threshold making the use of SQLite not optimal or even not possible, in which case SPHINX will use a more appropriate database that can handle the load of data.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

6 Visualisation, alerting and real-time information

6.1 Overview

Gathering data from a myriad of sources and systems and applying them to state of the art risk assessment and forecasting algorithms by itself doesn't achieve any of the goals set out to be met by a situational awareness framework. To fulfil those goals this information needs to somehow be communicated to the users of the systems, both to the security professionals and other members of the organisation.

Visualization of data , events and reports in cyber security has previously been the focus of a number of solutions although in the past security experts have had low numbers of adoptions of visualization technologies, mainly citing usability issues, where more "primitive" tools like Excel and command line provide more functionality and flexibility. (Fink, 2009) This doesn't mean visualisations are unnecessary on the contrary, this highlights the importance of well-designed and responsive visualisations.

More recent research has attempted to quantify and specify the different issues that arise by using visualisations (Best, 14). Specifically, those issues are:

- "Big Data"

Due to the sheer size of data produced by the various components that inhabit SPHINX's network like logs and data capture, it is expected to have similar issues such as those present in any sector handling big data. Even if users only use a subset of data each time, queries can take a lot of time, hampering the speed and responsive of SPHINX visualisations.

- Disparate and numerous data sources

With just a quick glance on the SPHINX Toolkit, it is apparent that there are a lot of different sources of data that provide information to cyber situational awareness. If using that data requires accessing many different tools or interfaces, this will lead to serious drops both in speed of the analysis and its quality. Additionally, understanding the real causes and effects among such disparate data can prove difficult, thus mechanisms should be in place to highlight those connections where available.

- Linking of data sources

Truly linking data is usually less of a purely technological issue, since most are structured and contain metadata, but correlating their different meanings and how they connect is a difficult exercise. A common way of solving this issue is using common attributes between the data sets, and basing the connections on them, the most usual attribute being time, but other data such as IPs can also serve the same purpose. Of course, such connections must be supported by the visual mediums used to project that data.

- Data quality

No proper results or decisions can be made when users doubt the data they have, whether those concerns arise from simple issues such as truncated data due to storage limits, or undelivered data due to network limitations, or more serious issues such as invalid data and quality of historic data. Especially regarding historic data, it is common to find large chunks missing. It is crucial that the visualisations can effectively deliver to the user information such as data age and source and accurately present gaps in the data, when they are missing.

- Baseline Status

Even in completely safe and healthy systems, errors and issues are always present, for those issues are naturally occurring.. While a security analyst responsible for a system may understand intrinsically which event is which, this needs to be represented or at least the necessary tools should be given to users in the visualization module,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

and especially the alerting system, in order to avoid false positives and the analysis of data that are not relevant to the situational awareness.

- Progression of threat escalation

When a security event occurs in the system, two different things need to be done. First, it is important to analyse and understand the event, how it happened and who or what was responsible. Secondly, it is mandatory to handle the consequences of that event. Visualisations can prove a liability in this regard, if there are no mechanisms that either automatically or manually allow the user to reuse and save views and states and reuse them in different data sets. In addition, visualization can support the forensic process by giving users easy or even automatic ways to incorporate mitigation measure and solutions in their views.

- Balancing Risk and Reward

There is an inherent cost when users gather information pertaining to a security event, since usually this is only one task of many. But the better users are able to analyse a problem, the better they can understand how to solve it. This allocation of resources can be aided by giving context and analyzing the risk of events, something already covered. Visualisations and alerting need to clearly present those risks and be able to build confidence in the user about its validity. They need to present the data that lead to these results as clearly as possible without misrepresentations.

6.2 Real-time information on assets, threats, logs and vulnerabilities

SPHINX contains components responsible for gathering data in near real-time as already discussed, specifically the vulnerability assessment, incidents and events management, honeypot and anomaly detection components. Those disparate data sources are generalized and linked in order to provide a better understanding of the current status of the system. Reducing the amount of data, and simultaneously providing a more specific information, helps users to comprehend a potential incident and respond more quickly to mitigate its impact. By monitoring these data flows, any deviation from the baseline status “informs” users of an unwanted event.

6.3 Key performance indicators monitoring

Key performance indicators (KPIs) are critical in translating the actual performance of the system, into actionable information that can help us understand the status of the system and guide decisions, like other forms of visualisation. In the SPHINX project, specific KPIs were outlined, developed in conjunction with the SPHINX users to best reflect their needs. Those KPIs are detailed in (Deliverable 7.1, 2020).

The risk assessment module of the situational awareness framework, in particular, can contribute significantly to those KPIs, with information about the predicted threats to the system and the number of security events. By leveraging information acquired from the other components previously described, the awareness can also contribute to other KPIs such as system availability and information about the actual resolution of security events.

6.4 Alerts and Notifications

Alerts and Notifications are vital in a situational awareness framework. Alerts and Notifications can be triggered from each individual tool in order to inform other tools or users about its state or through analysis and forecasting procedures to inform about an upcoming threat state. Especially risk-related alerts present the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

consequences of possible threats compared to their total economic impact or on other various facets like impact on workers or patients. Those alerts are triggered after the possible impact of those threats exceeds a set threshold. Those thresholds ideally are specified by the users beforehand, and they reflect the point at which taking an action about a problem becomes more important.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

7 Conclusions

This document provides the initial approach to the specifications of the SPHINX's Cyber Situational Awareness Framework. Several techniques, mechanisms, and tools shall be involved in automating many of the capabilities that have traditionally required a significant involvement of human analysts. The target is to cover as much as possible gaps and barriers towards providing an automated, seamless, secure, and precise SA, highlighted in (Deliverable 3.2, 2020). Given that currently all tools and methodologies are under the design and development phase, the degree of coverage of the target cannot be assessed; however, the broad description of this Framework can encapsulate the outcome of all SPHINX's tools. In the second version of this deliverable (D3.7 due to M30) the capabilities of each tool shall have been adequately defined, supporting a better assessment of the achieved degree of Cyber SA in SPHINX.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

8 References

A. Bar, P. C. (2014). Dbstream: an online aggregation, filtering and processing system for network traffic monitoring. *In: Proceedings of the 2014 international wireless communications and mobile computing conference*, (pp. 611–616).

A. D'Amico, M. K. (2005). "Information Assurance Visualisation for Specific Stages of Situational Awareness and Intended Uses: Lessons Learned", Workshop on Visualisation for Computer Security.

A. Stotz, M. S. (2007). Information fusion engine for real-time decision-making (INFERD): A perceptual system for cyber attack tracking. . *10th International Conference on Information Fusion.*

A.D'Amico, M. (2001). Methods of visualizing temporal patterns in and mission impact of computer security breaches. *Information Survivability Conference & Exposition II.*

A.F. Baba, D. K. (2009). Developing a Software for Fuzzy Group decision support System : A Case Study. *The Turkish Online Journal of Educational Technology, vol. 8, No. 3,* , pp 22-29.

Aitor Couce-Vieira, D. R. (2017). GIRA: a general model for incident risk analysis. *Journal of Risk Research*.

Arnborg S, A. H. (2000). Information awareness in command and control: precision, quality, utility. In: Proceedings of the Third International Conference on Information Fusion (FUSION 2000). Paris, France; ThB1/25e32.

B. McGuinness, L. F. (2000). A subjective measure of SA: the Crew Awareness Rating Scale (CARS). . *In Proc. of Human Performance, Situation Awareness and Automation: User-Centered Design for the New Millenium.*

Best, D. M. (14). Key Challenges for Visualization in Cyber Network Defense. *VizSec* (pp. 33-40). Paris, France: Association for Computing Machinery.

C. Onwubiko, T. J. (2011). Review of Situational Awareness for Computer Network Defense. *In C. Onwubiko and T.J. Owens (Eds.) Situational Awareness in Computer Network Defense: Principles, Methods and Applications*.

Chapman, C. a. (2000). Estimation and evaluation of uncertainty: A minimalist first pass approach. *International Journal of Project Management - INT J PROJ MANAG*, 369 -383.

D.Cumiford, L. (2006). Situation Awareness for Cyber Defense,. *CCRTS – The State of the Art and the State of the Practice, Sandia National Laboratories, MS 0455.*

D.J.Abadi, C. D. (2003). Aurora: a new model and architecture for data stream management. *VLDB J*, 12(2):120–139.

Deliverable 2.6. (2020). *SPHINX D2.6-SPHINX Architecture v2.*

Deliverable 3.2. (2020). *SPHINX Cyber Situation al Awareness Framework fitness/suitability- Real Time Risk Assessment Models v1.*

Deliverable 7.1. (2020). *Pilot plans including evaluation framework.*

E. McMillan, M. T. (2012). An Alternative Framework for Research on Situational Awareness in Computer Network Defense. . *Awareness in Computer Network Defense: Principles, Methods and Applications*, 71-85.

Endsley, M. (1995). "Toward a Theory of Situation Awareness in Dynamic Systems",. *Human Factors Journal,*, 37(1): 32-64.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Endsley, M. (1995). Measurement of situation awareness in dynamic systems. *Human Factors,*, 37: 65-84.

Endsley, M. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *In: Human Factors: The Journal of the Human Factors and Ergonomics Society* , 37(1): 32–64.

Endsley, M. (2001). "Designing for situation awareness in complex systems",.

Fenton, N. &. (2012). Fenton, Norman & Neil, Martin. *UPGRADE*.

Fink, G. &. (2009). Visualizing Cyber Security: Usable Workspaces. *Vizsec*.

G. Tadda, J. S. (2010). Overview of Cyber Situation Awareness. *Cyber Situational Awareness, Springer,* , 15-35.

J. Baulier, B. S. (1998). A database system for real-time event aggregation in telecommunication. *In: Proceedings of the 24th international conference on very large data bases,*, (pp. pp 680–684).

J. F. Buford, L. L. (2008). Insider threat detection using situation-aware MAS. . *11th International Conference on Information Fusion.*

J. Yen, M. M. (2010). RPD-based Hypothesis Reasoning for Cyber Situation Awareness. *Cyber Situational Awareness: Issues and Research, Springer.*, 39-49.

K.E. Weick, K. S. (2005). Organizing and the process of sensemaking. . *Organization Science*, 16(4).

M.R. Endsley, J. D. (2012). *Designing for situation awareness: An approach to human-centered design (2nd ed.).* London, : UK: Taylor & Francis.

M.W.Boyce, K. M.-R. (2011). Human Factors and Ergonomics Society 55th Annual Meeting.

N.A. Stanton et al. (2006). Distributed situation awareness in dynamic systems: theoretical development and application of an ergonomics methodology. *Ergonomics,*, 49(12-13): 1288-1311.

N.A. Stanton, P. S. (2009). Is situation awareness all in the mind? *Theoretical Issues in Ergonomics Science,*, 11(1-2): 29-40.

Rios Insua, D. J. (2009). Adversarial Risk Analysis. *Journal of the American Statistical Association*, 841 - 854.

S. J. Yang, A. S. (2009). High level information fusion for tracking and projection of multistage cyber attacks. . *Information Fusion*, 10(1): 107-121.

S. Jajodia, P. L. (2010). Cyber Situational Awareness.

SIDEL, R. (2014). Home depot's 56 million card breach bigger than target's.

SQLite Consortium. (n.d.). Retrieved from SQLite: https://www.sqlite.org/whentouse.html

V. Dutt, F. M. (2016). Role of intrusion-detection systems in cyber-attack detection. . *In Advances in Human Factors in Cybersecurity, Springer*, (pp. 97-109).

X. Peng, J. L. (2010). Using Bayesian networks for cyber security analysis. . *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN).*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Annex I: **Likelihood and Impact Factors**

Required adversary Skills

	Semi- Quantitative Values	Qualitative Values	Description
Not Applicable	0	Very Low	
Security penetration skills	0.2	Low	
Network and programming skills	0.4	Moderate	
Advanced computer user	0.6	High	
Advanced technical skills	0,8	Very High	
No technical skills	1	Catastrophic	
Default	0.6		
Undefined	0.5		

Adversary Motive

	Semi- Quantitative Values	Qualitative Values	Description
Not Applicable	0	Very Low	
Low or no reward	0.2	Low	
Possible reward	0.4	Moderate	
High reward	0.6	High	
High-value reward	1	Very High	
Default	0.6		
Undefined	0.5		

Adversary Targeting

	Semi- Quantitative Values	Qualitative Values	Description
Not Applicable	0	Very Low	not target any specific organizations or classes of organizations.
low-value reward	0.2	Low	target a class of high-value organizations or information, and seeks targets of opportunity within that class.
high-value reward	0.4	Moderate	target persistently specific high-value organizations or information
High reward	0.6	High	target persistently a specific organization, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

	Semi- Quantitative Values	Qualitative Values	Description
High-value reward	1	Very High	target persistently a specific organization, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions; specific employees or positions; supporting infrastructure providers/suppliers; or partnering organizations.
Default	0.6		
Undefined	0.5		

Opportunity

	Semi- Quantitative Values	Qualitative Values	Description
Full access	0	Very Low	full access is needed or expensive resources required
Special access	0.2	Low	Special access or resources required
Some access	0.4	Moderate	Some access or resources required
Common access	0.6	High	Common access or resources required
No access	1	Very High	No access or resources required
Default	0.6		
Undefined	0.5		

Population Size

	Semi- Quantitative Values	Qualitative Values	Description
Not Applicable	0	Very Low	
System Administrators	0.2	Low	
Intranet users	0.4	Moderate	
Partners	0.6	High	
Authorised users	0.8	Very High	
Anonymous Internet users	1	Catastrophic	
Default	0.6		
Undefined	0.5		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Non Adversarial

	Semi- Quantitative Values	Qualitative Values	Description
Minimal effect or Not Applicable	0	Very Low	The effects of the error, accident, or act of nature are minimal
Limited effect	0.2	Low	The effects of the error, accident, or act of nature are limited
Low-ranging effect	0.4	Moderate	The effects of the error, accident, or act of nature are low-ranging
Wide-ranging effect	0.6	High	The effects of the error, accident, or act of nature are wide-ranging
Extensive effect	0.8	Very High	The effects of the error, accident, or act of nature are extensive
Catastrophic effect	1	Catastrophic	the effects of the error, accident, or act of nature are catastrophic
Default	0.6		
Undefined	0.5		

Easy of Discovery

	Semi- Quantitative Values	Qualitative Values	Description
Not Applicable	0	Very Low	
Automated tools available	0.2	Low	
Easy	0.4	Moderate	
Difficult	0.6	High	
Practically impossible	1	Very High	
Default	0.6		
Undefined	0.5		

Ease of Exploit

	Semi- Quantitative Values	Qualitative Values	Description
Not Applicable	0	Very Low	
Theoretical	0.2	Low	
Difficult	0.4	Moderate	
Easy	0.6	High	
Automated tools available	1	Very High	
Default	0.6		
Undefined	0.5		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Awareness

	Semi- Quantitative Values	Qualitative Values	Description
Not Applicable	0	Very Low	
Unknown	0.2	Low	
Hidden	0.4	Moderate	
Obvious	0.6	High	
Common/public knowledge	1	Very High	
Default	0.6		
Undefined	0.5		

Intrusion Detection

	Semi- Quantitative Values	Qualitative Values	Description
Not Applicable	0	Very Low	
Active detection	0.2	Low	
Logged and reviewed	0.4	Moderate	
Logged without reviewed	0.6	High	
Not logged	1	Very High	
Default	0.6		
Undefined	0.5		

Extend of Deployment

	Semi- Quantitative Values	Qualitative Values	Description
Global - Not Applicable	0	Very Low	
Wide - ranging	0.2	Low	
Low - ranging	0.4	Moderate	
Limited	0.6	High	
Occasional	1	Very High	
Default	0.6		
Undefined	0.5		

Operational Effectiveness

	Semi- Quantitative Values	Qualitative Values	Description
Not Applicable	0	Very Low	
Full fledged	0.2	Low	
Medium fledged	0.4	Moderate	
Small fledged	0.6	High	
Occasional	1	Very High	
Default	0.6		
Undefined	0.5		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.