CYBERSANE

D10.1

Evaluation and Benchmarking Methodology

Project number:	833683
Project acronym:	CyberSANE
Project title:	Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures
Start date of the project:	1st September, 2019
Duration:	36 months
	H2020-SU-ICT-2018

Deliverable type:	Report
Deliverable reference number:	DS-01-833683 / D10.1/ N.1
Work package contributing to the deliverable:	WP 10
Due date:	10 2021 – M26
Actual submission date:	31 October 2021

Responsible organisation:	STS
Editor:	Konstantinos Kontakis
Dissemination level:	PU
Revision:	N.1

Abstract:	This report aims at providing the appropriate evaluation and benchmarking methodologies which are going to be leveraged for the stakeholders', technical, and business evaluation of the CyberSANE platform
Keywords:	Socio-economic and Techno-economic Evaluation, Usability Evaluation, KPI Properties, User and Technical Evaluation Templates
	The project CyberSANE has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833683.

Editor

Konstantinos Kontakis (STS)

Contributors (ordered according to beneficiary numbers)

Luís Landeiro Ribeiro (PDMFC)

Oleksii Osliak (CNR)

Armend Duzha, Menia Hatzikou (MAG)

Dr. Sophia Karagiorgou, George Pantelis, Petros Petrou (UBI)

Matej Kovacic (JSI)

Anthi Barmpaki, Eva Papadogiannaki, Kostas Georgopoulos (FORTH)

Andreas Miaoudakis, Konstantinos Kontakis, Sofia Spanoudakis, Tzortzia Koutsouri (STS)

Ana Maria Corrêa Harcus, Burcu Yaşar (KU LEUVEN)

Ángel Laguna Argente, Pablo Giménez Salazar (VPF)

Diarmuid O Connor, Filippo Bellini (LSE)

Dr. Lena Griebel (KN)

Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Executive Summary

The main objective of CyberSANE project is to provide a state-of-the-art cyber-security incident handling system, capable of dealing even with the most advanced cyber-threats targeting the European Critical Infrastructures (Papastergiou, et al., 2019). Therefore, the thorough and efficient evaluation of the CyberSANE framework and its components plays an essential role towards the realisation of project's main objective. In this report we present the evaluation and benchmarking methodology which will be followed in the rest of WP10 Tasks, as well as to WP9 Tasks due to its close relationship and interconnection with the workshop sessions and real-life demonstrations held there. The evaluation of CyberSANE framework will take into consideration several aspects of the system and the work done in the technical WPs of the project, adopting a series of methodologies, tools, and instruments for the analysis of data, the technical evaluation, and the business evaluation of the system and its components. The aforesaid analysis and evaluation will be done by security experts within the consortium in the context of T10.2 and T10.3, with the definition and evaluation process being described in T10.1.

Contents

List of Tables

Chapter 1 Introduction

This deliverable presents the findings and work performed in Task 10.1. We describe project's evaluation and benchmarking methodology by presenting several instruments and tools to sufficiently cover the evaluation of socio-economic, techno-economic, and usability aspects. Furthermore, special caution was also taken for the description of the template that will be followed regarding the future validation and benchmarking of CyberSANE's Key Performance Indicators (KPIs) defined in T2.4 of WP2, as well as for the user and technical requirements' evaluation defined in deliverable D2.3. Therefore, all tools and methodologies provided in this report are closely interconnected with the next two Tasks of WP10 and aim to serve as the basis for their expected outcomes. T10.2 shall receive and analyse the feedback received by stakeholders in terms of the CyberSANE Incident Handling approach, while the actual technical and business evaluation of the CyberSANE framework will take place in T10.3. The rest of this document is structured as follows:

- Chapter 2 describes the socio-economic and techno-economic evaluation of the CyberSANE framework
- Chapter 3 documents the KPI evaluation properties
- Chapter 4 describes the user and technical requirements' evaluation
- Chapter 5 features the concluding remarks of this deliverable
- Chapter 6 includes a glossary of the most commonly used abbreviations
- Chapter 7 concludes with all the bibliography of this deliverable
- Annex 1 includes the technical users' questionnaire
- Annex 2 includes the non-technical users' questionnaire

Chapter 2 Socio-economic & Techno-economic Evaluation

The socio-economic and techno-economic evaluation involved the creation of two general validation questionnaires which aim to measure the usefulness and practicability of the CyberSANE framework and its components. These two questionnaires were developed with the contribution of all consortium members and are going to be utilized in the upcoming workshop sessions of CyberSANE project. Their structure and the formulation of their questions was based on a set of recommendations that involved:

i. keeping the questions and statements as simple and short as possible
ii. questioning the interviewee one aspect or objective each time
iii. making use of an easy-to-understand language but with precise terminology
iv. making sure that the interviewee fully understands the context of the statement
v. avoiding overwhelming questionnaires with unnecessary, out-of-scope, or akin questions

Both questionnaires' objective is to identify potential problems and receive qualitative feedback from both technical and non-technical users in the context of Critical Infrastructures (CIs) and Critical Information Infrastructures (CIIs). We decided that these groups of users should have a different questionnaire, with each one including specific questions matching their expertise on cyber-security domain and business area of interest. In this way, we shall be able to properly receive and analyse an unbiased feedback based on their point-of-view on CyberSANE system. At this point, it is worth noticing that the perceived usability derives by the standardized statements of the System Usability Scale questionnaire (Lewis, 2018). As stated on introduction section as well, the outcomes of these two questionnaires will serve as the basis for the data analysis and stakeholders' evaluation, as well as the technical and business evaluation, which will take place on T10.2 and T10.3 respectively.

2.1 Technical Users' Questionnaire

The technical-related questionnaire targets end-users who shall be actively engaged in the demonstration of project's pilots and are quite experienced in the cyber-security domain, including but not limited to Computer Security Incident Response Teams (CSIRTs), Security Operations Centre (SOC) operators, IT engineers, or other types of cyber-security experts. All these users are expected to have sufficient technical knowledge and are responsible for setting up, monitoring, and maintaining an organisation's IT systems. Therefore, such users are deemed ideal for presenting them a prototype of the CyberSANE framework, let them navigate, interact with the system, and test as many as possible functionalities of the system.

Since technical users possess extensive knowledge in cyber-security domain, their feedback in these specific categories is of high importance for us and will be taken into consideration for potential enhancements or changes of the services provided through CyberSANE framework. The technical users' questionnaire comes with 8 question categories and 54 questions in total. Table

1 below displays all the categories that ultimately compose our technical users' questionnaire, followed by the number of questions which are contained in each category, respectively.

Category Name	Number of Questions
General Information	4
Architecture	6
Usability and Efficiency	13
Security and Results Quality	8
Legal and Ethical Compliance	15
Contract and Economic	3
External Communication	2
Other Comments	3

Table 1: Technical Users' Questionnaire Structure

It quickly becomes evident that the vast majority of these questions are focused on the architecture, usability, efficiency, security, and results quality of the CyberSANE system. Most answer options to these questions adopt the following range of options, covering all the possible responses an interviewee could request:

- Strongly agree
- Agree
- Neither agree, nor disagree
- Disagree
- Strongly disagree
- Do not know, not applicable

However, there are of course questions which come with another predefined set of answer options specific to that question alone (e.g., questions falling under "General Information" category), while a few others offer a free text area to the user in order to write down his response or provide his generic comments (e.g., questions falling under "Other Comments" category). The finally assembled questionnaire for the technical users of the CyberSANE platform can be seen at "Annex 1. Technical Users' Questionnaire" of this deliverable.

As mentioned, usability measurements will be included in the questionnaire for the technical users. To enriching this, there is the possibility of using more qualitative measurements as well during the pilot workshops where participating security experts might assess certain aspects of the CyberSANE prototype by performing user-based usability testing approaches, such as thinking aloud tests or focus group discussions.

2.2 Non-Technical Users' Questionnaire

The non-technical questionnaire involves users who possess quite limited or no experience in the cyber-security domain and are expected to face difficulties in operating adequately the CyberSANE platform at its whole. This type of questionnaire targets a wider audience of participants where a tutorial or video presentation of the platform should take place in advance, covering thus all participants and interested parties of our upcoming workshop sessions. In contrast to the technical users of the previous questionnaire, this group of users are not expected to have a live engagement with CyberSANE platform, mainly due to their lack of prior knowledge in cyber-security domain. However, such users are usually stakeholders that play an essential role in the daily operations and functionality of a CI or CII. So, the non-technical questionnaire comes with 7 question categories and 32 questions in total. Table 2 below displays all the categories which compose our non-technical users' questionnaire, followed by the number of questions included in each category.

Category Name	Number of Questions
General Information	4
Usability and Efficiency	4
Security and Results Quality	2
Legal and Ethical Compliance	15
Contract and Economic	4
External Communication	1
Other Comments	3

Table 2: Non-Technical Users' Questionnaire Structure

In this type of questionnaire, most questions (or statements) are mainly oriented towards the organisational and managerial aspects of an organisation. However, we decided to include a set of trivial and easy-to-answer questions about the usability, efficiency, and security of the presented system. Doing so, we will be also able to retrieve feedback on these features from the perspective of unskilled and non-technical users. Regarding the availability of answer options, most answers share the same satisfactory levels as described in the previous section of this chapter, ranging from "Strongly agree" to "Do not know, not applicable". Once more, this questionnaire comes as well with a couple of questions that adopt another set of answer options, or a free text area to be filled out by the interviewee. The non-technical users' questionnaire can be found and reviewed at "Annex 2. Non-Technical Users' Questionnaire" of this deliverable, while the analysis of the questionnaire outcomes will be done on another Task.

Chapter 3 KPI Evaluation

In this chapter we revisit the KPIs described in T2.4 and present the set of properties which are going to be used for their future evaluation and benchmarking. All these KPIs are closely related to one or more CyberSANE components and intend to assess their functionality in an objective manner. Each KPI has been attributed with an “Id”, “Name”, “Description”, and “Units” attribute to differentiate them. All KPIs’ assessment will take place by deploying a specific methodology or tool defined in section 3.1, aiming to satisfy a baseline value based on its unit attribute. In the vast majority of cases, this value is measured directly (i.e., number, percentage, or time), but there also occasions where the unit is not a metric, and the validation should be conducted through a short survey or questionnaire.

Id	Name	Description	Units
KPI_1	Incidents detected	The number of security incident detected by the tools provided by LiveNet/DarkNet/HybridNet	Number
KPI_2	False positives rate	The false positive rate for detected security incidents	Percentage
KPI_3	Adoption rate	Percentage of assets protected by CyberSANE (vs total number of assets of an organization)	Percentage
KPI_4	Security incidents response time	The average time it takes to respond to an incident for assets protected by CyberSANE	Time
KPI_5	Security incidents solving time	The average time it takes to respond & recover from a security incident for assets protected by CyberSANE	Time
KPI_6	Availability of CyberSANE platform	Percentage of actual uptime (in hours) of CyberSANE relative to the total numbers of planned uptime (in hours).	Percentage
KPI_7	Real Incidents shared	Percentage of security reported incidents shared with other entities	Percentage
KPI_8	Decision informed by shared incidents	Number of decisions taken due to information gathered from security incident reports provided by CyberSANE	Survey
KPI_9	Impressions on Incidents Shared	Number of users that consumed the CyberSANE shared incident reports	Number
KPI_10	Set up time	Average time it takes to integrate a new information source	Time
KPI_11	Onboarded Information sources	Number of distinct information source integrated with CyberSANE	Number
KPI_12	Supported out of the box source types	The number of distinct information sources, supported out of the box without requiring custom developments	Number
KPI_13	Incidents mined in the Dark Web	The number of security incidents detected from mining the Dark Web	Number

KPI_14	Events identified in media	The number of cybersecurity incidents detected from mining media articles, blog posts, and social media	Number
KPI_15	Social media sources crawled	The number of distinct social media sources crawled by DarkNet	Number
KPI_16	Models' training	The average time it takes to train a HybridNet model	Time
KPI_17	Models' lifetime	Time average time span an HybridNet model is valid and useful	Time
KPI_18	Monthly active users	The number of users that logged into the platform (by month)	Number
KPI_19	Security policies	The number of security policies defined by the CyberSANE components, it provides an indicator for how complete and deep the project is	Number
KPI_20	Privacy rules defined	The number of privacy rules defined that are used to protect sensitive data shared between multiple components or entities	Number
KPI_21	Incident anonymized	The number of incident reports anonymized to scrap sensitive data	Number
KPI_22	User tool satisfaction evaluation	Evaluate the user satisfaction score, from a scale of 1 (low) to 10 (very) measure how satisfied a user is with the provided tools	Survey

Table 3 below lists all KPIs which are going to be provided with such an evaluation methodology, as a mean to partially test, analyze, and measure the success of the project.

Id	Name	Description	Units
KPI_1	Incidents detected	The number of security incident detected by the tools provided by LiveNet/DarkNet/HybridNet	Number
KPI_2	False positives rate	The false positive rate for detected security incidents	Percentage
KPI_3	Adoption rate	Percentage of assets protected by CyberSANE (vs total number of assets of an organization)	Percentage
KPI_4	Security incidents response time	The average time it takes to respond to an incident for assets protected by CyberSANE	Time
KPI_5	Security incidents solving time	The average time it takes to respond & recover from a security incident for assets protected by CyberSANE	Time
KPI_6	Availability of CyberSANE platform	Percentage of actual uptime (in hours) of CyberSANE relative to the total numbers of planned uptime (in hours).	Percentage
KPI_7	Real Incidents shared	Percentage of security reported incidents shared with other entities	Percentage
KPI_8	Decision informed by shared incidents	Number of decisions taken due to information gathered from security incident reports provided by CyberSANE	Survey

KPI_9	Impressions on Incidents Shared	Number of users that consumed the CyberSANE shared incident reports	Number
KPI_10	Set up time	Average time it takes to integrate a new information source	Time
KPI_11	Onboarded Information sources	Number of distinct information source integrated with CyberSANE	Number
KPI_12	Supported out of the box source types	The number of distinct information sources, supported out of the box without requiring custom developments	Number
KPI_13	Incidents mined in the Dark Web	The number of security incidents detected from mining the Dark Web	Number
KPI_14	Events identified in media	The number of cybersecurity incidents detected from mining media articles, blog posts, and social media	Number
KPI_15	Social media sources crawled	The number of distinct social media sources crawled by DarkNet	Number
KPI_16	Models' training	The average time it takes to train a HybridNet model	Time
KPI_17	Models' lifetime	Time average time span an HybridNet model is valid and useful	Time
KPI_18	Monthly active users	The number of users that logged into the platform (by month)	Number
KPI_19	Security policies	The number of security policies defined by the CyberSANE components, it provides an indicator for how complete and deep the project is	Number
KPI_20	Privacy rules defined	The number of privacy rules defined that are used to protect sensitive data shared between multiple components or entities	Number
KPI_21	Incident anonymized	The number of incident reports anonymized to scrap sensitive data	Number
KPI_22	User tool satisfaction evaluation	Evaluate the user satisfaction score, from a scale of 1 (low) to 10 (very) measure how satisfied a user is with the provided tools	Survey

Table 3: CyberSANE's KPI List

3.1 KPI Evaluation Properties

The evaluation of CyberSANE's KPIs involves the definition of a set of properties which reflect common aspects that must be taken into consideration across all KPIs. Some of these properties aim to identify and differentiate each KPI, while others exclusively focus on the suggested instrument, tool, or methodology that will be used for that KPI's evaluation and benchmarking. All KPIs will be assigned to one or more consortium partners who either possess the relative expertise to evaluate that KPI, or they actually own the underlying component being evaluated. For that reason, a mapping of the engaged CyberSANE components will also take place to guarantee efficient evaluation. The components' mapping property is followed by the definition of the methodology and tools. They are going to be applied towards evaluating that KPI, while the baseline value property acts as a target value that must be satisfied during our assessment process. This baseline metric will be derived from trustworthy sources of information and will be based on literature finding, research studies, or the hands-on experience of appropriate consortium partner(s). Finally, we provide an additional property set which aim at recording the outcomes of each evaluation, the date upon which the evaluation took place, and a point of contact for historical, reference, and feedback purposes. The final list of the chosen KPI properties, along with a short property description, is presented below in Table 4. Before proceeding to the actual evaluation of the KPIs defined in T2.4, we consider this tabular set-up and provide each KPI with its own dedicated properties' table in cooperation with all consortium members. Therefore, this template is going to be used as a point of reference for the imminent technical evaluation and benchmarking of CyberSANE system in the upcoming Tasks of WP10.

Property Name	Property Description
ID	Identifier of the KPI
Description	Description of the KPI to be evaluated
Evaluation Strategy	The applied evaluation strategy (i.e., test-based, domain expert evaluation, questionnaires, etc.)
Responsible Partner(s)	Consortium partners who are responsible for the evaluation of this KPI
Components Mapping	Specify the CyberSANE components which fall under this KPI, and the evaluation strategy followed for each one (if multiple)
Methodology and Tools	Brief description of the performed evaluation (i.e., what kind of test cases were implemented, any literature or documentation used for the evaluation, third-party tools used, etc.)
Baseline Values	Baseline values for the evaluation (if applicable)
Evaluation Outcomes	Outcomes of the evaluation (i.e., success or failure in terms of baseline values, full or partial coverage, etc.)
Evaluation Date and Contact	Specify the evaluation date, as well as the email of the responsible partner

Table 4: KPI Properties Table

Considering the requirements status analysis done on the aforementioned KPIs as the project progresses over time, we were able to identify and attribute each KPI with its appropriate set of owner(s) and component(s). Therefore, an enhanced version of CyberSANE's KPI list can be viewed on Table 5, with the values depicted in the last two columns of this table to correspond to the properties of *Responsible Partner(s)* and *Components Mapping*, respectively. The rest of KPI properties (like details, configuration, and justifications about their evaluation and benchmarking techniques) shall be provided at the deliverable "D10.3 Technical and Business" during the evaluation phase of CyberSANE platform from a technical, technological, usability, and business perspective.

Id	Name	Component	Owner
KPI_1	Incidents detected	LiveNet/DarkNet/HybridNet	S2/JSI/ATOS
KPI_2	False positives rate	LiveNet	S2
KPI_3	Adoption rate	LiveNet	S2
KPI_4	Security incidents response time	All	All
KPI_5	Security incidents solving time	All	All
KPI_6	Availability of CyberSANE platform	All	All
KPI_7	Real Incidents shared	ShareNet	CNR
KPI_8	Decision informed by shared incidents	ShareNet	CNR
KPI_9	Impressions on Incidents Shared	ShareNet	CNR
KPI_10	Set up time	All	All
KPI_11	Onboarded Information sources	LiveNet	S2
KPI_12	Supported out of the box source types	LiveNet	S2
KPI_13	Incidents mined in the Dark Web	DarkNet	JSI
KPI_14	Events identified in media	DarkNet	JSI
KPI_15	Social media sources crawled	DarkNet	JSI
KPI_16	Models' training	HybridNet	ATOS
KPI_17	Models' lifetime	HybridNet	ATOS
KPI_18	Monthly active users	All	All
KPI_19	Security policies	ShareNet	CNR

KPI_20	Privacy rules defined	PrivacyNet	PDMFC
KPI_21	Incident anonymized	PrivacyNet	PDMFC
KPI_22	User tool satisfaction evaluation	All	All

Table 5: KPI Components & Owners

Chapter 4 User & Technical Requirements Evaluation

Besides CyberSANE's KPI list presented in the previous section of deliverable, an efficient evaluation of the system must consider the user requirements and technical requirements previously derived in deliverable "D2.3 User and Stakeholders Requirements and Reference Scenarios". The requirements' analysis and prioritisation followed in that report was based on the feedback received by a requirements-focused questionnaire and the MoSCoW methodology (Tudor & Walter, 2006), resulting thus to the definition of 52 user requirements and 73 technical requirements. In contract to CyberSANE's KPI list, we are not going to present each one of them in this report, both due to their multitude and because an extensive description of them already took place in that deliverable. Inside this chapter we provide an enhanced version of the initially proposed template, capable of efficiently measuring the outcomes of each requirement and deduct if CyberSANE platform has successfully met these requirements or not.

4.1 User Requirements Evaluation

The user requirements evaluation template considers all those characteristics which were firstly presented in section 2.1.7 of deliverable D2.3, namely the *ID*, *MoSCoW Priority*, *Score*, *Description*, and *Comment* properties. However, it further extends them by including an additional set of properties for the efficient evaluation of any user requirement, which are no other than the *Methodology and Tools*, *Evaluation Outcomes*, *Summary of Failure*, and *Evaluation Date and Contact* properties. A short description about the characteristics of each property along with the potential values they could receive, is depicted on Table 6 below.

ID	Identifier of the user requirement	**MoSCoW Priority**	Importance of the user requirement
		Score	The final average value
Description	Explanation of the user requirement to be evaluated		
Methodology and Tools	Brief description of the performed evaluation (i.e., what kind of test cases were implemented, any literature or documentation used for the evaluation, third-party tools used, etc.)		
Evaluation Outcomes	Outcomes of the evaluation (i.e., pass, failure, or untested)	**Summary of Failure**	Short description about the failed evaluation outcome (if applies)
Evaluation Date and Contact	Specify the evaluation date, as well as the email of the responsible partner		

Comment	Additional information worth mentioning about user actions, exclusions, system requirements, etc.

Table 6: User Requirements Evaluation Template

4.2 Technical Requirements Evaluation

The technical requirements evaluation template considers all those characteristics which were firstly presented in section 2.1.8 of deliverable D2.3, namely the *ID*, *MoSCoW Priority*, *Type*, *IT Domain*, *CSMC Function*, *Name*, *Description*, and *Use Cases* properties. However, it further extends them by including an additional set of properties for the efficient evaluation of any technical requirement, which are no other than the *Methodology and Tools*, *Evaluation Outcomes*, *Summary of Failure*, and *Evaluation Date and Contact*, and *Comment* properties. A short description about the characteristics of each property along with the potential values they could receive, is depicted on Table 7 below.

ID	Identifier of the technical requirement	**MoSCoW Priority**	Importance of the technical requirement
		Type	Type of the requirement (i.e., functional or non-functional)
IT Domain	Domain of the technical requirement	**CSMC Function**	Categorisation of the technical requirement (i.e., Identify, Protect, Detect, Respond, or Recovery)
Name	A self-explanatory name of the technical requirement		
Description	Explanation of the technical requirement to be evaluated		
Use Cases	Relationship of the technical requirement with a predefined use case		
Methodology and Tools	Brief description of the performed evaluation (i.e., what kind of test cases were implemented, any literature or documentation used for the evaluation, third-party tools used, etc.)		
Evaluation Outcomes	Outcomes of the evaluation (i.e., pass, failure, or untested)	**Summary of Failure**	Short description about the failed evaluation outcome (if applies)
Evaluation Date and Contact	Specify the evaluation date, as well as the email of the responsible partner		
Comment	Additional information worth mentioning about user actions, exclusions, system requirements, etc.		

Table 7: Technical Requirements Evaluation Template

Chapter 5 Conclusions

In this deliverable we described the necessary evaluation and benchmarking methodologies which are going to be followed in the upcoming Tasks of WP10, as the medium to evaluate the CyberSANE framework at its whole. At first, we created two different questionnaires for the socio-economic and techno-economic evaluation of the platform, providing several questions for the technical and non-technical users of our expected workshop sessions. Furthermore, the real-life demonstration of CyberSANE system which will take place for the needs of WP9 activities, shall also consider the feedback received by several external security experts. Such experts will be invited in advance and will have a thorough presentation and interaction with the platform, to be able to provide an as realistic as possible evaluation of the progress made so far. Afterwards, we presented our usability evaluation methodology in the context of effectiveness and convenience, followed by the provision of a properties table for the evaluation of the previously defined CyberSANE's KPI list. Finally, we revisited the user and technical requirements list derived from the relative user and stakeholders' requirements deliverable (D2.3), to provide an appropriate methodology to efficiently measure them.

The work presented where will be used as foundation to allow all evaluation and benchmarking methodologies for the next deliverables in this work package. They will provide the necessary results, or so to speak, the basis for the multi-purpose evaluation realized by T10.2 and T10.3.

Chapter 6 List of Abbreviations

Abbreviation	Translation
CI(s)	Critical Infrastructure(s)
CII(s)	Critical Information Infrastructure(s)
CSIRT(s)	Computer Security Incident Response Team(s)
CSMC	Cyber Security Management Center
KPI(s)	Key Performance Indicator(s)
MoSCoW	The Moscow method is a prioritization technique used in management, business analysis, project management, and software development to reach a common understanding with stakeholders on the importance they place on the delivery of each requirement; it is also known as MoSCoW prioritization or MoSCoW analysis.
SOC	Security Operations Centre

Chapter 7 Bibliography

Lewis, J. R., 2018. The System Usability Scale: Past, Present, and Future. *International Journal of Human–Computer Interaction,* 34(7), pp. 577-590.

Papastergiou, S., Mouratidis, C. & Kalogeraki, E., 2019. *Cyber Security Incident Handling, Warning and Response System for the European Critical Information Infrastructures (CyberSANE).* Xersonisos, Greece, Springer, Cham, pp. 476-487.

Tudor, D. & Walter, G. A., 2006. *Using an agile approach in a large, traditional organisation.* Visegrád, IEEE Computer Society, pp. 367-373.

Annex 1. Technical Users' Questionnaire

1. General Information

Question / Statement

1.1. What is your organisation's type?

Answer Options

○ Public ○ Small medium enterprise ○ Large enterprise ○ Other private organisation

Question / Statement

1.2. What is your organisation's area of interest?

Answer Options

○ Logistics ○ Energy provider ○ Healthcare operator ○ Bank and insurances

○ Telecommunications ○ Law-enforcement ○ Academia and R&D ○ Cyber-security

○ Technology provider ○ Other Critical Infrastructure or Critical Information Infrastructure

Question / Statement

1.3. What is your current position in your organisation?

Answer

Question / Statement

1.4. What kind of cyber-security activities do you undertake in your organisation?

Answer Options

○ None ○ Incident response tasks ○ Forensic analysis ○ Vulnerabilities' Assessment

○ Other type of activity, please specify:

2. Architecture

Question / Statement

2.1. I think that CyberSANE framework provides a comprehensive overview and management of all its components

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

2.2. I think that the functionalities offered by all CyberSANE components are well integrated into the architecture

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

2.3. I think that CyberSANE can interoperate with other existing systems in my organisation with a minimum effort

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

2.4. I think that CyberSANE can interoperate with other security policies in my organisation with a minimum effort

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

2.5. I think that CyberSANE could replace one or more existing security components of my organisation

Answer Options

○ Yes, one component could be replaced ○ Yes, more components could be replaced

○ Yes, all components could be replaced ○ No, no components could be replaced

Question / Statement

2.6. If you disagree or strongly disagree with the question 2.5, then please state potential hindrances to replace your existing solution(s) with the CyberSANE framework?

Answer

3. Usability and Efficiency

Question / Statement

3.1. I think that CyberSANE framework is easy and intuitive to use on a daily basis

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

3.2. I think that CyberSANE is more efficient and effective in terms of time spend

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

3.3. I think that CyberSANE’s dashboard is easy-to-navigate and provides a comprehensive, unified overview of all its components

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

3.4. I think that CyberSANE’s dashboard comes with advanced visualization and interactive control processes, as well as detailed reports to the system users

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

3.5. I found that framework’s information and alerting capabilities are helpful enough and clearly viewable

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

3.6. I am satisfied with the performance of the system in terms of speed

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

3.7. I found the system unnecessarily complex and cumbersome to use

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

3.8. If you encountered systemic errors and application crashes during the execution of tasks, then please provide your feedback about such errors/crashes below

Answer

Question / Statement

3.9. I think that CyberSANE features all the functionalities expected from a cyber-security system

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Report possible missing functionalities:

Question / Statement

3.10. I think that I would find CyberSANE useful in my tasks at work

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

3.11. If you disagree or strongly disagree with the question 3.10, then please state why you would not find CyberSANE useful in your tasks at work

Answer

Question / Statement

3.12. I think that it would be easy for me to become skilful at using CyberSANE system

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

3.13. If you disagree or strongly disagree with the question 3.11, then please mention below the biggest barriers towards becoming skilful on CyberSANE system

Answer

4. Security and Results Quality

Question / Statement

4.1. I think that CyberSANE provides faster identification and better classification of security threats compared to the existing deployed solution within my organisation

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

4.2. I think that CyberSANE framework enables the faster reaction and lowers the average time needed to respond to a cyber-threat

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

4.3. I found that CyberSANE provides an improved decision support mechanism which improves the situational awareness about my organisation

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

4.4. I think that the correlation of incidents and the cascading effects of a security incident are easy-to-notice and are presented in an understandable way

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

4.5. I found that CyberSANE allows the prioritization of alerts, security incidents, and recovery actions
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
4.6. I think that CyberSANE improves the internal collaboration and information sharing of security incidents between different teams and operators
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
4.7. I found that CyberSANE enables the efficient protection against cyber-threats and can sufficiently cover the cyber-security needs of my organisation
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
4.8. I think that CyberSANE could assist my organisation in investigating cyber incidents and cybercrime, as well as collecting the appropriate forensic evidence
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable

5. Legal and Ethical Compliance

Question / Statement
5.1. I think that CyberSANE components adequately facilitate the computer incident handling process
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
5.2. I think that CyberSANE complies with the EU General Data Protection Regulation (GDPR), as well as with the local data protection and privacy laws applicable to my organisation

Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
5.2.1.I think CyberSANE takes all the measures to protect the data it collects and processes
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
5.2.2.I think all the data CyberSANE collects is really necessary for the purpose of its processing
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
5.2.3.I think CyberSANE has a legal basis for processing personal data
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
5.2.4.I think CyberSANE stores personal data only for the period of time necessary to the achievement of its purposes
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
5.2.5.I think CyberSANE has policies that ensure that personal data are rectified or erased in case it is inaccurate
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement

5.2.6. I am aware about what to do (for example, following an internal reporting procedure) if privacy breach occurs
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
5.3. I think that CyberSANE complies with the EU legal framework on cyber-security
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
5.4. I think that CyberSANE complies with the EU legal and ethical framework on artificial intelligence
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
5.5. If you disagree or strongly disagree with one or more statements in 5.1-5.4, then please explain the reason(s) why you disagree or strongly disagree
Answer
Question / Statement
5.6. I am participating into the CyberSANE research voluntarily
Answer
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
5.7. I am not a minor
Answer
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement

5.8. I am informed about the purposes, methods and intended possible uses of the CyberSANE technology
Answer
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
5.9. As a participant to the CyberSANE research project, I received information on by whom, how and why my personal data will be processed
Answer
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable

6. Contract and Economic

Question / Statement
6.1. I think that CyberSANE could provide economic benefits to my organisation
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
6.2. I think that CyberSANE could provide compliance benefits to my organisation
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
6.3. I think that CyberSANE could provide security benefits to my organisation
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable

7. External Communication

Question / Statement

7.1. I think that CyberSANE improves the external collaboration and information sharing of CTI between different organisations

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

7.2. I think that CyberSANE adopts trustworthy and secure mechanisms for the management and interchange of incident-related information

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

8. Other Comments

Question / Statement

8.1. What are your main concerns regarding CyberSANE framework?

Answer

Question / Statement

8.2. What is the biggest advantage of CyberSANE framework in your opinion?

Answer

Question / Statement

8.3. What are other needs you feel should be addressed?

Answer

Annex 2. Non-Technical Users' Questionnaire

1. General Information

Question / Statement

1.1. What is your organisation's type?

Answer Options

○ Public ○ Small medium enterprise ○ Large enterprise ○ Other private organisation

Question / Statement

1.2. What is your organisation's area of interest?

Answer Options

○ Logistics ○ Energy provider ○ Healthcare operator ○ Bank and insurances

○ Telecommunications ○ Law-enforcement ○ Academia and R&D

○ Technology provider ○ Other Critical Infrastructure or Critical Information Infrastructure

Question / Statement

1.3. What is your current position in your organisation?

Answer

Question / Statement

1.4. What is your expertise on cyber-security domain?

Answer Options

○ None ○ Basic ○ Intermediate ○ Advanced

2. Usability and Efficiency

Question / Statement

2.1. I think that CyberSANE can interoperate with the existing workflows and infrastructure defined within my organisations

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

2.2. I think that I would need the support of a security expert to be able to use CyberSANE framework

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

2.3. I think that the learning curve and familiarisation with CyberSANE components is a quite fast and straightforward procedure

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

2.4. I think that I have to learn a lot of things before I could get going with this system on a daily basis

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

3. Security and Results Quality

Question / Statement

3.1. I think that CyberSANE enhances the security awareness of a Security Operations Centre (SOC), Computer Security Incident Response Team (CSIRT), or other cyber-security related personnel of my organisation

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

3.2. If you think that CyberSANE can enhance the security posture of your organisation, then please explain how such a thing could be achieved from your perspective

Answer

4. Legal and Ethical Compliance

Question / Statement
4.1. I think that CyberSANE would support my organisation to ensure compliance with the EU General Data Protection Regulation (GDPR), as well as with the applicable local data protection and privacy laws
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
4.1.1.I think CyberSANE takes all the measures to protect the data it collects and processes
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
4.1.2.I think all the data CyberSANE collects is really necessary for the purpose of its processing
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
4.1.3.I think CyberSANE has a legal basis for processing personal data
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
4.1.4.I think CyberSANE stores personal data only for the period of time necessary to the achievement of its purposes
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
4.1.5.I think CyberSANE has policies that ensure that personal data are rectified or erased in case it is inaccurate
Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
4.1.6.I am aware about what to do (for example, following an internal reporting procedure) if privacy breach occurs
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
4.2. I think that CyberSANE complies with the EU legal framework on cyber-security
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
4.3. I think that CyberSANE complies with the EU legal and ethical framework on artificial intelligence
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
4.4. If you disagree or strongly disagree with one or more statements in 4.1-4.3, then please explain the reason(s) why you disagree or strongly disagree
Answer
Question / Statement
4.5. I think that CyberSANE modules comply with the industry standards of my organisation
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
4.6. I am participating into the CyberSANE research voluntarily
Answer

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
4.7. I am not a minor
Answer
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
4.8. I am informed about the purposes, methods and intended possible uses of the CyberSANE technology
Answer
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
4.9. As a participant to the CyberSANE research project, I received information on by whom, how and why my personal data will be processed
Answer
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable

5. Contract and Economic

Question / Statement
5.1. I find the contracts' pricing offered by CyberSANE consortium to be economically viable for my organisation
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree ○ Strongly disagree ○ Do not know, not applicable
Question / Statement
5.2. I think that CyberSANE could reduce the expenses of my organisation regarding the handling of cyber-security incidents
Answer Options
○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

5.3. Are you interested in CyberSANE framework as a unified solution?

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

Question / Statement

5.4. If you agree or strongly agree with the question 5.3, then please choose the CyberSANE component(s) you are interested in

Answer Options

□ LiveNet □ DarkNet □ HybridNet □ ShareNet □ PrivacyNet

6. External Communication

Question / Statement

6.1. I think that CyberSANE could improve the communication and sharing of threat information with other external organisations

Answer Options

○ Strongly agree ○ Agree ○ Neither agree, nor disagree ○ Disagree

○ Strongly disagree ○ Do not know, not applicable

7. Other Comments

Question / Statement

7.1. What are your main concerns regarding CyberSANE framework?

Answer

Question / Statement

7.2. What is the biggest advantage of CyberSANE framework in your opinion?

Answer

Question / Statement

7.3. What are other needs you feel need to be addressed?
Answer