CYBERSANE

D10.2

Stakeholders Evaluation

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
Programme:	H2020-SU-ICT-2018

Deliverable type:	Report
Deliverable reference number:	DS-01-833683 / D10.2 / Final | 1.0 Stakeholders Evaluation
Work package contributing to the deliverable:	WP 10
Due date:	August 2022 – M36
Actual submission date:	24/10/2022

Responsible organisation:	KLINIKUM NURNBERG
Editor:	Andrius Patapovas
Dissemination level:	PU
Revision:	< FINAL | 1.0 >

Abstract:	This deliverable reports the outcomes of task T10.2 “Stakeholders Evaluation”. It provides a concrete analysis of the stakeholders’ evaluation feedback for the CyberSANE system (end-users and external users), in the context of the pilots and internal and external users involvement, and provides the consolidated results.
Keywords:	Stakeholders evaluation, end users evaluation, external users evaluation, stakeholders, evaluation, questionnaire, end-users, external users, CyberSANE system.
	The project CyberSANE has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 833683.

Editor

Andrius Patapovas (KN)

Contributors

Manfred Criegee-Rieck (KN)

Pablo Giménez (VPF)

Andreas Miaoudakis (STS)

Jorge Martins (PDMFC)

Burcu Yasar (LSE)

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.

The goal of the current deliverable is to present the evaluation results based on reception and analysis of CIIs operators' and stakeholders' feedback in terms of the CyberSANE incident handling approach. The feedback from CIIs operators' (end-users), who participated in the pilot preparation and execution, and from stakeholders' (external-users), who were only participated in the demonstration of pilot operation, was received by responding to technical and non-technical technical questionnaires, respectively.

Contents

Executive Summary 2

Contents 3

List of Figures 4

List of Tables 4

Chapter 1. Introduction 5

1.1 Scope 5

1.2 Contributions to other work packages 5

1.3 Structure of the document 5

Chapter 2. Methodology 6

2.1 Introduction to the method 6

2.2 Scope and Objectives 7

2.3 Target Groups of the CyberSANE Evaluation process 8

2.4 Description and analysis of the method 8

2.5 Pilot end-users survey 8

Chapter 3. Results and Evaluation 9

3.1 End-users evaluation questionnaire results 9

3.2 External users' evaluation questionnaire results 14

Chapter 4. Summary and Conclusion 19

Chapter 5. List of Abbreviations 20

Chapter 6. Bibliography 21

List of Figures

Figure 3-1. Distribution of general information by end-user respondents......................... 9

Figure 3-2. Distribution of general information by external-user respondents................ 14

Figure 3-3. Selected components for CyberSANE as a unified solution by external-users 16

List of Tables

Table 2-1. Technical Users' Questionnaire Structure 6

Table 2-3. Non-Technical Users' Questionnaire Structure.. 7

Chapter 1. Introduction

1.1 Scope

Based on T10.1 a set of technical and non-technical user questionnaires were developed in the deliverable D10.1 for collecting feedback from internal and external stakeholders about CyberSANE Incident Handling approach and its components. The deliverable 10.2 provides evaluation of questionnaire results.

1.2 Contributions to other work packages

Based on T10.2 the feedback received by stakeholders in terms of the CyberSANE Incident Handling approach was analysed, while the actual technical and business evaluation of the CyberSANE framework will take place in T10.3. The evaluation results of technical questionnaires will be incorporated into the deliverable 10.3 "Technical and Business Evaluation".

1.3 Structure of the document

The document is structured as follows:

- Chapter 2 describes the methodology for socio-economic and techno-economic evaluation of the CyberSANE framework
- Chapter 3 summarizes the results of technical for end-users and non-technical for external-users questionaries' evaluation
- Chapter 4 features the concluding remarks of this deliverable
- Chapter 5 includes a glossary of the most commonly used abbreviations
- Chapter 6 concludes with all the bibliography of this deliverable

Chapter 2. Methodology

2.1 Introduction to the method

The socio-economic and techno-economic evaluation involved the creation of two general validation questionnaires for technical and non-technical stakeholders 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 used to evaluate both stakeholder groups. 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

The vast majority of questions provided in a technical questionnaire were focused on the architecture, usability, efficiency, security, and results quality of the CyberSANE system. In total 53 questions were created that are categorized in 8 question categories as shown in Table 1.

Table 2-1. Technical Users' Questionnaire Structure

Category Name	Number of Questions
General Information	4
Architecture	6
Usability and Efficiency	16
Security and Results Quality	8
Legal and Ethical Compliance	11
Contract and Economic	3
External Communication	2
Other Comments	3

Most answer options to these questions adopted 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

Some questions were created with a predefined set of answers option in order to categorize the answers. A few questions offered a text area for generic comment.

The non-technical questionnaire contained 29 question that fall within 7 question categories. **Error! Reference source not found.** below displays all the categories which compose non-technical users' questionnaire, followed by the number of questions included in each category.

Table 2-2. Non-Technical Users' Questionnaire Structure

Category Name	Number of Questions
General Information	4
Usability and Efficiency	4
Security and Results Quality	2
Legal and Ethical Compliance	11
Contract and Economic	4
External Communication	1
Other Comments	3

In the non-technical questionnaire, most questions (or statements) were mainly oriented towards the organisational and managerial aspects of an organisation. Additionally, a set of trivial and easy-to-answer questions about the usability, efficiency, and security of the presented system was included.

Similar to technical questionnaire mostly set of answer were ranging from "Strongly agree" to "Do not know, not applicable" as well as predefined set of answer options and a free text area for a generic comment were provided.

Almost all questions were mandatory.

2.2 Scope and Objectives

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). Each questionnaire included its specific questions matching the expertise of the stakeholders on cyber-security domain and business area of interest. In this way we were able to properly receive and analyse an unbiased feedback based on the stakeholders' point-of-view on CyberSANE system. The perceived usability was derived by the standardized statements of the System Usability Scale questionnaire (Lewis, 2018). The outcomes of the technical and non-technical questionnaires served as the basis for the data analysis and stakeholders' evaluation, as well as the technical and business evaluation, which took place in the context of T10.3.

2.3 Target Groups of the CyberSANE Evaluation process

The technical-related questionnaire targeted end-users who are actively engaged in the demonstration of project's pilots, quite experienced in the cyber-security domain, have sufficient technical knowledge and responsible for setting up, monitoring, and maintaining an organisation's IT systems. Therefore, such end-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.

The non-technical questionnaire involved external-users who possess quite limited or no experience in the cyber-security domain and were expected to face difficulties in operating adequately the CyberSANE platform at its whole. In contrast to the experienced end users, this group of external users was only participating in a pilot operation demonstration. However, such external users are usually stakeholders that play an essential role in the daily operations and functionality of a CI or CII.

2.4 Description and analysis of the method

The survey results of technical and non-technical questionnaires were separately extracted and analyzed. Each question was evaluated representing a total number of respondents who "agree" or "strongly agree" to the statement in the question followed by a total number of the range "disagree" or "strongly disagree".

Additionally, a total number of respondents who chosen the answer "neither agree, or disagree" as well as "I don't know/not applicable" was provided, if the total number significant higher.

Answers to questions with free text entry were listed entirely.

To visualize dependencies on provided information in the general section such as organization's type, organization's area of interest, current position in respondent's organization and an expertise on cyber-security topics a Sankey type of diagram was conducted.

2.5 Pilot end-users survey

The technical-related questionnaire targets end-users who were actively engaged in the preparation and 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 since they are typically responsible for setting up, monitoring, and maintaining an organization's IT systems.

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 by the CyberSANE framework.

Chapter 3. Results and Evaluation

Evaluation feedback was received in the scope of the pilot preparation and operation i.e. as part of internal and external stakeholders' involvement in the pilot use of the system. The CyberSANE system and its main components (LiveNet, DarkNet, HybridNet, ShareNet and PrivacyNet) along with the respective tools that supported corresponding scope of realistic threat scenarios of three sectorial services were carried out on different dates, i.e.:

- Container Cargo Transportation Service (Container Transportation) on the 2nd of February 2022
- Solar Energy Production, Storage and Distribution Service (Solar Energy pilot) on the 5th of April 2022
- Cyber-threat identification and communication in healthcare on the 1st of July 2022 (Healthcare pilot)

Following up each pilot execution, internal and external stakeholders / participants were invited to fill a technical and non-technical questionnaire respectively.

3.1 End-users evaluation questionnaire results

Following findings were determined from 6 filled technical questionnaires by end-users.

General Information

Q1.1-Q1.3: Based on the provided answers in the section of general information the Figure 3-1 shows the profiles of respondents visualising the dependencies between organization's type, organization's area of interest and current position of respondent.

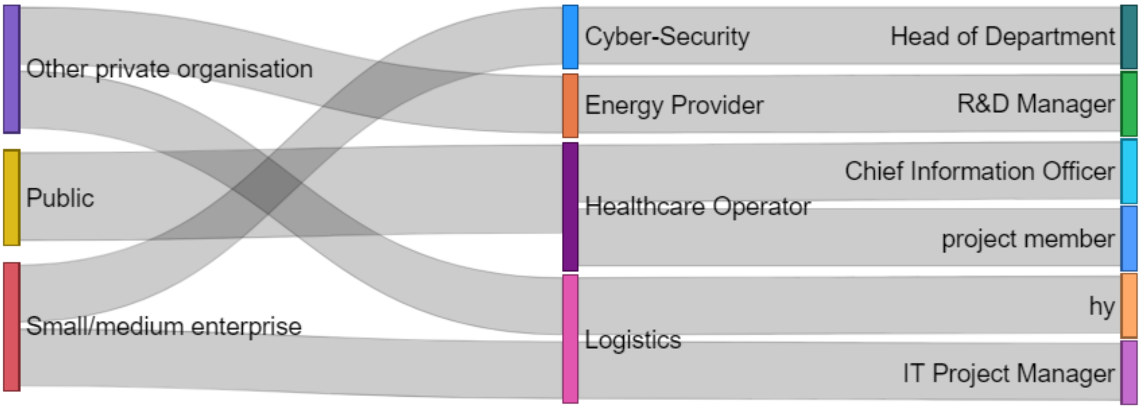

Figure 3-1. Distribution of general information by end-user respondents

Following key findings on topics architecture, usability & efficiency, security & results quality, economic aspects and external communications were determined from the filled questionnaires.

Architecture Results

Q2.1: 5 of 6 respondents agree or strongly agree that CyberSANE can interoperate with other existing systems in their organisation with a minimum effort.

Q2.2: 5 of 6 respondents agree or strongly agree that the functionalities offered by all CyberSANE components are well integrated into the architecture.

Q2.3: 5 of 6 respondents agree or strongly agree that CyberSANE can interoperate with other existing systems in my organisation with a minimum effort.

Q2.4: 5 of 6 respondents CyberSANE can interoperate with other security policies in my organisation with a minimum effort.

Q2.5: 4 of 6 respondents think that CyberSANE could replace one or more existing security components of their organisation. One respondent points to the fact that the usage of CyberSANE would be primarily focused on thread detection. Other respondent stated to use the CyberSANE components in combination with already existing security components in an organisation.

Usability and Efficiency Results

Q3.1: 5 of 6 respondents agree that the CyberSANE framework is easy and intuitive to use on a daily basis.

Q3.2: 2 of 6 respondents agree that CyberSANE is more efficient and effective in terms of time spent in contrast to other cyber-security solutions. One respondent disagrees.

Q3.3: 5 of 6 respondents agree or strongly agree that CyberSANE's dashboard is easy to navigate and provides a comprehensive, unified overview of all its components.

Q3.4: 5 of 6 respondents agree or strongly agree that CyberSANE's dashboard comes with advanced visualization and interactive control processes, as well as with detailed reports to the system users.

Q3.5: 5 of 6 respondents agree or strongly agree that the CyberSANE framework's information and alerting capabilities are helpful enough and clearly viewable.

Q3.6: 5 of 6 respondents agree or strongly agree to be satisfied with the performance of the system in terms of speed.

Q3.7: 4 of 6 respondents disagree to have found the system unnecessarily complex and cumbersome to use. 2 respondents neither agree, nor disagree.

Q3.9: 4 of 6 respondents agree or strongly agree that CyberSANE features all the functionalities expected from a cyber-security system.

Following functionalities were reported to be missing at CyberSANE:

- *“Should include automatic response to some predefined threats”*
- *“Perform countermeasures when an attack is detected”*

Q3.10: 5 of 6 respondents agree that they would find CyberSANE useful in their tasks at work.

Q3.12: All respondents agree or strongly agree that it would be easy for me to become skilful at using the CyberSANE system.

Q3.14: 3 of 6 respondents agree that CyberSANE will be accepted and used by their colleagues given that it was implemented at their organization. One respondent disagrees and 2 respondents don’t know.

Q3.15: Respondent who disagreed with the statement of the Q3.14 explains as follows:

- *“parts of CyberSANE are experimental, which is not harmful, but not suitable at that point of matureness for daily operations. Missing is the information on a competitive sparring with existing solutions and their performance. From a purchase perspective CyberSANE has no reputation.”*

Q3.16: 5 of 6 respondents agree that it would be implemented in their organization and they had access they intend to use the CyberSANE system.

Security and Quality Results

Q4.1: 5 of 6 respondents agree that CyberSANE provides faster identification and better classification of security threats compared to the existing deployed solution within their organisation.

Q4.2: 5 of 6 respondents agree or strongly agree that the CyberSANE framework enables a faster reaction and lowers the average time needed to respond to a cyber-threat.

Q4.3: 5 of 6 respondents agree or strongly agree that CyberSANE provides an improved decision support mechanism which improves the situational awareness within their organisation.

Q4.4: 5 of 6 respondents agree or strongly agree that, within the CyberSANE system, the correlation of incidents and the cascading effects of a security incident are easy to notice and presented in an understandable way.

Q4.5: 4 of 6 respondents agree or strongly agree that CyberSANE allows the prioritization of alerts, security incidents, and recovery actions.

Q4.6: 4 of 6 respondents agree or strongly that CyberSANE improves the internal collaboration and information sharing of security incidents between different teams and operators.

Q4.7: 4 of 6 respondents agree that CyberSANE enables the efficient protection against cyber-threats and can sufficiently cover the cyber-security needs of their organisation.

Q4.8: 5 of 6 respondents agree or strongly agree that CyberSANE could assist my organisation in investigating cyber-incidents and cyber-crime, as well as collecting the appropriate forensic evidence.

Legal and Ethical Compliance

Q5.1: 5 of 6 respondents agree or strongly agree that CyberSANE components adequately facilitate the computer incident handling process.

Q5.2: 4 of 6 respondents agree or strongly agree that CyberSANE complies with the EU General Data Protection Regulation (GDPR) as well as with local data protection and privacy laws applicable to my organisation.

Q5.2.1: 3 of 6 respondents agree or strongly agree that CyberSANE takes all the measures to protect the data it collects and processes.

Q5.2.2: 4 of 6 respondents agree or strongly agree that all the data CyberSANE collects is really necessary for the purpose of its processing.

Q5.2.3: 2 of 6 respondents agree or strongly agree that CyberSANE has a legal basis for processing personal data.

Q5.2.4: 4 of 6 respondents agree or strongly agree that CyberSANE stores personal data only for the period of time necessary to the achievement of its purposes.

Q5.2.5: all respondents agree or strongly agree that CyberSANE has policies that ensure that personal data are rectified or erased in case they are inaccurate.

Q5.2.6: 3 of 6 respondents agree or strongly agree that they are aware about what to do if a privacy breach occurs in CyberSANE.

Q5.3: 5 of 6 respondents agree or strongly agree that CyberSANE complies with the EU legal framework on cyber-security.

Q5.4: 2 of 6 respondents agree or strongly agree that CyberSANE complies with the EU legal and ethical framework on Artificial Intelligence. 2 respondents neither agree, nor disagree, 2 don't know.

Economic Aspects Results

Q6.1: 5 of 6 respondents agree or strongly agree that CyberSANE could provide economic benefits to my organisation.

Q6.2: 5 of 6 respondents agree or strongly agree that CyberSANE could provide compliance benefits to my organisation.

Q6.3: all respondents agree or strongly agree that CyberSANE could provide security benefits to my organisation.

External Communication Results

Q7.1: 5 of 6 respondents agree or strongly agree that CyberSANE improves the external collaboration and information sharing between different organisations.

Q7.2: 5 of 6 respondents agree or strongly agree that CyberSANE adopts trustworthy and secure mechanisms for the management and interchange of security incident-related information.

Concerns, advantages and further comments

Q8.1: Following concerns were provided regarding the CyberSANE framework by 4 respondents:

- *"Integration with the current systems"*
- *"Medium to long-term concerns of brought into company as a system. Who will be responsible for overall system when H2020 projects ends"*
- *"It is experimental and scarcely proved for operational use. Few is known about effectiveness and efficiency. Valuable insight e.g. the benchmark with and against other solutions is missing."*
- *"Share the lessons learned with other health care providers to react on threats as fast as possible"*

Q8.2: Following advantages considered the point of view of 5 respondents to be the biggest advantages of the CyberSANE framework:

- *"Integration of many components to detect threats and anomalies as well as the possibility to share information of attacks"*
- *"Extensive threat monitoring in a single platform and the capability to share them"*
- *"The cross-thinking in IT-security and the idea sharing security information with others"*
- *"The platform accessibility for all participating partners"*
- *"The integrated platform with all the layers and underlying functionalities."*

In summary is the biggest advantage of the CyberSANE framework is the capability to share the knowledge across all participating partners.

Q8.3: Following issues were addressed by 4 respondents:

- *"It just detects the attack and informs but it does not have any workflow defined that could be used to solve at least the most usual cyber-security issues"*

- *“If selling onto the market, there needs to be a clear business plan, price plan and medium-term security that update will be made and overall system kept up and running.”*
- *“As a business user, my role is to purchase, implement and run information security solutions, which provide the prove to reduce a specific, existing risk significantly. For that decision making we expect a clear USP compared with other solutions and an implementation concept which is harmony with our architecture and our solution checklist. In order to assess benefit and effort.”*
- *“Integration of core components”*

3.2 External users' evaluation questionnaire results

Following findings were determined from 25 filled non-technical questionnaires.

General Information

Q1.1-Q1.4: Based on the provided answers in the section of general information the Figure 3-2 shows the profiles of respondents visualising the dependencies between organization's type, organization's area of interest, current position of respondent in organization and expertise on cyber-security topics.

- organization's type
  - 65% of stakeholders were from small/medium enterprise
  - 20% of stakeholders were from public sector
- organization's area of interest
  - 32% of stakeholders related to logistic
  - 24% of stakeholders related to cyber-security
  - 16% of stakeholders related to academia and R&D
- expertise on cyber-security topics
  - 40% of stakeholders estimate to have an intermediate level
  - 32% of stakeholders estimate to have an advance level
  - 20% of stakeholders estimate to have a basic level

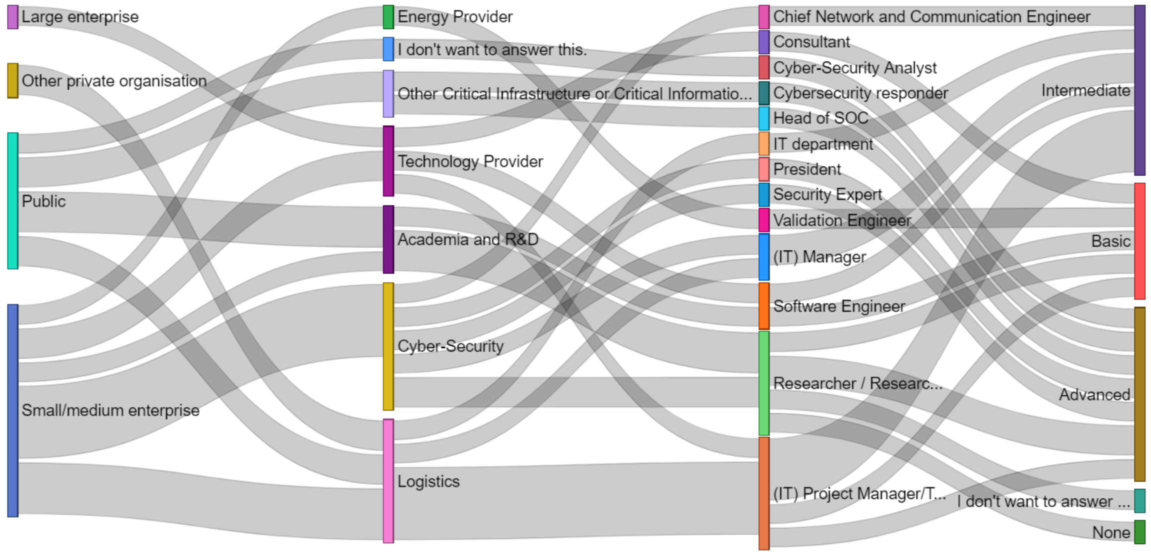

Figure 3-2. Distribution of general information by external-user respondents

Usability and Efficiency

Q2.1: 84% of respondents (18 agree and 3 strongly agree) think that CyberSANE can interoperate with the existing workflows and infrastructure defined within my organization. Other respondents neither agree, nor disagree or don't know.

Q2.2: 68% of respondents (10 agree or 7 strongly agree) think that they would need the support of a security expert to be able to use the CyberSANE framework. 20% of respondents (5) disagree and other neither agree, nor disagree.

Q2.3: 88% of respondents (20 agree and 2 strongly agree) think that the learning curve and familiarisation with CyberSANE components is a quite fast and straightforward procedure. Other respondents neither agree, nor disagree.

Q2.4: 28% of respondents (6 agree or 1 strongly agree) think that they have to learn a lot of things before they could get going with the CyberSANE system on a daily basis. 72%

respondents (7 disagree and 11 strongly disagree) don't think that they have to learn a lot of things.

Security and Results Quality

Q3.1: 92% of respondents (13 agree or 10 strongly agree) think that CyberSANE enhances the security awareness of a Security Operations Centre (SOC), Computer Security Incident Response Team (CSIRT), or other security-related personnel of my organisation. Rest respondents neither agree, not disagree or don't know.

Q3.2: 13 respondents provided following explanations how CyberSANE can enhance the security posture of respondents' organisation from their perspective:

- *"Detect incidents and prevent attacks"*
- *"Early notify and live monitoring of relative incidents to organisation"*
- *"Time reduction for training new SOC and CSIRT team members"*
- *"CyberSANE can enhance the security posture of my organisation a lot because it offers live monitoring and alerting mechanism, and search and analysis tools in the web and the dark web"*
- *"Increase the knowledge of threats and risks"*
- *"Increase the agility of the security posture of organisation"*
- *"Help to give a C-level overview about relevant incidents in the organization."*
- *"Raise security awareness, support simulation and analysis of what-if scenarios, provide feedback based on lessons learnt"*
- *"Produce a set of automated responses to threat types, that can lead the way for security analysts"*
- *"It can provide information from different systems and external sources"*
- *"It will be necessary to educate the relevant personnel and share the info with faculty, administration and specialized students."*
- *"It joins many different components of cyber security in one place, which can make job a lot easier for a sec tech, instead of using many different products."*
- *"To have an overall insight of cyber-security health status in the organization."*

Legal and Ethical Compliance

Q4.1: 68% of respondents (16 agree and one strongly agrees) think that CyberSANE would support their organisation to ensure compliance with the EU General Data Protection Regulation (GDPR), as well as with the applicable local data protection and privacy laws. One respondent disagrees and rest respondents neither agree, nor disagree or don't know.

Q4.1.1: 68% of respondents (10 agree and 7 strongly agree) think that CyberSANE takes all the measures to protect the data it collects and processes. Rest respondents neither agree, not disagree or don't know.

Q4.1.2: 88% of respondents (14 agree and 8 strongly agree) think that all the data CyberSANE collects is really necessary for the purpose of its processing. Rest respondents neither agree, not disagree or don't know.

Q4.1.3: 64% of respondents (11 agree and 5 strongly agree) think that CyberSANE has a legal basis for processing personal data. Rest respondents neither agree, not disagree or don't know.

Q4.1.4: 68% of respondents (12 agree and 5 strongly agree) think that CyberSANE stores personal data only for the period of time necessary to the achievement of its purposes. Rest respondents neither agree, not disagree or don't know.

Q4.1.5: 72% of respondents (13 agree and 5 strongly agree) think that CyberSANE has policies to ensure that personal data are rectified or erased in case they are inaccurate. Rest respondents neither agree, not disagree or don't know.

Q4.1.6: 72% of respondents (17 agree and one strongly agrees) are aware about what to do if a privacy breach occurs in CyberSANE (e.g. following an internal reporting procedure). 3 respondents disagree. Rest respondents neither agree, not disagree or don't know.

Q4.2: 88% of respondents (17 agree and 5 strongly agree) think CyberSANE complies with the EU legal framework on cyber-security. Rest respondents neither agree, nor disagree or don't know.

Q4.3: 68% of respondents (12 agree and 5 strongly agree) think that CyberSANE complies with the EU legal and ethical framework on Artifical Intelligence. Rest respondents neither agree, nor disagree or don't know.

Q4.5: 88% of respondents (19 agree and 3 strongly agree) think that CyberSANE modules comply with the industry standards of their organisation. One respondent neither agrees, nor disagrees and 2 respondents don't know.

Contract and Economic

Q5.1: 16% of respondents (4 agree) find the contract's pricing offered by the CyberSANE consortium to be economically viable for my organisation. 52% (13 neither agree, nor disagree) of respondents are neutral to the pricing. 32 % (8) of respondents don't know.

Q5.2: 64% of respondents (16 agree) think that CyberSANE could reduce the expenses of their organisation regarding the handling of cyber-security incidents. 32 % (8) neither agree, nor disagree about reduction of the expenses. One respondent doesn't know.

Q5.3: 80% of respondents (8 very interested and 12 somewhat interested) interested in the CyberSANE framework as a unified solution. 20% of respondents (5) are undecided whether they are interested or not.

Q5.4: 56 % of respondents (14) are interested in CyberSANE as a unified solution with all components. 2 respondents haven't chosen any components. 2 of respondents chosen combination of LiveNet + DarkNet + HyberNet. The total distribution of chosen components is showed in the **Error! Reference source not found.**.

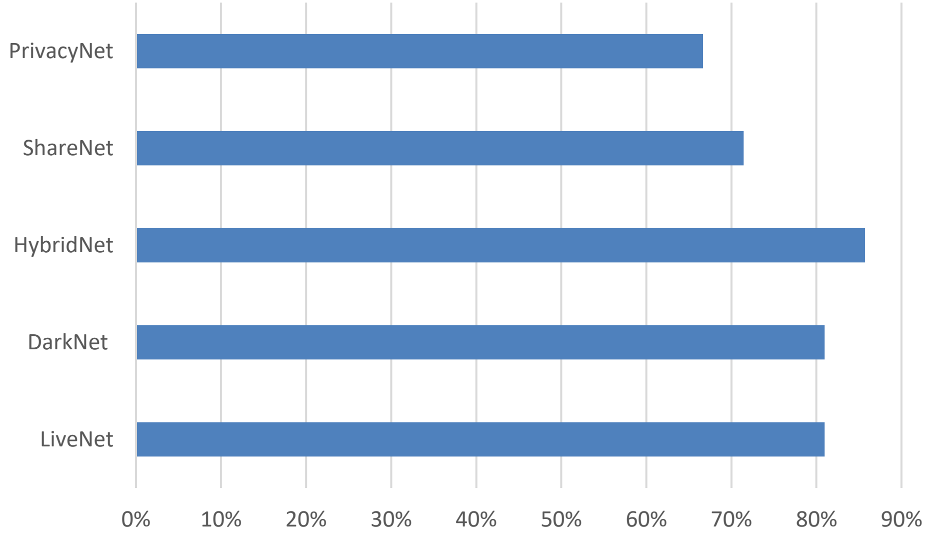

Figure 3-3. Selected components for CyberSANE as a unified solution by external-users

External Communication

Q6.1: 92% of respondents (12 agree and 11 strongly agree) think that CyberSANE could improve the communication and sharing of threat information with other external organisations. 2 of respondents whether agree, nor disagree with the statement.

Concerns, advantages and comments

Q7.1: 13 respondents provided following main concerns regarding the CyberSANE framework:

- *“Good integration of all the tools”*
- *“Integration with current systems”*
- *“Its stability and performance when scaling up”*
- *“Time required to adopt at company wide scale”*
- *“Its still in a development phase”*
- *“Main concern is about the sharing of information among Critical Infrastructures and the compliance with each organisations internal regulations.”*
- *“Sharing of information among Critical Infrastructures and the compliance with each organisation internal regulations”*
- *“It offers a general point of view about several relevant tools and the ability to define our own procedures and lessons learnt, which help to improve incident in the future”*
- *“Easy applicability to diverse domains”*
- *“Complexity of modules interaction”*
- *“The integration with the current components”*
- *“It may prove to be very general”*
- *“Integrating this product with the existing ones.”*

Q7.1: 15 respondents provided following the biggest advantages of the CyberSANE framework from their point of view:

- *“All the options to detect attacks and anomalies”*
- *“Live monitoring”*
- *“Integrated solution with all the cyber-security information”*
- *“Its simplicity of operation”*
- *“Meta platform to engage with all the other security tools existing in the company”*
- *“All the options to discover cybersecurity issues”*
- *“The technologies and the different components that it has”*
- *“Standardization of information and procedures between security tools”*
- *“Smooth usage flow, easy integration and extensibility of the platform”*
- *“All the features that it offers”*
- *“Centralization of multiple tools”*
- *“An only platform to assess the security from all the organization”*
- *“Easy to integrate with current procedures”*
- *“As mentioned, it covers or contains many tools join in one framework”*
- *“Overall incident handling system”*

Q7.3: 9 respondents addressed following issues concerning CyberSANE:

- *“Tools updates”*
- *“Threat intelligence feeds for zero-days”*
- *“I think that the clear view of ShareNet and PrivactNet should be defined”*
- *“Orchestration and active response (e.g., isolating infected machines, disabling compromised accounts...)”*

- *“Out of the box value, should not require much user setup”*
- *“Automatic or manual actions to respond to attacks”*
- *“Clear compliance with all security laws and directives.”*
- *“Maybe adding an incident response option (like TheHive or RTIR) which is also included within the framework, so you do not have to use third party tool for IR.”*
- *“Integration with CTI platforms and TAXII/STIX support”*

Chapter 4. Summary and Conclusion

In this deliverable the survey results of both technical and non-technical questionnaires were evaluated. At first a methodology of evaluation was explained. Then the survey results of 6 CII operators (end-users, involved in preparation of pilot operation) and 25 stakeholders (external-users, only participating in pilot operation demonstration) were evaluated.

For most of the topics, the CyberSANE Incident Handling approach prepared and demonstrated during pilot operations was positively accepted by CII operators and stakeholders.

Although one end-user is concerned about the ability of full integration of the CyberSANE platform with existing systems in the organisations, the majority identify the capability to share the knowledge across all participating partners as the biggest advantage of the CyberSANE framework and think that it would be easy for them to become skilful at using CyberSANE.

In fact, 72% of stakeholders don’t think that they have to learn a lot of things before they could get going with the CyberSANE system on a daily basis. Still, 68% of stakeholders would need the support of a security expert to be able to use the CyberSANE framework.

Especially, lots of free text answers considering issues related to CyberSANE as well as advantages and disadvantages were provided, showing a good level of interest and participation.

Finally, the evaluation results of the technical questionnaire were integrated into T10.3 and used for the deliverable D10.3 Business and Technical Evaluation.

Chapter 5. List of Abbreviations

Abbreviation	Translation
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CSIRT	Computer Security Incident Response Teams
GDPR	General Data Protection Regulation
IT	Information Technology
PC	Personal Computer
SOC	Security Operations Centre
TNA	UTraining Needs Analysis
USP	Unique Selling point

Chapter 6. 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.