FP7-610416-PANOPTESEC

Dynamic Risk Approaches for Automated Cyber Defence

D8.2.3: Operational Workshop Report

Work-Package	WP8	Deliverable	D8.2.3
Due Date	31-10-2016	Submission Date	07-11-2016
Main Author(s)	ACEA, RHEA		
Contributors	All project participants		
Version	V2.0	Status	Final
Dissemination Level	PU	Nature	R
Keywords	Operational Workshops, Validation, SME		

Part of the Seventh

Framework Programme

Funded by the EC - DG Connect

EXECUTIVE SUMMARY

This document provides a description of the Operational Workshops organized in ACEA premises (organized between the 17th of October 2016 and the 28th October 2016) and structured to let external stakeholders to evaluate the integrated PANOPTESEC System.

This document describes the performed Operational Workshops, examines the sector/industry the attendees belong to, analyses their feedbacks with a focus on the SMEs participants.

HISTORY

Version	Date	Name/Partner	Comment
V0.0	28-10-2016	Francesco Bosco/ACEA	Initial creation of the document.
V0.1	03/11/2017	Francesco Bosco/ACEA	Added detail on operational workshops
V0.2	04/11/2016	Francesco Bosco/ACEA	Modified format of tables and figures
V0.3	04/11/2016	Francesco Bosco/ACEA	Further modification of format of tables and figures
V0.4	05/11/2016	Francesco Bosco/ACEA	Added 3.4 analysis of internal stakeholders' feedback
V0.4	05/11/2016	Matteo Merialdo/RHEA	QA Peer Review
V0.5	06/11/2016	Francesco Bosco/ACEA	Peer review comments implemented
V1.0	06/11/2016	Francesco Bosco/ACEA	Document closed, comments from QA implemented
V2.0	28/11/2016	Francesco Bosco/ACEA	Added results of 23 and 24 November sessions

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

ACRONYMS AND DEFINITIONS

Table 1: Acronym List

Acronym	Meaning
UzL	University of Lubeck
ACEA	ACEA S.p.A.
ALBLF	NOKIA
CIS-UROME	Universita Degli Studi Di Roma La Sapienza
EPIST	Epistematica SRL
IMT	Institut Mines-Telecom
RHEA	RHEA System S.A.
SUPELEC	Ecole Supérieure D'Électricité

Table 2: Definitions

Word or Phrase	Meaning
TPM	Technical Project Manager
WP	Work Package
QR	Qualification Review
EAB	External Advisory Board
SME	Small-Medium Enterprise
AR	Acceptance Review

1 INTRODUCTION

1.1 Context

After the delivery of [D7.4.1], the PANOPTESEC System prototype has been installed during Month 35 within the ACEA Demonstration Environment, composed by the Emulation Environment (an operational testing emulation of a segment of the production environment of the Command and Control network of Acea areti -former Acea Distribuzione) and the Deployment Environment, a separated network hosting all PANOPTESEC System Virtual Machines.

The PANOPTESEC Installed Demonstration Prototype has been used for the first PANOPTESEC Workshops, useful for the Qualification Review (QR), at the end of Month 35 [D8.2.2]. The aim of these Workshops was to start the PANOPTESEC System Validation phase through a set of live demo and presentations with internal stakeholders and the PANOPTESEC External Advisory Board.

In the Month 36 the PANOPTESEC Installed Demonstration Prototype has been used to organize the Operational Workshops held as the final dissemination/validation activity.

1.2 Purpose

The purpose of this deliverable is to capture the results of the operational workshop and describe its preparation and philosophy including the results of industry observer feedback and surveys.

1.3 Scope

The scope of this deliverable includes a summary of the performed activities and of the live demo and presentations conducted on the operational domain of the ACEA infrastructure.

1.4 Document Structure

This [D.8.2.3] deliverable is structured in the following manner:

Section 1	Introduction: describes the context, purpose and scope of the deliverable.
Section 2	Methodology: describes the methodology followed for the development of the live demo and the proposed surveys.
Section 3	Live demo and surveys results analysis
Section 4	Conclusion: summarizes the findings and results.

2 METHODOLOGY

2.1 Information collection

After the installation of the [D7.4.1] (described within [D8.2.2]) and the Qualification Review conducted on the 11th of October 2016, two weeks of the Operational Workshops were

organized in ACEA at the end of Month 36 for the final Validation phase of the PANOPTESEC System.

Two additional session of the Operational Workshops were held on the 23rd and 24th of November in order to reach stakeholders who could not participate at the end of October.

As a result from the live demonstrations, the Consortium collected a feedback questionnaire (on paper), given to all attendees.

The questionnaires were processed to analyse the feedback.

Each question was given a rank between 0 and 5 following the scale:

- 0: not applicable
- 1: very poor/no
- 2: poor
- 3: sufficient
- 4: good
- 5: very good/yes

The questionnaire is reported in Table 3:

Table 3: Operational Workshops questionnaire

Operational Workshop	
Date	
Surname	
Name	
Company	

Role							
email							
	0: not applicable 1: very poor/no 2: poor 3: sufficient 4: good 5: very good/yes						
DA01	**Monitored System Overview**						
1.1	Does the System show a correct network, topology and system inventory (comprehensive asset identification)?	0	1	2	3	4	5
1.2	Is the network, topology and system inventory appropriate for the project's goals?	0	1	2	3	4	5
1.3	Is the network reconstruction showing useful geographical information?	0	1	2	3	4	5
DA02	**Monitored System Vulnerability Surface**						
2.1	Does the System show a correct vulnerability inventory (correlation of assets to known vulnerabilities)?	0	1	2	3	4	5
2.2	Is the vulnerability inventory appropriate for the project's goals?	0	1	2	3	4	5
DA03	**Monitored System Mission Impact assessment**						
3.1	Does the System show a correct view of the business processes of the Company, correlated with the dependent ICT/SCADA devices?	0	1	2	3	4	5
3.2	Is the view of the business processes and their relationship with the ICT/SCADA device appropriate for the project's goals?	0	1	2	3	4	5
DA04	**Risk Analysis, Proactive Risk and Attack Graph**						
4.1	Does the System show a correct detection of the possible attack paths within the Monitored System, given a set of entry points?	0	1	2	3	4	5
4.2	Is the attack paths detection consistent with the network topology reconstruction?	0	1	2	3	4	5
4.3	Is the attack paths detection useful?	0	1	2	3	4	5
4.4	Does the System show a reconstruction of the quantification of the level of the Risk of the System?	0	1	2	3	4	5
4.5	Is the Risk quantification analysis appropriate for the project's goals?	0	1	2	3	4	5

DA05	**Strategic Response Overview**						
5.1	Does the System show a prioritized strategic dashboard, with related strategic response plans optimized by risk reduction, response on financial investment impact evaluation and operational impact evaluation?	0	1	2	3	4	5
5.2	Is the strategic response plan computation consistent with the topology of the Monitored System and the quantification of the actual level of the Risk?	0	1	2	3	4	5
5.3	Is the strategic dashboard useful?	0	1	2	3	4	5
DA06	**Architecture Component Overview**						
6.1	Is the software architecture of the Panoptesec coherent with the purposes of the Project?	0	1	2	3	4	5
6.2	Are the Panoptesec software security mechanisms (authentication, crtiptography, etc.) providing an adequate protection for sensitive data?	0	1	2	3	4	5
DA07	**Incident Correlation Overview (IAP analysis)**						
7.1	Is the System able to correlate perceived security incidents with the computed attack paths?	0	1	2	3	4	5
7.2	Does the System visualize these correlations in order to alert the operator that an attack is on going?	0	1	2	3	4	5
7.3	Is the System able to quantify the reactive level of the Risk, given a set of correlated incidents?	0	1	2	3	4	5
DA08	**Tactical Response Plan**						
8.1	Does the System show a prioritize reactive dashboard, with related tactical response plans optimized by risk reduction and operational impact evaluation?	0	1	2	3	4	5
8.2	Are the tactical response plans coherent with the perceived correlated incidents?	0	1	2	3	4	5
8.3	Is the tactical dashboard useful?	0	1	2	3	4	5
Q01	**Do you think that the attack scenarios are realistic?**	0	1	2	3	4	5
Q02	**Do you think that the Panoptesec response time from a proactive perspective is appropriate?**	0	1	2	3	4	5
Q03	**Do you think that the Panoptesec response time from a reactive perspective is appropriate?**	0	1	2	3	4	5

Q04	**Is the graphical user interface appropriate for the project's goals?**	0	1	2	3	4	5
Q05	**Do you think that the Panoptesec or some part of the Panoptesec could be useful in your organization?**	0	1	2	3	4	5
Q06	**Does the system provide useful information?**	0	1	2	3	4	5
Q07	**Does the system provide up to date information?**	0	1	2	3	4	5
Q08	**Is the information clear?**	0	1	2	3	4	5
Q09	**Is the system easy to use?**	0	1	2	3	4	5
Comments:							

The survey follows the storyline of the Workshops, as it has been described within [D8.2.1]. Each Workshop is divided in Demonstration Activities (DA), which cover the validation of the System Requirements from [D2.2.1]. For each Demonstration Activity, a specific set of questions is proposed. Additional questions are then asked as a summary for the session.

2.2 Information analysis

The preliminary results were commented between the partners during the TPM call of 27th October afternoon. The complete results will be commented during the Acceptance Review in November 2016.

2.3 Quality assurance

The QA in the PANOPTESEC Project relies on the assessment of a work product (i.e. deliverable) according to lists of QA checks (QA checklists) established by a QAM, validated at a Consortium level and centralized in the Project Handbook [PH15].

For the purpose of the QA of the [D8.2.2], the deliverable MUST be assessed according the following checklists:

- PEER REVIEW (PR) QA CHECKLIST: the [D8.2.3] deliverable is a report: it then requires a proper peer review.

3 OPERATIONAL WORKSHOPS

3.1 Organization of the Workshops

After the first set of Workshops with internal stakeholders (described within [D8.2.2]), the Installed Prototype has been validated with a set of Operational Workshops open to external stakeholders from the industry, covering banking sector, defence, SMEs, critical infrastructures, public organizations, telecommunication companies, IT companies.

The Workshops were organised on several sessions during the two weeks between 17 and 28 October 2016.

- 17/10/2016: a session in the morning and a session in the afternoon (both with a feedback survey);
- 18/10/2016: a session in the morning and a session in the afternoon (both with a feedback survey);
- 20/10/2016: a session in the morning (with a feedback survey);
- 21/10/2016: a session in the morning and a session in the afternoon (both with a feedback survey);
- 24/10/2016: a session in the morning and a session in the afternoon (both with a feedback survey);
- 25/10/2016: a session in the morning and a session in the afternoon (both with a feedback survey);
- 26/10/2016: a session in the morning and a session in the afternoon (both with a feedback survey);
- 27/10/2016: a session in the morning (with a feedback survey);

- 28/10/2016: a session in the morning and a session in the afternoon (both with a feedback survey);
- 23/11/2016 a session in the morning (with a feedback survey);
- 24/11/2016 a session in the afternoon (with a feedback survey).

These Workshops have been configured as a Live Demo of the PANOPTESEC System through a set of Demonstration Activities (with the same structure of the internal workshops detailed within [D8.2.2]) involving attacks scenarios, cyber security awareness status analysis and up-to-date project results in order to receive external stakeholders feedback to validate the prototype itself.

Proactive scenarios addressed use cases involving collection, correlation and analysis of infrastructure and non-infrastructure (e.g., public vulnerability awareness) data. Reactive scenarios addressed detection, analysis and response to active attacks.

Each demonstration took around 2-3.5 hours, while attendees could interact and make questions and comments about the PANOPTESEC System.

During the demonstrations, after each chapter/scenario, the attendees were asked to fill the feedback questionnaire section dedicated to the specific Demonstration Activity.

The ratio of organizing 20 different sessions with few very qualified attendees for each instead of one/two only crowed event was giving to each attendee time and room to deeply interact with the PANOPTESEC Consortium representatives, ask questions, enter into details.

During these sessions **110** external qualified stakeholders and other **13** internal stakeholders (who could not participate to the Qualification Review) joined the Operational Workshops.

In the following Sections, a specific focus is given to the SMEs attendees among the external stakeholders.

3.1.1 The external stakeholders

The external and qualified stakeholder belong to a number of sectors identified as strategic for the future development of the PANOPTESEC. Among these, the attendees came from the following sectors/industries:

Table 4: Attendees per Sectors/Industry

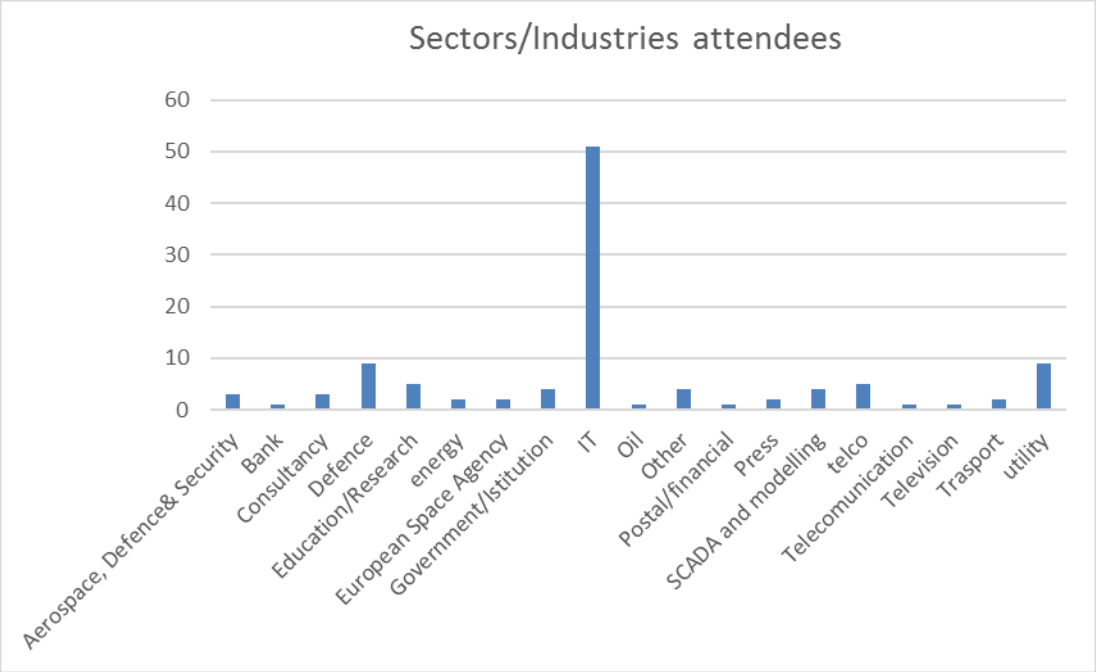
Industry	Attendees
Telecommunication	1
IT	51
Aerospace, Defence & Security (*)	3
SCADA and network modelling	4
Press	2
Energy	2
Government/Institution	4
Banks	1
Consultancy	3
European Space Agency	2
Education/Research	5
Television	1
Telco	5
Transport	2
Defence(**)	9
Utility	9
Postal/Financial	1
Other (***)	4
Oil	1

(*) Companies in the defence Industry

(**) Defence: Ministry of Defence, Military Academies, Army, Air Force, Navy

(***) Canada Embassy

Figure 1: Attendees per Sectors/Industries



In the following table the number of attendees divided per sector and company/public body is reported:

Table 5: Attendees per sector and company/public body

Sector/Companies(public body)	Nr of Attendees
Aerospace, Defence& Security	**3**
Leonardo Company	1
Vitrociset	2
Bank	**1**
San Paolo Inv	1
Consultancy	**3**
consultant	1
PWC Advisory	2
Defence	**9**
Commando C4 Difesa	1
Military Communication Institute (Poland)	2
Ministero Difesa	1
SM Difesa	1
SM Difesa (ITA MOD)	3
SME Difesa (ITA MOD)	1

Education/Research	**5**
CINECA	1
GARR	3
Università Roma La sapienza	1
energy	**2**
Meta Energia	2
European Space Agency	**2**
ESA	2
Government/Istitution	**4**
ENAC	1
Min Interno - CNAIPIC	3
IT	**51**
Acsi Informatica Srl	3
ADFL Consulting	2
Akito	3
Business-E S.p.A.	1
CMP Link Srl	2
DGS	2
EPS Datacom	1
Ericsson	1
ESET	2
Fast Impact	1
Fire Eye	2
Gruppo DAMAN	1
Gruppo PA	4
IBM	2
Info solution	1
Innovery	1
Lutech SpA	3
NSR	3
R1 S.p.A.	8
rds lab	1
Security Matters	2
Servi tecno	1
SIRTI	3
SOGEI SpA	1
Oil	**1**
ERG S.p.A.	1
Other	**4**
Canada Embassy	1
Link Campus/student	1
Utilitalia	2
Postal/financial	**1**
Poste Italiane	1

Press	**2**
Cyber Affairs	1
Fly Orbit news	1
SCADA and modelling	**4**
ATI Srl	1
IDeA Srl	1
Proteo	1
Schneider-Electric	1
telco	**5**
H3G	1
TIM	4
Telecomunication	**1**
BT	1
Television	**1**
RAI	1
Trasport	**2**
Ferrovie dello Stato Italiane	2
utility	**9**
Altop Garda Servizi SpA	1
ASM Terni SpA	2
Dolomiti Energia	2
HERA	1
IREN SPA	3
Total	**110**

3.1.1.1 The Small-Medium Enterprises

During the Operational Workshops SMEs were well represented with 20 attendees belonging to 13 different companies, especially from the industry of IT/ICT and SCADA/integrators.

Table 6: SMEs per sector

Sector/Companies	Nr of Attendees
IT	**17**
Acsi Informatica Srl	3
ADFL Consulting	2
Akito	1
CMP Link Srl	2
Gruppo DAMAN	1
Info solution	1
NSR	3
rds lab	1
Security Matters	2
Servi tecno	1
SCADA and modelling	**3**

ATI Srl	1
IDeA Srl	1
Proteo	1
Total	**20**

3.1.2 The Internal stakeholders

The Internal stakeholders involved within the 2 weeks of the Operational Workshops belong to the Acea Group or to RHEA Group and were not involved in the PANOPTESEC Project (but some of them participated to the Requirements Elicitation phase from Month 1 to 4).

In Table 7 the list of attendees, their company and role:

Table 7: Operational Workshops with internal stakeholders list of attendees

Name/Surname		Company	Role/Dpt
Luciano	Caroti	Acea S.p.A.	ICT Head of Group Solution&Architecture
Fabrizio	Furnò	Acea S.p.A.	Head of ICT Operation Systems
Laura	Diaco	Elabori	Research and Innovation
Alberto	Scarlatti	areti	Supervisor
Azzurra	Trinci	areti	Systems and Technologies
Mario	Bizzi	Rhea	General Manager
Alastair	Pidgeon	Rhea	Business Development
Marco	Peverini	areti	Maintenance Engineering
Luana	Esposito	areti	Engineer
Corrado	Mattaccini	Acea S.p.A.	Security
Domenico	Carletti	Acea S.p.A.	Security
Umberto	Perroni	Acea IP	Public lightening SCADA
Sandro	Marinelli	Acea IP	Public lightening SCADA

Among them, Mrs Diaco could not attend the whole workshop and did not complete the questionnaire.

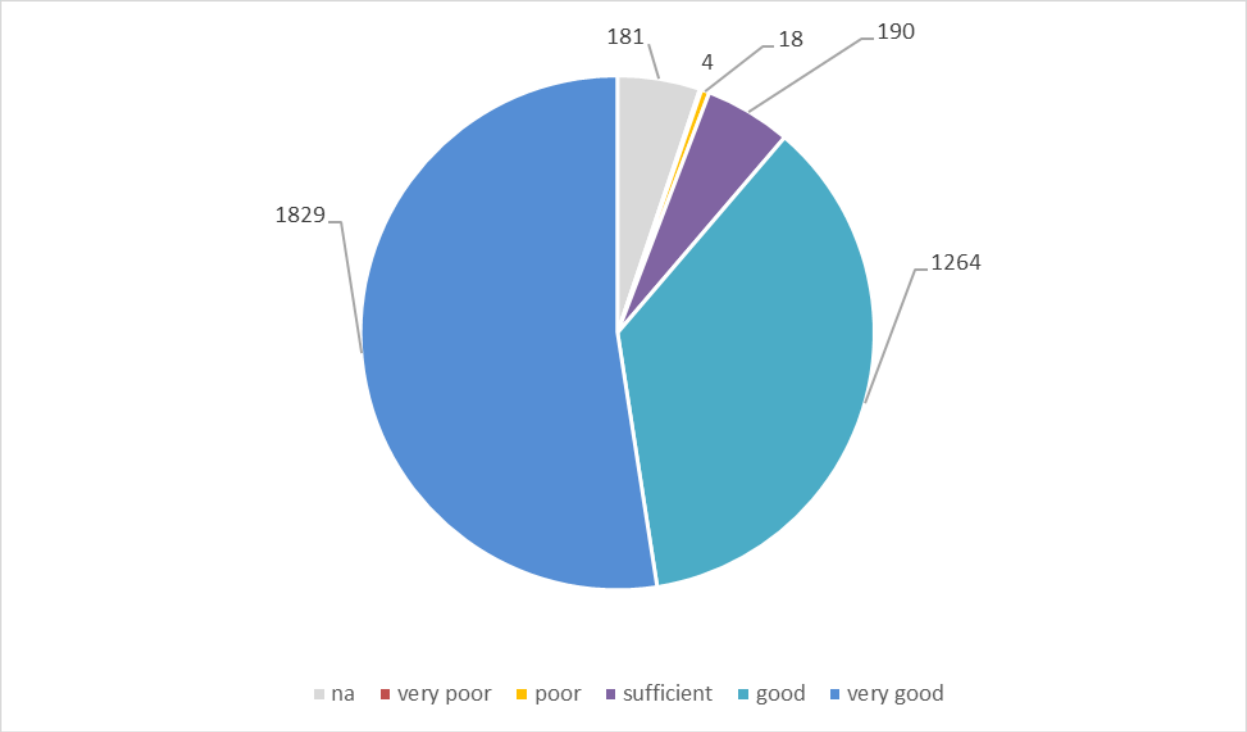
3.2 Results of the survey for external stakeholders

All participants expressed a general satisfaction with the demonstrated PANOPTESEC System.

Out of **109** filled questionnaires (a participant did not fill the questionnaire) and a total of 3486 questions it is possible to count 1829 "very good/yes (5)" and 1264 "good (4)" with an overall average of 4,48.

In the following figures the results are shown.

Figure 2: Overall results for external stakeholders



The details of results are shown in the following figures divided per Demonstration Activity (from [D8.2.1] and questions.

DA01	**Monitored System Overview**
1.1	Does the System show a correct network, topology and system inventory (comprehensive asset identification)?
1.2	Is the network, topology and system inventory appropriate for the project's goals?
1.3	Is the network reconstruction showing useful geographical information?

Score			
na	3	1	1
1	0	1	1
2	1	0	0
3	4	5	6
4	40	37	33
5	61	65	68
mean	4,52	4,53	4,55
	DA01		
	1.1	**1.2**	**1.3**

DA02	**Monitored System Vulnerability Surface**
2.1	Does the System show a correct vulnerability inventory (correlation of assets to known vulnerabilities)?
2.2	Is the vulnerability inventory appropriate for the project's goals?

Score		
na	2	3
1	0	0
2	3	3
3	6	9
4	37	36
5	61	58
mean	4,46	4,41
	DA02	
	2.1	**2.2**

DA03	Monitored System Mission Impact assessment
3.1	Does the System show a correct view of the business processes of the Company, correlated with the dependent ICT/SCADA devices?
3.2	Is the view of the business processes and their relationship with the ICT/SCADA device appropriate for the project's goals?

Score		
na	3	4
1	0	0
2	0	1
3	7	5
4	36	38
5	62	61
mean	4,52	4,51
	DA03	
	3.1	**3.2**

DA04	Risk Analysis, Proactive Risk and Attack Graph
4.1	Does the System show a correct detection of the possible attack paths within the Monitored System, given a set of entrypoints?
4.2	Is the attack paths detection consistent with the network topology reconstruction?
4.3	Is the attack paths detection useful?
4.4	Does the System show a reconstruction of the quantification of the level of the Risk of the System?
4.5	Is the Risk quantification analysis appropriate for the project's goals?

Score					
na	5	4	3	5	4
1	0	0	0	0	0
2	0	0	0	0	0
3	3	2	2	9	7
4	37	38	32	40	40
5	64	65	72	55	58
mean	4,59	4,60	4,66	4,44	4,49
	DA04				
	4.1	**4.2**	**4.3**	**4.4**	**4.5**

DA05	Strategic Response Overview
5.1	Does the System show a prioritized strategic dashboard, with related strategic response plans optimized by risk reduction, response on financial investment impact evaluation and operational impact evaluation?
5.2	Is the strategic response plan computation consistent with the topology of the Monitored System and the quantification of the actual level of the Risk?
5.3	Is the strategic dashboard useful?

Score			
na	4	4	4
1	0	0	0
2	0	0	0
3	1	3	2
4	41	46	46
5	63	56	57
mean	4,59	4,50	4,52
	DA05		
	5.1	**5.2**	**5.3**

DA06	Architecture Component Overview
6.1	Is the software architecture of the Panoptesec coherent with the purposes of the Project?
6.2	Are the Panoptesec software security mechanisms (authentication, cryptography, etc.) providing an adequate protection for sensitive data?

Score		
na	2	11
1	0	0
2	0	0
3	3	10
4	40	47
5	64	41
mean	4,57	4,32
	DA06	
	6.1	**6.2**

DA07	Incident Correlation Overvew (IAP analysis)
7.1	Is the System able to correlate percieved security incidents with the computed attack paths?
7.2	Does the System visualize these correlation in order to alert the operator that a an attack is on going?
7.3	Is the System able to quantify the reactive level of the Risk, given a set of correlated incidents?

Score			
na	7	7	7
1	0	0	0
2	0	0	0
3	5	9	4
4	43	35	40
5	54	58	58
mean	4,48	4,48	4,53
	DA07		
	7.1	**7.2**	**7.3**

DA08	Tactical Response Plan
8.1	Does the System show a prioritize reactive dashboard, with related tactical response plans optimized by risk reduction and operational impact evaluation?
8.2	Are the tactical response plans coherent with the percieved correlated incidents?
8.3	Is the tactical dashboard useful?

Score			
na	8	9	8
1	0	0	0
2	0	0	0
3	2	5	2
4	41	41	32
5	58	54	67
mean	4,55	4,49	4,64
	DA08		
	8.1	**8.2**	**8.3**

Q01	**Do you think that the attack scenarios are realistic?**
Q02	**Do you think that the Panoptesec response time from a proactive perspective is appropriate?**
Q03	**Do you think that the Panoptesec response time from a reactive perspective is appropriate?**

Score			
na	10	8	11
1	0	0	0
2	1	0	1
3	8	11	6
4	32	39	44
5	58	51	47
mean	4,48	4,40	4,40
	Q01	**Q02**	**Q03**

Q04	**Is the graphical user interface appropriate for the project's goals?**
Q05	**Do you think that the Panoptesec or some part of the Panoptesec could be useful in your organization?**
Q06	**Does the system provide useful information?**

Score			
na	8	11	5
1	0	1	0
2	0	5	0
3	5	14	3
4	40	41	39
5	56	36	62
mean	4,50	4,09	4,57
	Q04	**Q05**	**Q06**

Q07	**Does the system provide up to date information?**
Q08	**Is the information clear?**
Q09	**Is the system easy to use?**

Score			
na	6	6	7
1	0	0	1
2	0	1	2
3	7	7	18
4	43	40	50
5	53	55	31
mean	4,45	4,45	4,06
	Q07	**Q08**	**Q09**

The result of the survey states a general full appreciation of the PANOPTESEC System.

Particularly the question DA01-1.3 *"Is the network reconstruction showing useful geographical information?",* had 68 "very good/yes" out of 109 answers (62%) – including the "na" answers - and DA04-4.3." *Is the attack paths detection useful?"* had 72 "very good/yes" out of 109 answers (66%) – including the "na" answers.

The Q09 *"Is the system easy to use?"* received 31 "very good/yes" and 50 "good". It is an important positive feedback (74%) considering that the PANOPTESEC System it is not a commercial product but it is a research software project, with the aim of developing a prototype. This result has been possible thanks to the deep usability refinement performed over the Visualization System during Month 35.

3.2.1.1 Results of the survey for SMEs external stakeholders

All participants belonging to SMEs expressed a general satisfaction with the demonstrated PANOPTESEC System.

Out of 20 filled questionnaires and a total of 643 questions it is possible to count 297 "very good/yes (5)" and 229 "good (4)" with an overall average of 4,37.

In the following figures the results are shown.

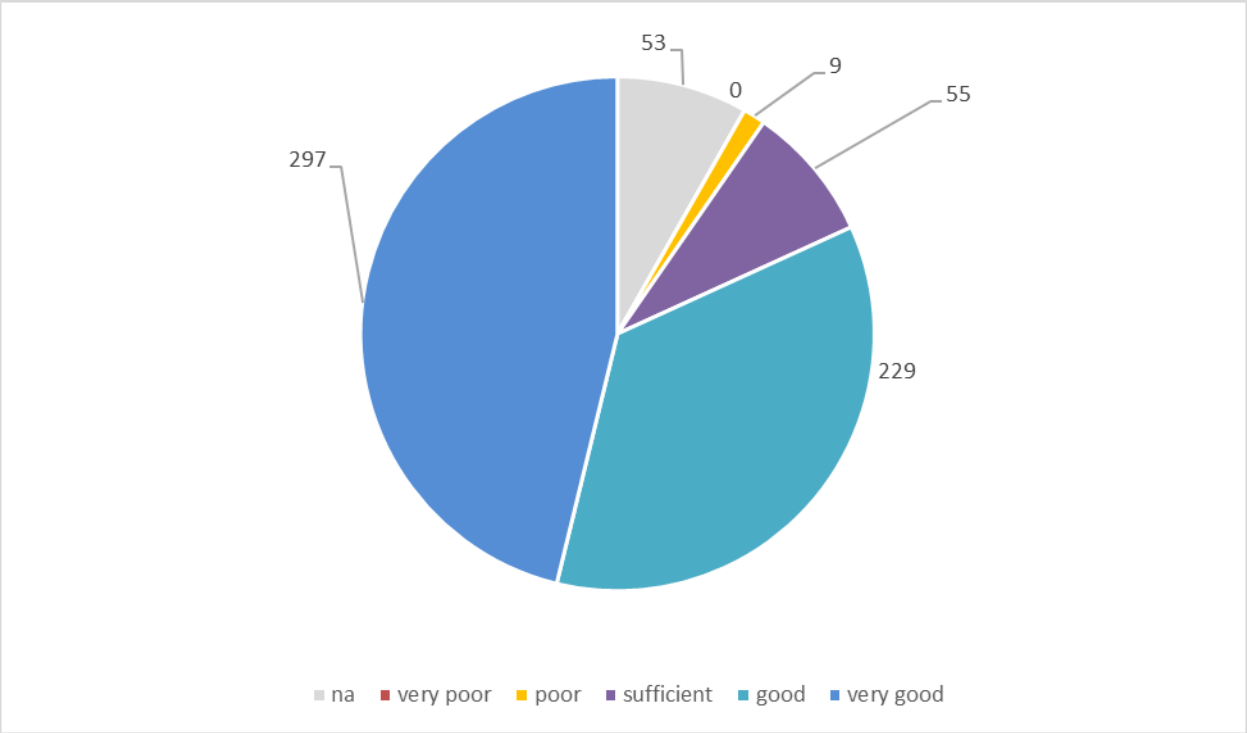


Figure 3: overall results for external stakeholders from SMEs

The details of results are shown in the following figures divided per Demonstration Activity (from [D8.2.1] and questions.

DA01	**Monitored System Overview**
1.1	Does the System show a correct network, topology and system inventory (comprehensive asset identification)?
1.2	Is the network, topology and system inventory appropriate for the project's goals?
1.3	Is the network reconstruction showing useful geographical information?

Score			
na	1	0	1
1	0	0	0
2	0	0	0
3	2	2	1
4	6	9	5
5	11	9	14
mean	4,47	4,35	4,65
	DA01		
	1.1	**1.2**	**1.3**

DA02	**Monitored System Vulnerability Surface**
2.1	Does the System show a correct vulnerability inventory (correlation of assets to known vulnerabilities)?
2.2	Is the vulnerability inventory appropriate for the project's goals?

Score		
na	0	1
1	0	0
2	1	1
3	3	3
4	6	6
5	10	9
mean	4,25	4,21
	DA02	
	2.1	**2.2**

DA03	**Monitored System Mission Impact assessment**
3.1	Does the System show a correct view of the business processes of the Company, correlated with the dependent ICT/SCADA devices?
3.2	Is the view of the business processes and their relationship with the ICT/SCADA device appropriate for the project's goals?

Score		
na	0	0
1	0	0
2	0	0
3	2	2
4	6	7
5	12	11
mean	4,50	4,45
	DA03	
	3.1	**3.2**

DA04	**Risk Analysis, Proactive Risk and Attack Graph**
4.1	Does the System show a correct detection of the possible attack paths within the Monitored System, given a set of entrypoints?
4.2	Is the attack paths detection consistent with the network topology reconstruction?
4.3	Is the attack paths detection useful?
4.4	Does the System show a reconstruction of the quantification of the level of the Risk of the System?
4.5	Is the Risk quantification analysis appropriate for the project's goals?

Score					
na	1	1	3	1	2
1	0	0	0	0	0
2	0	0	0	0	0
3	1	0	1	3	1
4	7	7	5	5	4
5	11	12	13	11	13
mean	4,53	4,63	4,63	4,42	4,67
	DA04				
	4.1	**4.2**	**4.3**	**4.4**	**4.5**

DA05	Strategic Response Overview
5.1	Does the System show a prioritized strategic dashboard, with related strategic response plans optimized by risk reduction, response on financial investment impact evaluation and operational impact evaluation?
5.2	Is the strategic response plan computation consistent with the topology of the Monitored System and the quantification of the actual level of the Risk?
5.3	Is the strategic dashboard useful?

Score			
na	2	2	2
1	0	0	0
2	0	0	0
3	1	1	1
4	6	10	9
5	11	7	8
mean	4,56	4,33	4,39
	DA05		
	5.1	**5.2**	**5.3**

DA06	Architecture Component Overview
6.1	Is the software architecture of the Panoptesec coherent with the purposes of the Project?
6.2	Are the Panoptesec software security mechanisms (authentication, crtiptography, etc.) providing an adequate protection for sensitive data?

Score		
na	0	0
1	0	0
2	0	0
3	2	3
4	6	4
5	12	13
mean	4,50	4,50
	DA06	
	6.1	**6.2**

DA07	**Incident Correlation Overvew (IAP analysis)**
7.1	Is the System able to correlate percieved security incidents with the computed attack paths?
7.2	Does the System visualize these correlation in order to alert the operator that a an attack is on going?
7.3	Is the System able to quantify the reactive level of the Risk, given a set of correlated incidents?

Score			
na	2	2	2
1	0	0	0
2	0	0	0
3	1	2	1
4	9	7	7
5	8	9	10
mean	4,39	4,39	4,50
	DA07		
	7.1	**7.2**	**7.3**

DA08	Tactical Response Plan
8.1	Does the System show a prioritize reactive dashboard, with related tactical response plans optimized by risk reduction and operational impact evaluation?
8.2	Are the tactical response plans coherent with the percieved correlated incidents?
8.3	Is the tactical dashboard useful?

Score			
na	2	2	3
1	0	0	0
2	0	0	0
3	0	1	0
4	10	12	9
5	8	5	8
mean	4,44	4,22	4,47
	DA08		
	8.1	**8.2**	**8.3**

Q01	Do you think that the attack scenarios are realistic?
Q02	**Do you think that the Panoptesec response time from a proactive perspective is appropriate?**
Q03	**Do you think that the Panoptesec response time from a reactive perspective is appropriate?**

Score			
na	2	2	2
1	0	0	0
2	1	0	1
3	1	3	2
4	3	9	6
5	13	6	9
mean	4,56	4,17	4,28
	Q01	**Q02**	**Q03**

Q04	**Is the graphical user interface appropriate for the project's goals?**
Q05	**Do you think that the Panoptesec or some part of the Panoptesec could be useful in your organization?**
Q06	**Does the system provide useful information?**

Score			
na	3	6	2
1	0	0	0
2	0	2	0
3	0	7	2
4	9	4	9
5	8	1	7
mean	4,47	3,29	4,28
	Q04	**Q05**	**Q06**

Q07	**Does the system provide up to date information?**
Q08	**Is the information clear?**
Q09	**Is the system easy to use?**

Score			
na	2	2	2
1	0	0	0
2	0	1	2
3	3	1	2
4	9	8	10
5	6	8	4
mean	4,17	4,28	3,89
	Q07	**Q08**	**Q09**

3.3 Results of the survey for Internal stakeholders

During these sessions 13 internal stakeholders who could not participate to the Qualification Review set of workshops joined the Operational Workshops and gave their feedbacks, expressing a general satisfaction with the demonstrated PANOPTESEC System.

Out of 12 filled questionnaires and a total of 384 questions, it is possible to count 285 “very good/yes (5)” and 85 “good (4)” with an overall average of 4,71.

In the following figures the results are shown.

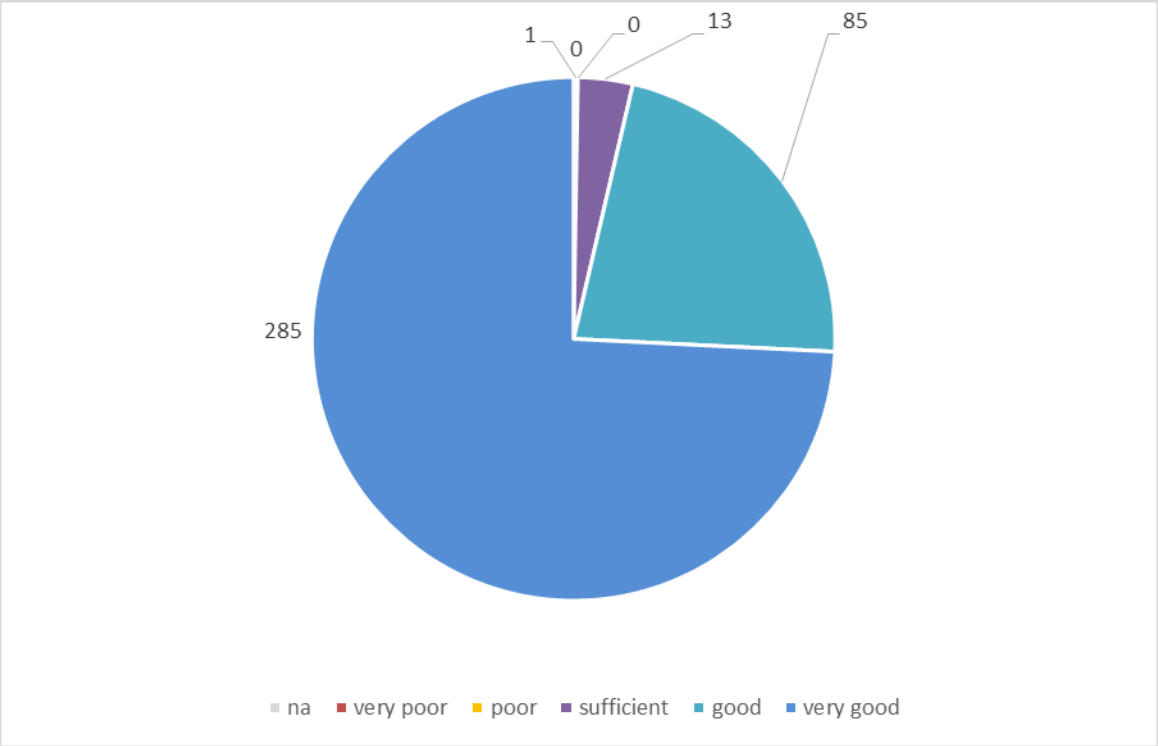


Figure 4: overall results for internal stakeholders

The details of results are shown in the following figures divided per Demonstration Activity (from [D8.2.1] and questions.

DA01	Monitored System Overview
1.1	Does the System show a correct network, topology and system inventory (comprehensive asset identification)?
1.2	Is the network, topology and system inventory appropriate for the project's goals?
1.3	Is the network reconstruction showing useful geographical information?

Score			
na	0	0	0
1	0	0	0
2	0	0	0
3	0	0	0
4	6	4	4
5	6	8	8
	4,50	4,67	4,67
	DA01		
	1.1	**1.2**	**1.3**

DA02	Monitored System Vulnerability Surface
2.1	Does the System show a correct vulnerability inventory (correlation of assets to known vulnerabilities)?
2.2	Is the vulnerability inventory appropriate for the project's goals?

Score		
na	0	0
1	0	0
2	0	0
3	0	0
4	2	2
5	10	10
	4,83	4,83
	DA02	
	2.1	**2.2**

DA03	Monitored System Mission Impact assessment
3.1	Does the System show a correct view of the business processes of the Company, correlated with the dependent ICT/SCADA devices?
3.2	Is the view of the business processes and their relationship with the ICT/SCADA device appropriate for the project's goals?

Score		
na	0	0
1	0	0
2	0	0
3	1	0
4	2	2
5	9	10
	4,67	4,83
	DA03	
	3.1	**3.2**

DA04	Risk Analysis, Proactive Risk and Attack Graph
4.1	Does the System show a correct detection of the possible attack paths within the Monitored System, given a set of entrypoints?
4.2	Is the attack paths detection consistent with the network topology reconstruction?
4.3	Is the attack paths detection useful?
4.4	Does the System show a reconstruction of the quantification of the level of the Risk of the System?
4.5	Is the Risk quantification analysis appropriate for the project's goals?

Score					
na	0	0	0	0	0
1	0	0	0	0	0
2	0	0	0	0	0
3	2	0	0	0	1
4	1	2	3	5	2
5	9	10	9	7	9
	4,58	4,83	4,75	4,58	4,67
	DA04				
	4.1	**4.2**	**4.3**	**4.4**	**4.5**

DA05	**Strategic Response Overview**
5.1	Does the System show a prioritized strategic dashboard, with related strategic response plans optimized by risk reduction, response on financial investment impact evaluation and operational impact evaluation?
5.2	Is the strategic response plan computation consistent with the topology of the Monitored System and the quantification of the actual level of the Risk?
5.3	Is the strategic dashboard useful?

Score			
na	0	0	0
1	0	0	0
2	0	0	0
3	1	0	1
4	2	1	3
5	9	11	8
	4,67	4,92	4,58
	DA05		
	5.1	**5.2**	**5.3**

DA06	**Architecture Component Overview**
6.1	Is the software architecture of the Panoptesec coherent with the purposes of the Project?
6.2	Are the Panoptesec software security mechanisms (authentication, cryptography, etc.) providing an adequate protection for sensitive data?

Score		
na	0	0
1	0	0
2	0	0
3	0	1
4	2	1
5	10	10
	4,83	4,75
	DA06	
	6.1	**6.2**

DA07	**Incident Correlation Overvew (IAP analysis)**
7.1	Is the System able to correlate percieved security incidents with the computed attack paths?
7.2	Does the System visualize these correlation in order to alert the operator that a an attack is on going?
7.3	Is the System able to quantify the reactive level of the Risk, given a set of correlated incidents?

Score			
na	0	0	0
1	0	0	0
2	0	0	0
3	0	1	0
4	2	2	3
5	10	9	9
	4,83	4,67	4,75
	DA07		
	7.1	**7.2**	**7.3**

DA08	Tactical Response Plan
8.1	Does the System show a prioritize reactive dashboard, with related tactical response plans optimized by risk reduction and operational impact evaluation?
8.2	Are the tactical response plans coherent with the percieved correlated incidents?
8.3	Is the tactical dashboard useful?

Score			
na	0	0	0
1	0	0	0
2	0	0	0
3	1	0	0
4	0	2	3
5	11	10	9
	4,83	4,83	4,75
	DA08		
	8.1	**8.2**	**8.3**

Q01	Do you think that the attack scenarios are realistic?
Q02	**Do you think that the Panoptesec response time from a proactive perspective is appropriate?**
Q03	**Do you think that the Panoptesec response time from a reactive perspective is appropriate?**

Score			
na	0	0	0
1	0	0	0
2	0	0	0
3	1	0	0
4	5	4	2
5	6	8	10
	4,42	4,67	4,83
	Q01	**Q02**	**Q03**

Q04	**Is the graphical user interface appropriate for the project's goals?**
Q05	**Do you think that the Panoptesec or some part of the Panoptesec could be useful in your organization?**
Q06	**Does the system provide useful information?**

Score			
na	0	1	0
1	0	0	0
2	0	0	0
3	1	0	0
4	4	1	2
5	7	10	10
	4,50	4,91	4,83
	Q04	**Q05**	**Q06**

Q07	**Does the system provide up to date information?**
Q08	**Is the information clear?**
Q09	**Is the system easy to use?**

Score			
na	0	0	0
1	0	0	0
2	0	0	0
3	0	1	1
4	1	4	6
5	11	7	5
	4,92	4,50	4,33
	Q07	**Q08**	**Q09**

4 CONCLUSIONS

4.1 Significant results achieved

It has been proved, once again, that the Demonstration System Prototype ([D7.4.1]) has been successfully installed within the Demonstration Environment during Month 35.

In terms of the performed Operational Workshops, the Consortium organized 18 sessions between 17 and 28 October 2016 and additional 2 session on the 23 and 24 November 2016 These Workshops received good scores within all surveys.

110 external stakeholders, covering many different industry sectors and various level of responsibilities (from CEOs to Security Operators), joined the Workshops and expressed a high level of interest for the PANOPTESEC System results and concepts. Demonstration sessions lasted for an average of 2 hours and 45 minutes, allowing all participants to ask questions and explore in details concepts, algorithms and methodologies.

4.2 Deliverable validation

This deliverable has been validated in accordance with the quality assurance plan of the PANOPTESEC project as outlined in the [PH15] and following supporting quality review procedures.

5 REFERENCES

[D2.2.1] PANOPTESEC Consortium, *"Operational Requirements", Project deliverable D2.2.1*, Version 2.1, 27.03.2015

[D7.4.1] PANOPTESEC Consortium, *"Demonstration System Prototype", Project deliverable D7.4.1,* Version 1, 31.08.2016

[D7.4.1R] PANOPTESEC Consortium, *"Demonstration System Prototype Verification Report", Project deliverable D7.4.1,* Version 1, 31.08.2016

[D7.4.2] PANOPTESEC Consortium, *"Demonstration System Prototype Report", Project deliverable D7.4.2,* Version 1, 31.10.2016

[D8.2.2] PANOPTESEC Consortium, *"Installed Demonstration System Prototype", Project deliverable D8.2.2,* Version 1, 30.09.2016

[D8.2.2R] PANOPTESEC Consortium, *"Installed Demonstration System Prototype Verification Report", Project deliverable D8.2.2,* Version 1, 30.09.2016

[IEEE-STD-610] The Institute of Electrical and Electronics Engineers (IEEE), *"IEEE Standard Glossary of Software Engineering Terminology"*, *IEEE Std 610.12-1990*, 28.09.1990

[PH15] PANOPTESEC Consortium, *"PANOPTESEC Project Handbook", Project internal document,* version 0.1, 27.03.2015.