FP7-610416-PANOPTESEC

Dynamic Risk Approaches for Automated Cyber Defence

D8.1.4 – Exploitation Report

Work-Package	WP8	Deliverable	D8.1.4
Due Date	M36	Submission Date	14/11/2016
Main Author(s)	RHEA, ACEA		
Contributors	All project participants		
Version	V1.0	Status	FINAL
Dissemination Level	CO	Nature	R
Keywords	Dissemination, exploitation, events, publications, external communications, commercialisation		

Part of the Seventh

Framework Programme

Funded by the EC - DG Connect

EXECUTIVE SUMMARY

This is the deliverable D8.1.4 – Exploitation Report of the FP7 project Dynamic Risk Approaches for Automated Cyber Defence (PANOPTESEC). This work was carried out as part of the WP8 Dissemination and Demonstration and specifically Task 8.1 Information Dissemination and Exploitation.

An important goal of the PANOPTESEC project is to ensure the sustainability of the project's outcomes through the exploitation activities following project closure. To achieve this, it is important to have a clear identification of project outputs, comparison to market technologies and commercial products, combined with a comprehensive exploitation strategy and plan developed by each partner and in collaboration with each other. This document captures the project perspective related to the primary technology outputs, matches capabilities in comparison to commercial products and describes each partner plans for exploitation.

HISTORY

Version	Date	Name/Partner	Comment
V0.0	03-03-2016	Hervé Debar/IMT	Initial creation of the document with ToC and writing assignments. TODOs: - Section 3: for each partner, fill in the table for each component. One subsection per component - Section 3: RHEA, fill in the consolidated products - Section 5: for each partner, revise text
V0.1	22/10/2016	Francesco Bosco/ACEA	Description of actions undertaken by Acea Added actions, papers, event of all the other partners
V0.2	04/11/2016	Francesco Bosco/ACEA	Minor revisions and corrections Added forthcoming event of dissemination
V0.3	09/11/2016	Douglas Wiemer/RHEA	Various updates and insertions from partners relevant to their specific exploitation plans. Additional updates and insertions relevant to comparative assessment to other products.
V0.4	10/11/2016	Douglas Wiemer/RHEA	Various updates and insertions from partners relevant to their specific exploitation plans
V0.5	13/11/2016	Douglas Wiemer/RHEA	Completed completed comparative assessment to other products. Additional inserts updated.
V1.0	14/11/2016	Hervé Debar/IMT	Final version following QA.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 2
HISTORY 3
TABLE OF CONTENTS 4
TABLE OF FIGURES 7
ACRONYMS AND DEFINITIONS 8
1 INTRODUCTION 9
1.1 PURPOSE 9
1.2 SCOPE OF THE PANOPTESEC EXPLOITATION PLAN 9
1.3 DOCUMENT STRUCTURE 9
2 METHODOLOGY 10
2.1 STAKEHOLDER IDENTIFICATION 10
2.2 QUALITY ASSURANCE 10
3 PANOPTESEC OUTPUTS 11
3.1 INDIVIDUAL OUTPUTS 11
3.1.1 Integration Framework 12
3.1.2 Network Inventory Processor 13
3.1.3 Vulnerability Inventory Processor 14
3.1.4 Reachability Matrix Correlator (ontology based) 15
3.1.5 Reachability Matrix Correlator (non-ontology based) 16
3.1.6 Low Level Correlator 17
3.1.7 Network Dependency Analyzer 18
3.1.8 Automata-based Engine, High-level Online Correlator 19
3.1.9 Query-based Engine, High-level Online Correlator 21
3.1.10 Mission Impact Module 22
3.1.11 Attack Graph Generator – Threat Risk Quantifier 24
3.1.12 Strategic Response Decider 26
3.1.13 Tactical Response Decider 27
3.1.14 Visual Analytics Environment 28

3.1.15 Policy Deployer 29
3.1.16 Fast Network Scanner (NetworkInventoryProcessorAgent) 30
3.1.17 ACEA Emulation Environment 32
3.2 PACKAGED OUTPUTS 33
3.2.1 PSEC for Business Risk Management (BRM) 33
3.2.2 Security Incident Management (SIM) 34
3.2.3 Packing roadmaps compared to market delivery 34
3.3 COMPETITIVE MARKET ASSESSMENT 35
3.3.1 Information Technology Risk Management 35
3.3.2 Security Information and Event Management 38
4 EXPLOITATION STRATEGY 42
4.1 INDICATIVE EXPLOITATION PLANS 42
4.2 INTELLECTUAL PROPERTY RIGHTS PRINCIPLES 42
5 PANOPTESEC EXPLOITATION FOR COMMERCIAL PARTNERS 44
5.1 PANOPTESEC EXPLOITATION BY RHEA 44
5.1.1 Partner profile and background 44
5.1.2 Exploitation results and strategy 44
5.1.2.1 Exploitation Results 44
5.1.2.2 Product Packaging and Branding 45
5.1.2.3 Target markets and approach 45
5.1.3 Risks and mitigation strategy 47
5.1.4 Implementation strategy 48
5.2 PANOPTESEC EXPLOITATION BY ALCATEL-LUCENT (ALBFL) 48
5.3 PANOPTESEC EXPLOITATION BY EPISTEMATICA SRL 49
5.3.1 Spin-off 49
5.3.2 Reason for New Company 50
5.3.3 General information 50
5.3.3.1 Name 50
5.3.3.2 Director 50
5.3.3.3 Business 50
5.3.3.4 Product 50
5.3.3.5 Market 50
5.3.3.6 Target 50

5.3.3.7 Beneficiaries 50
5.3.3.8 Other assets 50
5.3.3.9 Startup strategy 50
5.3.3.10 Communication plan 51
5.3.3.11 Future exploitation activities 51
6 PANOPTESEC EXPLOITATION FOR END-USER PARTNERS 52
6.1 PANOPTESEC EXPLOITATION BY ACEA 52
6.1.1 Partner profile and background 52
6.1.2 Exploitation results and strategy 52
6.1.3 Risks and mitigation strategy 52
6.1.4 Implementation strategy 53
7 PANOPTESEC EXPLOITATION FOR ACADEMIC PARTNERS 56
7.1 PANOPTESEC EXPLOITATION BY INSTITUT MINES-TELECOM 56
7.1.1 Partner profile and background 56
7.1.2 Exploitation results and strategy 56
7.1.3 Risks and mitigation strategy 56
7.1.4 Implementation strategy 56
7.1.5 Papers and publications 57
7.2 PANOPTESEC EXPLOITATION BY UNIVERSITÄT ZU LÜBECK (UZL) 57
7.2.1 Partner profile and background 57
7.2.2 Exploitation results and strategy 57
7.2.3 Risks and mitigation strategy 58
7.2.4 Implementation strategy 58
7.2.5 Papers and publications 59
7.3 PANOPTESEC EXPLOITATION BY CENTRALE SUPÉLEC 59
7.3.1 Partner profile and background 59
7.3.2 Exploitation results and strategy 59
7.3.3 Risks and mitigation strategy 60
7.3.4 Implementation strategy 60
7.3.5 Papers and publications 60
7.4 PANOPTESEC EXPLOITATION BY UROME 60
7.4.1 Partner profile and background 60

7.4.2 Exploitation results and strategy *61*
7.4.3 Risks and mitigation strategy *61*
7.4.4 Implementation strategy *62*
7.4.5 Papers and publications *62*
8 CONCLUSIONS 63

TABLE OF FIGURES

FIGURE 1: PANOPTESEC (PSEC) MARKETING PACKAGES 35
FIGURE 2: GARTNER MQ FOR ITRM (MAY 2016) 36
FIGURE 3: GARTNER MQ FOR SIEM (AUGUST 2016) 39

LIST OF TABLES

TABLE 1: ACRONYM LIST 8
TABLE 2: SUMMARY OF PARTNER EXPLOITATION OUTCOMES 11
TABLE 3: PANOPTESEC COMPARISON TO GARTNER MQ IDENTIFIED ITRM CAPABILITIES AND COMPANIES 37
TABLE 4: PANOPTESEC FEATURE COMPARISON TO GARTNER MQ IDENTIFIED ITRM COMPANIES 38
TABLE 5: PANOPTESEC COMPARISON TO GARTNER MQ IDENTIFIED SIEM CAPABILITIES AND COMPANIES 40
TABLE 6: PANOPTESEC FEATURE COMPARISON TO GARTNER MQ IDENTIFIED SIEM COMPANIES 41
TABLE 7: SUMMARY OF PARTNER EXPLOITATION OUTCOMES 63

ACRONYMS AND DEFINITIONS

Table 1: Acronym List

Acronym	Meaning
ACEA	ACEA S.p.A.
ALBLF	Alcatel-Lucent Bell Labs France
UROME	Università Degli Studi Di Roma La Sapienza
DoW	Description of Work
EPIST	Epistematica SRL
ICT	Information and Communication Technology
IMT	Institut Mines-Telecom
RHEA	RHEA System S.A.
SUPELEC	Ecole Supérieure D'Électricité
UCD	User-centered design
UoL	Universität zu Lübeck
D&E	Dissemination and Exploitation
ESA	European Space Agency
EO	Earth Observation
HPC	High Performance Computing
SCADA	Supervisory Control And Data Acquisition
IRT	Institut de Recherche Technologique
EGS-CC	European Ground Systems - Common Core
CDSA	Cyber Defence Situational Awareness
RFI	Request for Information
NATO	North Atlantic Treaty Organization
SSE	Secure Software Engineering
IPR	Intellectual Property Rights

1 INTRODUCTION

1.1 Purpose

The purpose of this document is to provide information concerning the exploitation of its results for the needs and goals of the EU-funded study into Dynamic Risk Approaches for Automated Cyber Defence (PANOPTESEC). Exploitation objectives are set and future steps are defined.

1.2 Scope of the PANOPTESEC Exploitation Plan

The main purpose of the PANOPTESEC Exploitation Plan is to provide a strategy for the exploitation of the project's results after completion of the project. Given the variety of project partners, exploitation strategies and plans will vary in objectives.

1.3 Document Structure

Following this introductory section, this document is divided into five sections covering aspects of exploitation activities and related schedule. The first section covers the dissemination plans including the main tools and channels that will be used to communicate the major project results. This section is followed by the methodology that was followed to develop the D&E plan. The next section outlines the activities in a timeline grid according to the project development year. Finally, the exploitation section provides information about the academic and commercial usage of the project's results. The document concludes with a summary of the results and recommendations.

Section 1 Introduction: describes the context, purpose and scope of the deliverable.

Section 2 Methodology: describes the approach for the development of the D&E plan.

Section 3 Activities: describes the activities done/foreseen in a timeline grid

Section 4 Exploitation Plans: describes the methodology followed in the development of the Exploitation Plans and how each partner plans to exploit the results of this project

Section 5 Conclusion: summarises the findings, results and recommendations.

2 METHODOLOGY

2.1 Stakeholder identification

The PANOPTESEC project has identified the different types of stakeholders, that is persons or entities that may be affected by or may affect the scope and intended use of the system developed in the PANOPTESEC project.

A detailed description of the stakeholders has been included in the document D2.2.1: Operational Requirements (section 2.1 Stakeholder identification). In brief, the following categories have been identified: 1) client stakeholders; 2) market stakeholders; 3) partner stakeholders; and 4) user stakeholders.

The dissemination and exploitation strategy is based on the analysis of the stakeholders identified above.

2.2 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) [18] [19] established by a QAM, validated at a Consortium level and centralised in the Project Handbook [17].

For the purpose of the QA of the D8.1.2, the deliverable has been assessed according the following checklists:

- PEER REVIEW (PR) QA CHECKLIST [18]: the D8.1.2 deliverable is a report, it then requires a proper peer review according to the checks defined in this checklist;
- REQUIREMENTS REVIEW (RR) QA CHECKLIST [19]: the D8.1.2 deliverable being a Requirement documents, it requires the assessment of the checks including in this checklist.

This QA validation process followed the Quality Review Procedure established by the QAM and was validated by the consortium. Detailed results of the review are captured in a report (called QRSR2.1.1). Checklists are available on the PANOPTESEC SVN.

3 PANOPTESEC OUTPUTS

3.1 Individual outputs

The PANOPTESEC project has resulted in a collection of innovative and relevant technology outputs summarized in this section. There are seventeen identified technology outputs. Table 7 summarizes the distribution of participation among identifiable outputs and contributions by project partners.

Table 2: Summary of partner exploitation outcomes

Partner	Participation in Project Outputs	Project Output
IMT	2	Strategic Response Decider, Policy Deployer
SUPELEC	2	High-level Online Correlator (both Query Based and Automaton Based)
UROME	6	Reachability Matrix Correlator (non-ontology), Low-level correlator, High-level Online Correlator (both Query Based and Automaton Based), Mission Impact Module, Visual Analytics Environment
UzL	6	Low-level Correlator, Network Dependency Analyzer, High-level Online Correlator (both Query Based and Automaton Based), Mission Impact Module, Visual Analytics Environment
ACEA	1*	Emulation Environment, All
RHEA	17**	Integration framework, Network Inventory Processor, Vulnerability Inventory Processor, Fast Network Scanner, Emulation Environment, All
ALBLF	3	Attack Graph Generator – Threat Risk Quantifier, Tactical Response Decider, Policy Deployer
EPIST	1	Reachability Matrix Correlator (ontology-based)

* Although ACEA is noted specifically for their contribution to the Emulation Environment, it is further recognized that the contributions of ACEA in the area of use cases, threat scenarios, and access to a test environment was essential to the development of all project outputs.

** In their capacity as leads for System Architecture as well as System Integration and Test, RHEA made contributions to the progress of all components as related to their compliance with the data model, interfaces, and execution orchestration. From verification perspective, RHEA provided analysis of outcomes against the emulation environment ground truth, leading to identification of processing errors, etc. thereby contributing to all outcomes.

3.1.1 Integration Framework

Exploitable result	
Functionality	The Integration Framework is the glue of the PANOPTESEC System. Based on an open source Java technological stack, it manages the integration of each PANOPTESEC System component and the interactions with the Visual Analytics Environment. The IF also manages the messaging orchestration between the components, their runtime management and the security of the messaging system itself
Purpose	The initial purpose of the Integration Framework was to allow a modular architecture for the PANOPTESEC System, enabling an easy integration of the various components and the management of their messages exchange
Innovation	The Integration Framework is based on well-known Java open source technologies and frameworks. The resulting development, however, has been proven as extremely reliable and easy to use. Components integration proceeded much faster than expected in similar projects, due to the efficient integration procedures. Dependability features, not present in the original technological stack from Apache, have been added. The development of the Integration Framework directly derives from the Low Level Design of the System: several parts of the Framework are code-generated. This allowed the developers and the architects to have a fast verification over the architecture months before the real integration of the components.
Partner(s) involved	RHEA
Role and activities	Research, Design, Development, Integration and Test
How the result will be exploited	(RHEA) The approach followed for the Integration Framework can be adapted on several different contexts, were large scale integration of Java components is needed. The code-generation capabilities will be explored by RHEA: an extension of the feature, as a separate development from the PANOPTESEC, is already scheduled. The component capabilities will be used by RHEA as part of a future commercial product under RHEA unique branding but overall encompassing all PANOPTESEC features and augmented by supporting

	features including for example, incident work flow management. The code will form the basis of a more complete cyber integration test and engineering framework (CITEF) to be delivered under a wider funding programme of the European Space Agency and supported by the Belgium Science Policy Organization (BelSPO).
Additional research and development work	(RHEA) The possibility to code-generate the Integration Framework is extremely interesting, from an architectural verification perspective. Due to its structure, it is possible to code-generate a complete set of integrated (empty, but with basic functionalities, and all the correct orchestration and messaging means already working) components, managing interfaces and messaging means. From an architecture verification point of view (usually it is very difficult to verify a complex modular architecture) such feature could be extremely useful, allowing the architect to generate a running modular System directly from the Design.
IPR measures	Protected under various copyright statements incorporated into PANOPTESEC related design documents and code, supported by relevant publications and presentations.
Commercial contacts	(RHEA) Commercial contacts have been identified with Leonardo, Raytheon, Lutech, Telecom Italia Mobile, MetaEnergia, the European Defence Agency (EDA) and the Polish Military Communications, Institute.
Target groups	(RHEA) As part of a RHEA branded product or embedded technology in cyber security supply chain to Aerospace, Defence, Critical Infrastructure, Banking / Finance, Crisis Management and Response.

3.1.2 Network Inventory Processor

Exploitable result	
Functionality	The NetworkInventoryProcessor manages the collection of topology/inventory data from the Monitored System. It is able to connect with different network scanners, orchestrate their scan results and reconstruct the NetworkInventory
Purpose	Within the context of the PANOPTESEC System, the NetworkInventoryProcessor computes the NetworkInventory from the MonitoredSystem and starts the proactive chain
Innovation	The NetworkInventoryProcessor does not depend from the data sources: it is able to connect and to orchestrate data coming from multiple different sources. Its architecture allows the component to use different parsers for the different data sources: adding a data source just requires

	the development of a new parser and the orchestration rules useful for integrating the new set of data
Partner(s) involved	RHEA
Role and activities	Research, Design, Development, Integration and Test
How the result will be exploited	(RHEA) The NetworkInventoryProcessor can be extremely feasible on any topology data collection process. With the fast scanner based on Nmap (NetworkInventoryProcessorAgent), it can be deployed on different network and easily collect topology data useful for security/network assessment. The component capabilities will be used by RHEA as part of a future commercial product under RHEA unique branding but overall encompassing all PANOPTESEC features and augmented by supporting features including for example, incident work flow management.
Additional research and development work	(RHEA) The NetworkInventoryProcessor will be further developed in order to improve its open architecture and performance.
IPR measures	Protected under various copyright statements incorporated into PANOPTESEC related design documents and code, supported by relevant publications and presentations.
Commercial contacts	(RHEA) Commercial contacts have been identified with Leonardo, Raytheon, Lutech, Telecom Italia Mobile, MetaEnergia, the EDA and the Polish Military Communications, Institute.
Target groups	(RHEA) As part of a RHEA branded product or embedded technology in cyber security supply chain to Aerospace, Defence, Critical Infrastructure, Banking / Finance, Crisis Management and Response.

3.1.3 Vulnerability Inventory Processor

Exploitable result	
Functionality	The VulnerabilityInventoryProcessor manages the collection of vulnerability data from the Monitored System. It is able to connect with different vulnerability scanners, orchestrate their scan results (combined with the topology scans results) and reconstruct the VulnerabilityInventory
Purpose	Within the context of the PANOPTESEC System, the

	VulnerabilityInventoryProcessor computes the VulnerabilityInventory from the MonitoredSystem
Innovation	The VulnerabilityInventoryProcessor does not depend from the data sources: it is able to connect and to orchestrate data coming from multiple different sources. Its architecture allows the component to use different parsers for the different data sources: adding a data source just requires the development of a new parser and the orchestration rules useful for integrating the new set of data
Partner(s) involved	RHEA
Role and activities	Research, Design, Development, Integration and Test
How the result will be exploited	(RHEA) The VulnerabilityInventoryProcessor can be extremely feasible on any vulnerability data collection process. The component capabilities will be used by RHEA as part of a future commercial product under RHEA unique branding but overall encompassing all PANOPTESEC features and augmented by supporting features including for example, incident work flow management.
Additional research and development work	(RHEA) The VulnerabilityInventoryProcessor will be further developed in order to improve its open architecture and performance.
IPR measures	Protected under various copyright statements incorporated into PANOPTESEC related design documents and code, supported by relevant publications and presentations.
Commercial contacts	(RHEA) Commercial contacts have been identified with Leonardo, Raytheon, Lutech, Telecom Italia Mobile, MetaEnergia, the EDA and the Polish Military Communications, Institute.
Target groups	(RHEA) As part of a RHEA branded product or embedded technology in cyber security supply chain to Aerospace, Defence, Critical Infrastructure, Banking / Finance, Crisis Management and Response.

3.1.4 Reachability Matrix Correlator (ontology based)

Exploitable result	
Functionality	The Reachability Matrix Correlator (RMC) computes the Reachability_Matrix, needed by the Dynamic Risk Management Response System, the Mission Impact Model and the Visualization

	System. This Correlator component performs the reachability computation across data collected from the Monitored System(s) to deduct if two nodes are reachable from each other in the network, for all pairs of nodes representing Device(s) of the Monitored System(s)
Purpose	The Reachability Matrix Correlator (RMC) computes the Reachability Matrix
Innovation	The Reachability Matrix Correlator has been developed using semantic technologies
Partner(s) involved	Epistematica, RHEA
Role and activities	Research, Dissemination, Design, Development, Integration and Test
How the result will be exploited	Epistematica is creating a startup (Renodes) that will sell online digital services and the licence of the software component (RMC), through a specialized e-commerce website.
Additional research and development work	(EPIST) After the published paper "A semantic approach to reachability matrix computation", Epistematica is writing a new paper to extend this semantic approach to the data protection field (following The General Data Protection Regulation - UE 2016/679).
IPR measures	Copyleft for the RMC ontology. Protected under various copyright statements incorporated into PANOPTESEC related design documents and code, supported by relevant publications and presentations.
Commercial contacts	(RHEA) Commercial contacts have been identified with Leonardo, Raytheon, Lutech, Telecom Italia Mobile, MetaEnergia, the EDA and the Polish Military Communications, Institute.
Target groups	Companies and people worldwide that would like manage its cyber security risks, without having strong technical competencies. (RHEA) As part of a RHEA branded product or embedded technology in cyber security supply chain to Aerospace, Defence, Critical Infrastructure, Banking / Finance, Crisis Management and Response.

3.1.5 Reachability Matrix Correlator (non-ontology based)

Exploitable result	
Functionality	The Reachability Matrix Correlator (RMC) computes the Reachability_Matrix, needed by the Dynamic Risk Management Response System, the Mission Impact Model and the Visualization System. This Correlator component performs the reachability

	computation across data collected from the Monitored System(s) to deduct if two nodes are reachable from each other in the network, for all pairs of nodes representing Device(s) of the Monitored System(s)
Purpose	The Reachability Matrix Correlator (RMC) computes the ReachabilityMatrix
Innovation	The Reachability Matrix Correlator (non-ontology version) includes innovation in areas of process algorithm optimization.
Partner(s) involved	UROME, RHEA
Role and activities	Research, Design, Development, Integration and Test
How the result will be exploited	(RHEA/UROME) The component capabilities will be used by RHEA as part of a future commercial product under RHEA unique branding but overall encompassing all PANOPTESEC features and augmented by supporting features including for example, incident work flow management.
Additional research and development work	(RHEA/UROME) The ReachabilityMatrixCorrelator (non-ontology-based) will be further developed in order to improve its open architecture and performance.
IPR measures	Protected under various copyright statements incorporated into PANOPTESEC related design documents and code, supported by relevant publications and presentations.
Commercial contacts	(RHEA) Commercial contacts have been identified with Leonardo, Raytheon, Lutech, Telecom Italia Mobile, MetaEnergia, the EDA and the Polish Military Communications, Institute.
Target groups	(RHEA) As part of a RHEA branded product or embedded technology in cyber security supply chain to Aerospace, Defence, Critical Infrastructure, Banking / Finance, Crisis Management and Response.

3.1.6 Low Level Correlator

Exploitable result	
Functionality	The Low Level Correlator additionally comprises the Alert Normalization Processor (ANP) functionalities and parts of the Data Collection Processor (DCP) functionalities. Its purpose is to normalize security events generated by heterogeneous data sources and correlate them whilst being usable in different

	networks. The event normalization is generated based on Syslog-ng Server
Purpose	Its purpose is to normalize security events generated by heterogeneous data sources and correlate them whilst being usable in different networks.
Innovation	The Low Level Correlator encompasses innovative approaches to integration and correlation of event data from multiple independent sources including analysis within specified time windows.
Partner(s) involved	UzL, RHEA, UROME
Role and activities	Research, Dissemination, Design, Development, Integration and Test
How the result will be exploited	(RHEA/UzL) The component capabilities will be used by RHEA as part of a future commercial product under RHEA unique branding but overall encompassing all PANOPTESEC features and augmented by supporting features including for example, incident work flow management.
Additional research and development work	(RHEA/UzL) The LowLevelCorrelator will be further developed in order to improve its open architecture and performance.
IPR measures	Protected under various copyright statements incorporated into PANOPTESEC related design documents and code, supported by relevant publications and presentations.
Commercial contacts	(RHEA) Commercial contacts have been identified with Leonardo, Raytheon, Lutech, Telecom Italia Mobile, MetaEnergia, the EDA and the Polish Military Communications, Institute.
Target groups	(RHEA) As part of a RHEA branded product or embedded technology in cyber security supply chain to Aerospace, Defence, Critical Infrastructure, Banking / Finance, Crisis Management and Response.

3.1.7 Network Dependency Analyzer

Exploitable result	
Functionality	The Network Dependency Analyser component is responsible for analysing collected TCPDumps with the network traffic of the Monitored System and correlates this information with the latest version of the Network Inventory, in order to continuously assess dependencies between network assets. The output, the Shallow Network Dependency

	Model, is used by the Mission Impact Module in order to verify the correctness of the dependencies identified in the Mission Graph produced by the Mission Impact Module.
Purpose	The Network Dependency Analyser component is responsible for verifying the correctness of the dependencies identified in the MissionGraph produced by the Mission Impact Model
Innovation	Incorporates innovative approaches to analysis of system dependencies comparing known asset inventory information with event data.
Partner(s) involved	UzL, RHEA
Role and activities	Research, Dissemination, Design, Development, Integration and Test
How the result will be exploited	(RHEA/UzL) The component capabilities will be used by RHEA as part of a future commercial product under RHEA unique branding but overall encompassing all PANOPTESEC features and augmented by supporting features including for example, incident work flow management.
Additional research and development work	(RHEA/UzL) The NetworkDependencyAnalyzer will be further developed in order to improve its open architecture and performance.
IPR measures	Protected under various copyright statements incorporated into PANOPTESEC related design documents and code, supported by relevant publications and presentations.
Commercial contacts	(RHEA) Commercial contacts have been identified with Leonardo, Raytheon, Lutech, Telecom Italia Mobile, MetaEnergia, the EDA and the Polish Military Communications, Institute.
Target groups	(RHEA) As part of a RHEA branded product or embedded technology in cyber security supply chain to Aerospace, Defence, Critical Infrastructure, Banking / Finance, Crisis Management and Response.

3.1.8 Automata-based Engine, High-level Online Correlator

Exploitable result	
Functionality	The ABE-HOC aims at providing the detection of multi-step attacks against the monitored system, by correlating low level alerts. The component takes as input the description of the expected attack scenarios (called Attack Paths) and generate automata capable of

	detecting a sequence of Low Level Alerts compatible with at least one of the defined Attack Paths.
Purpose	The purpose of this component is to correlate low level alerts to enhance the knowledge of the administrator about the ongoing multi-step attacks occurring in its monitored system. It prevents the administrator to be annoyed by overwhelming low semantic low level alerts.
Innovation	The algorithms deployed are efficient and permit to detect approximate attack paths, which is a novelty compared to previous explicit correlation approaches.
Partner(s) involved	Supelec, UROME, RHEA, UzL
Role and activities	Research, Teaching, Design, Development, Integration and Test
How the result will be exploited	(SUPELEC) We have already been approached by potential industrial partners that are interested by the developed technology, and could aim at adapting our approach to their products. Further developments will be performed in the context of student projects to support teaching activities in the context of intrusion detection courses. (RHEA) The component capabilities will be used by RHEA as part of a future commercial product under RHEA unique branding but overall encompassing all PANOPTESEC features and augmented by supporting features including for example, incident work flow management.
Additional research and development work	(SUPELEC) A thesis with an industrial partner on this topic is planned to begin at the beginning of October 2016. (RHEA) Concept optimization and component rework will be pursued to improve the open architecture and component performance before re-integration into the wider RHEA branded product.
IPR measures	Protected under various copyright statements incorporated into PANOPTESEC related design documents and code, supported by relevant publications and presentations.
Commercial contacts	(SUPELEC) Thales, DGA-MI (RHEA) Commercial contacts have been identified with Leonardo, Raytheon, Lutech, Telecom Italia Mobile, MetaEnergia, the EDA and the Polish Military Communications, Institute.
Target groups	Companies that develop SIEMs and correlator components (RHEA) As part of a RHEA branded product or embedded technology in cyber security supply chain to Aerospace, Defence, Critical Infrastructure,

	Banking / Finance, Crisis Management and Response.

3.1.9 Query-based Engine, High-level Online Correlator

Exploitable result	
Functionality	QBE-HOC is an engine able to analyse streams of low level alerts and detect multi-step attacks against the monitored system. This is done, by matching the alert stream flow with multi-step attack models.
Purpose	The purpose of this component is to correlate low-level alerts with the aim to provide network administrators with a higher degree of situation awareness, in order to help them to take decisions without being flooded by the large number of low-level alerts.
Innovation	The main innovation is given by the on-line matching done through complex event processing based on attacks graphs. The detection is done through an estimation that is able to take in to account different issues coming from the deployment in large-scale networks i.e., absence of perfect synchronization, incomplete or inaccurate information, message loss.
Partner(s) involved	UROME, RHEA, UzL, Supelec
Role and activities	Research, Teaching, Design, Development, Integration and Test
How the result will be exploited	(UROME) UROME are starting to present the preliminary results of the experimentation in several research meetings (both including academics and industrial partners). UROME received many manifestations of interests from potential industrial partners that are interested by the developed technology, and could aim at adapting the approach to their products. This is a starting point for the definition of other initiatives (e.g. H2020 IA) that will bring the component from the prototype stage towards the integration in to market products. In addition, being an academic partner, UROME will continue our investigation on the pure research side by continue the development in the context of student projects to support teaching activities of the Master Degree Program. (RHEA/UROME) The component capabilities will be used by RHEA as part of a future commercial product under RHEA unique branding but overall encompassing all PANOPTESEC features and augmented by supporting

	features including for example, incident work flow management.
Additional research and development work	(UROME) Three Master thesis have been recently concluded (in October 2016). The main outcomes have been (i) the definition of a new metric to evaluate the similarity between a sequence of alert and one of the attack scenario represented in the Attack Graph, (ii) an heuristic to discard past alert with the final aim to minimize the impact of memory cleaning on the generation of false negative and (iii) a first algorithm for the Potential Attack Identification (PAI) module. Other thesis are available to improve some aspects of the QBE-HOC component and to understand how it can be decupled by the whole PANOPTESEC architecture. This is the basic step for the feasibility analysis of a new spin-off around this asset. (RHEA/UROME) Concept optimization and component rework will be pursued to improve the open architecture and component performance before re-integration into the wider RHEA branded product.
IPR measures	Protected under various copyright statements incorporated into PANOPTESEC related design documents and code, supported by relevant publications and presentations.
Commercial contacts	UROME has many contacts with SOGEI and Finmeccanica (now Leonardo) that can be exploited for further development of our component. (RHEA) Commercial contacts have been identified with Leonardo (collaboration with UROME), Raytheon, Lutech, Telecom Italia Mobile, MetaEnergia, the EDA (collaboration with UROME) and the Polish Military Communications, Institute.
Target groups	Companies that develop SIEMs and correlator components and entities interested in supporting the experimentation in other domains. (RHEA) As part of a RHEA branded product or embedded technology in cyber security supply chain to Aerospace, Defence, Critical Infrastructure, Banking / Finance, Crisis Management and Response.

3.1.10 Mission Impact Module

Exploitable result	
Functionality	The MIM is used to obtain a mission impact assessment, i.e., an assessment of local impacts created due to widespread events onto a higher goal. A higher goal, e.g., a mission or company, is modelled from an operational mission perspective and from an operational resource perspective. Resources form a dependency network with locally affected

	nodes. The impact of a local affection of a resource and transitive invoked impacts of dependent resources is assessed towards the highest goal modelled from an operational mission perspective.
Purpose	The MIM is used in the Panoptesec system to assess "collateral damage" potentially caused by proposed response plans, which are local actions invoked on resources leading to local impacts, onto a higher goal, i.e., the company of a use case. Further, the MIM is used to assess an impact onto a company based on vulnerabilities present on individual ICT devices, i.e., resources.
Innovation	Current approaches attempting to solve mission impact assessment employ score-based algorithms leading to spurious results. We identify a fourfold problem with score-based algorithms: 1) score-based algorithms enforce deep training of experts to employed frameworks for specification (non-context-free), 2) require reference results for interpreting obtained results (non-bias-free), 3) require assessments outside of an experts' expertise (non-local), and 4) require validation of end-results against ground truth. The MIM provides a formal, mathematical model for bias- and context-free mission impact assessment. Based on a probabilistic model mission impact assessment is reduced to a well-understood mathematical problem based on definitions from local expertise and allow for a validation at data level. This is useful for areas and applications where qualitative assessments are required, such as assessments in critical infrastructures or military contexts.
Partner(s) involved	UzL, RHEA, UROME
Role and activities	Research, Dissemination, Design, Development, Integration and Test
How the result will be exploited	(UzL) Theory developed towards a probabilistic mission impact assessment used inside the MIM is exploited towards scientific publications. Further, fundamental research on probabilistic graphical model lead to scientific publication on artificial intelligence in major conferences such as IJCAI and is further used as part of an PhD thesis. Commercial exploitation is underway by a redistribution of the technology behind the MIM. UzL stand in contact with security software development company CYPP[1] and end-user Plath[2]. (RHEA/UzL) The component capabilities will be used by RHEA as part of a

[1] http://www.cypp.de
[2] http://www.plath.de

	future commercial product under RHEA unique branding but overall encompassing all PANOPTESEC features and augmented by supporting features including for example, incident work flow management.
Additional research and development work	(UzL/RHEA) In order for the MIM to be distributed as a standalone assessment product, an integrated bundle of NetworkDependencyAnalyzer, NetworkInventoryProcessor and VulnerabilityInventoryProcessor is required, which is partially available. Further, an individual GUI is required. Therefore, the component will be further developed in order to improve its capabilities.
IPR measures	Protected under various copyright statements incorporated into PANOPTESEC related design documents and code, supported by relevant publications and presentations.
Commercial contacts	(UzL) The University of Lübeck stands in contact with security company CYPP and end-user company Plath. (RHEA) Commercial contacts have been identified with Leonardo, Raytheon, Lutech, Telecom Italia Mobile, MetaEnergia, the EDA and the Polish Military Communications, Institute.
Target groups	Companys developing security related products as licensee and redistributor of MIM related theory and components. End users of small medium enterprises requiring a feasible assessment of probable impacts onto an IT infrastructure. (RHEA) As part of a RHEA branded product or embedded technology in cyber security supply chain to Aerospace, Defence, Critical Infrastructure, Banking / Finance, Crisis Management and Response.

3.1.11 Attack Graph Generator – Threat Risk Quantifier

Exploitable result	
Functionality	The Attack Graph Generator and Threat Risk Quantifier (i.e. AGG-TRQ) software component is a unified component that implements two functions of the global Functional Architecture of the PANOPTESEC: Attack Graph Generator and Threat Risk Quantifier functions. First, AGG-TRQ calculates the exposure of the Monitored System to threats. This is achieved by calculating an Attack Graph, as a set of Attack paths. Each Attack path depicts an attack scenario that starts from a predefined entry point, and reaches to a critical machine in the system (Monitored System). This exposure is captured on two levels: • Proactive level: AGG-TRQ calculates attack graphs corresponding

	to all potential attack scenarios for the Monitored System. Hence, the exposure of the Monitored System is captured regardless whether there are ongoing attack attempts in the monitored system. This exposure is relevant to assess the proactive risk posture of the Monitored System, which characterises the risk profiles of the monitored systems on the mid-long term. • Reactive level: AGG-TRQ calculates attack graphs corresponding to observed and ongoing attack scenarios. Hence, the exposure is captured considering detected attack events and corresponding alerts detected by the intrusion detections systems. Such exposure is relevant to assess the reactive risk posture of the Monitored System, which characterizes the risk profile of the Monitored System on the short-term while considering ongoing and observed attacks.
Purpose	Within the context of the PANOPTESEC Project, the AGG-TRQ works both on the Proactive and on the Reactive Chain. Within the Proactive Chain, it computes all attack paths given hypothetical entry points, and evaluates the actual level of the risk. Within the reactive chain, it receives and analyses the alerts from the correlators in order to evaluate the dynamic level of the risk given a possible attack situation
Innovation	Incorporates Attack Graph concepts into a risk-based analysis approach for both proactive and reactive risk calculations.
Partner(s) involved	ALBLF, RHEA
Role and activities	Research, Dissemination, Design, Development, Integration and Test
How the result will be exploited	(RHEA) The component capabilities will be used by RHEA as part of a future commercial product under RHEA unique branding but overall encompassing all PANOPTESEC features and augmented by supporting features including for example, incident work flow management.
Additional research and development work	(RHEA) Concept optimization and component rework will be pursued to improve the open architecture and component performance before re-integration into the wider RHEA branded product.
IPR measures	Protected under various copyright statements incorporated into PANOPTESEC related design documents and code, supported by relevant publications and presentations.
Commercial contacts	(RHEA) Commercial contacts have been identified with Leonardo, Raytheon, Lutech, Telecom Italia Mobile, MetaEnergia, the EDA and the

	Polish Military Communications, Institute.
Target groups	(RHEA) As part of a RHEA branded product or embedded technology in cyber security supply chain to Aerospace, Defence, Critical Infrastructure, Banking / Finance, Crisis Management and Response.

3.1.12 Strategic Response Decider

Exploitable result	
Functionality	The SRD-RFIA component aims at handling reported threats identified against the Monitored System, by processing abstract policies, pre-authorized lists of mitigation actions and producing concrete response policies. It conducts a financial evaluation of the response policies based on a Return On Response Investment (RORI) index. It evaluates and selects mitigation actions from a pool of candidates, by ranking them. The purpose of this component is to preselect sets of combined mitigation actions that are identified as optimal from a financial perspective and propose them to reduce the risk of threats against the Monitored System
Purpose	The purpose of this component is to preselect sets of combined mitigation actions that are identified as optimal from a financial perspective and propose them to reduce the risk of threats against the Monitored System
Innovation	The component provides a way to close the loop between detection of a threat and mitigation. Since time is of the essence when reacting to cyber-threats, it supports operators in successfully selecting the appropriate countermeasures to a set of ongoing threats.
Partner(s) involved	IMT, RHEA
Role and activities	Research, Dissemination, Design, Development, Integration and Test
How the result will be exploited	(IMT) Results are exploited through scientific publications in peer reviewed international conferences and journals. 10 publications have been achieved (published or under review) during the lifetime of the project. Beyond the project, IMT is working on the development of a patent portfolio and the associated business plan (see commercial contacts). Results are exploited through scientific publications in peer reviewed international conferences and journals. (RHEA/IMT) The component capabilities are intended to be used by

	RHEA as part of a future commercial product under RHEA unique branding but overall encompassing all PANOPTESEC features and augmented by supporting features including for example, incident work flow management.
Additional research and development work	(IMT) Additional research continues in the development of visualization tools that project security actions in an n-dimensional system so that impacts of malicious and benign actions could be assessed appropriately. (RHEA) Concept optimization and component rework will be pursued to improve the open architecture and component performance before re-integration into the wider RHEA branded product.
IPR measures	One patent has been granted. Protected under various copyright statements incorporated into PANOPTESEC related design documents and code, supported by relevant publications and presentations.
Commercial contacts	(IMT) In contact with France Brevet, with the goal to build a patent portfolio on this technology applied to a specific domain, in order to prepare a marketable portfolio that can be sold to network equipment vendors. (RHEA) Commercial contacts have been identified with Leonardo, Raytheon, Lutech, Telecom Italia Mobile, MetaEnergia, the EDA and the Polish Military Communications, Institute.
Target groups	Companies developing security related products, as well as enterprises requiring a feasible assessment of probable impacts onto an IT infrastructure. ((RHEA) As part of a RHEA branded product or embedded technology in cyber security supply chain to Aerospace, Defence, Critical Infrastructure, Banking / Finance, Crisis Management and Response.

3.1.13 Tactical Response Decider

Exploitable result	
Functionality	While the Strategic Response Decider component envisages identified risks mitigation on a long-term proactive perspective, detection of on-going attacks' progressions towards critical Assets of the organization may increase the value of some identified risks beyond an acceptable level. Moreover, detection of new attackers may raise new risks, if the detected entry point of this new attacker is not a node of an already computed and monitored AttackGraph. In these cases, a reprioritization of the risks that should be addressed needs to be performed and MitigationAction(s) have to be taken with this new reactive perspective.

	This is the main function of the Tactical Response Decider component, which obviously has to coordinate its decided Response Plans with the proactive Response Plans established by the Strategic Response Decider component.
Purpose	The main function of the Tactical Response Decider component is to react to a detection of an attack and compute tactical mitigation actions
Innovation	Provides automated decision support capabilities through evaluation and prioritization of response plans.
Partner(s) involved	ALBLF, RHEA
Role and activities	Research, Dissemination, Design, Development, Integration and Test
How the result will be exploited	(RHEA) The component capabilities will be used by RHEA as part of a future commercial product under RHEA unique branding but overall encompassing all PANOPTESEC features and augmented by supporting features including for example, incident work flow management.
Additional research and development work	(RHEA) Concept optimization and component rework will be pursued to improve the open architecture and component performance before re-integration into the wider RHEA branded product.
IPR measures	Protected under various copyright statements incorporated into PANOPTESEC related design documents and code, supported by relevant publications and presentations.
Commercial contacts	(RHEA) Commercial contacts have been identified with Leonardo, Raytheon, Lutech, Telecom Italia Mobile, MetaEnergia, the EDA and the Polish Military Communications, Institute.
Target groups	(RHEA) As part of a RHEA branded product or embedded technology in cyber security supply chain to Aerospace, Defence, Critical Infrastructure, Banking / Finance, Crisis Management and Response.

3.1.14 Visual Analytics Environment

Exploitable result	
Functionality	The Visual Analytic environment is able to connect to the PANOPTESEC System and visualize all relevant data from the proactive and reactive chains. It is also capable of interact with the PANOPTESEC System for configuration purposes or for the selection of the Response Plans proposed by the Strategic Response Decider or the Tactical Response

	Decider. It is composed by a set of configurable views.
Purpose	Visualization of PANOPTESEC System relevant data from a proactive and reactive perspective, in order to allow the Security Operator gain awareness of the cyber-security situation of the Monitored System.
Innovation	Leverages advanced and innovative concepts for visualization of large and complex data sets.
Partner(s) involved	UROME, RHEA, UzL
Role and activities	Research, Dissemination, Design, Development, Integration and Test
How the result will be exploited	(RHEA/UROME) The component capabilities will be used by RHEA as part of a future commercial product under RHEA unique branding but overall encompassing all PANOPTESEC features and augmented by supporting features including for example, incident work flow management.
Additional research and development work	(RHEA/UROME) Visual interface features will be augmented and extended to support, for example, security operations task management, workflow and authorization. Visual analytics engine will be packaged according to product under a RHEA branding approach.
IPR measures	Protected under various copyright statements incorporated into PANOPTESEC related design documents and code, supported by relevant publications and presentations.
Commercial contacts	(RHEA) Commercial contacts have been identified with Leonardo, Raytheon, Lutech, Telecom Italia Mobile, MetaEnergia, the EDA and the Polish Military Communications, Institute.
Target groups	(RHEA) As part of a RHEA branded product or embedded technology in cyber security supply chain to Aerospace, Defence, Critical Infrastructure, Banking / Finance, Crisis Management and Response.

3.1.15 Policy Deployer

Exploitable result	
Functionality	The PolicyDeployer is a component related to the Proactive and Reactive chains. The aim of the component is to deploy in the Monitored System, where possible, the MitigationActions enforced by the Strategic Response Decider (on the proactive chain) and the Tactical Response Decider (on the reactive chain). In case the Policy Deployer does not have access to

	the enforcement point, it will send an email/open a ticket to the network operators
Purpose	The aim of the component is to deploy in the Monitored System, where possible, the MitigationActions enforced by the Strategic Response Decider (on the proactive chain) and the Tactical Response Decider (on the reactive chain). In case the Policy Deployer does not have access to the enforcement point, it will send an email/open a ticket to the network operators
Innovation	The main innovation is related to the overall comprehensive perspective of the PANOPTESEC System, leveraging from detection and network reconstruction to actuation of the Mitigation Action
Partner(s) involved	RHEA, IMT, ALBLF
Role and activities	Research, Dissemination, Design, Development, Integration and Test
How the result will be exploited	(RHEA) The component capabilities will be used by RHEA as part of a future commercial product under RHEA unique branding but overall encompassing all PANOPTESEC features and augmented by supporting features including for example, incident work flow management.
Additional research and development work	(RHEA) Concept optimization and component rework will be pursued to improve the open architecture and component performance before re-integration into the wider RHEA branded product.
IPR measures	Protected under various copyright statements incorporated into PANOPTESEC related design documents and code, supported by relevant publications and presentations.
Commercial contacts	(RHEA) Commercial contacts have been identified with Leonardo, Raytheon, Lutech, Telecom Italia Mobile, MetaEnergia, the EDA and the Polish Military Communications, Institute.
Target groups	(RHEA) As part of a RHEA branded product or embedded technology in cyber security supply chain to Aerospace, Defence, Critical Infrastructure, Banking / Finance, Crisis Management and Response.

3.1.16 Fast Network Scanner (NetworkInventoryProcessorAgent)

Exploitable result	
Functionality	A recent development within the PANOPTESEC Project, NIPA is a Java based application which uses the Nmap scanner in order to collect and

	store on database topology information at high speed (due to its internal parallel computation). It can be deployed from small to large size networks, maintaining interesting speed results. NIPA can be deployed in multiple instances on different IPDomains, still centralizing the results on a common database.
Purpose	Rapidly scan an environment to accurately populate a network topology within a specified domain or set of domains.
Innovation	Nmap is a widely used topology scanner. Java APIS using Nmap, however, often suffers in areas of performance and flexibility of the results. NIPA aim is to improve the actual offer with a reliable and flexible scanner adaptable to networks different in size and topology.
Partner(s) involved	RHEA
Role and activities	Research, Design, Development, Integration and Test
How the result will be exploited	(RHA) An Open-Source version of the scanner is envisioned, and it can be used with the NetworkInventoryProcessor in order to reconstruct network topologies and keep them up-to-date. This approach is very feasible for security and network assessments. The component capabilities will be used by RHEA as part of a future commercial product under RHEA unique branding but overall encompassing all PANOPTESEC features and augmented by supporting features including for example, incident work flow management.
Additional research and development work	(RHEA) NIPA will be refined after the end of the PANOPTESEC Project, in order to improve performances and configurability
IPR measures	Protected under various copyright statements incorporated into PANOPTESEC related design documents and code, supported by relevant publications and presentations.
Commercial contacts	(RHEA) Commercial contacts have been identified with Leonardo, Raytheon, Lutech, Telecom Italia Mobile, MetaEnergia, the EDA and the Polish Military Communications, Institute.
Target groups	(RHEA) As part of a RHEA branded product or embedded technology in cyber security supply chain to Aerospace, Defence, Critical Infrastructure, Banking / Finance, Crisis Management and Response.

3.1.17 ACEA Emulation Environment

Exploitable result	The PANOPTESEC Emulation Environment provides a complex environment suitable as a supporting infrastructure for cyber security experimentation, research and development, test and training in a protected manner.
Functionality	The PANOPTESEC Emulation Environment includes a combination of real and virtual assets collected to emulate a complex energy distribution network including control systems, front-end gateways, remote terminal units, redundant network connectivity and supporting information anc communications technology (ICT) infrastructures, along with various network and security sensors and services. The environment also provides functionality for advanced cyber attack simulation in support of experimentation, research and development, test and training.
Purpose	Supported PANOPTESEC development, test and validation activities.
Innovation	Leverages state-of-the-art cloud technologies into a collection of advanced cyber simulation capabilities.
Partner(s) involved	RHEA, ACEA
Role and activities	Research, Dissemination, Design, Development, Integration and Test
How the result will be exploited	(ACEA) ACEA will continue to use the emulation environment in support of ongoing research, experimentation, test and development of improved cyber security systems and operations procedure improvements both within ACEA and in support of the critical infrastructure community. The environment will also be investigated for use in operator training scenarios. (RHEA) RHEA has already leveraged the experience and concepts into the European Space Agency Cyber Range project. This will be further extended as part of a more complete cyber integration test and engineering framework (CITEF) to be delivered under a wider funding programme of ESA and supported by the Belgium Science Policy Organization (BelSPO), with the eventual intent to provide a environment for independent security testing of space assets.
Additional research and development work	(RHEA) The concepts developed under the PANOPTESEC project have already undergone additional refinement as part of the ESA Cyber Range project. This includes development of an operator interface for configuration and management of cyber and domain specific assets. The concepts have undergone preliminary branding as the RHEA CyberSim.
IPR measures	Protected under various copyright statements incorporated into

	PANOPTESEC related design documents and code, supported by relevant publications and presentations.
Commercial contacts	(RHEA) Commercial contacts have been identified with Leonardo, Raytheon, Lutech, Telecom Italia Mobile, MetaEnergia, the EDA and the Polish Military Communications, Institute.
Target groups	(RHEA / ACEA) Utilities operators, system integrators, national cyber authorities, other critical infrastructure operators and suppliers. (RHEA) As part of a RHEA branded product or embedded technology in cyber security supply chain to Aerospace, Defence, Critical Infrastructure, Banking / Finance, Crisis Management and Response.

3.2 Packaged outputs

As part of branding and packaging, several options for incremental delivery of features have been identified. These are grouped into version for Business Risk Management and Security Incident Management. From a branding perspective, it is proposed that the PANOPTESEC project name will be shortened to the more manageable "PSEC", while the Peacock Feature Logo will remain the same. The packaged versions provide an incremental approach to market uptake with added benefit of increasing customer engagement across increasing scale of deployment. These versions also provide a means to control the complexity of initial installation and configuration based on business need. The packaged options are outlined below:

3.2.1 PSEC for Business Risk Management (BRM)

The PSEC-BRM version is proposed to consist of the following editions:

1. Standard Edition: Including productised versions of the Network Inventory Processor (NIP), Vulnerability Inventory Processor (VIP) and Mission Impact Module (MIM). This version supports essential capabilities for asset inventory, understanding of asset vulnerabilities with critical assessment of business, mission or service impacts due to those vulnerabilities with interdependency analysis;
2. Advanced Edition: Packaged as PSEC-BRM Standard Edition plus Reachability Matrix Correlator (RMC) and Attack Graph Generator-Threat Risk Quantifier (AGG-TRQ). Provide more advanced information to the security manager supporting deeper understanding of the business risks and impacts.
3. Enterprise Edition: Packaged as the PSEC-BRM Advanced Edition plus Strategic Response Decider (SRD) and Tactical Response Decider (TRD). Use of SRD and TRD also imply embedded use of the Low Level Correlator (LLC) and High-Level Online Correlators (HoCs). This version provides essential decision support capabilities to the operator, enabling identification of pre-approved authorized mitigation actions.

4. Enterprise Response Edition: Packaged as the PSEC-BRM Enterprise Edition with additional support for response management via the Policy Deployer. This version will support an incremental roadmap based on level of operator intervention in response selection and activation as required by the customer organization.

The BRM version has particular market potential because good solutions that combine network topology, vulnerability topology and business topology are not present in the market today. Current market products have a high probability to provide many false "risks assessment" because they do not consider the security topology, defence perimeter and system interdependencies. This packaging will help the security manager answer critical security questions like, "Does my infrastructure have a good level of defensive capability?"; "Can my infrastructure limit the number and types of risks to my business?"; and "What risks are not covered by my security systems and what are the resulting impacts?". The target market should be the Security Manager in support of his responsibility to provide information related to the evaluation of security risks and impact to top management.

3.2.2 Security Incident Management (SIM)

The PSEC-SIM version is proposed to consist of the following editions:

1. Standard Edition: Including productised versions of the NIP, VIP, LLC, RMC, AGG-TRQ and HOCs. This version supports essential capabilities for security incident management with a new and innovative point of view resulting from the AGG and localization of attacks on the graph using the LLC and HOCs;
2. Enterprise Edition: Packaged as the PSEC-SIM Standard Edition plus Strategic Response Decider (SRD) and Tactical Response Decider (TRD). This version provides essential decision support capabilities to the operator, enabling identification of pre-approved authorized mitigation actions.
3. Enterprise Response Edition: Packaged as the PSEC-SIM Enterprise Edition with additional support for response management via the Policy Deployer. This version will support an incremental roadmap based on level of operator intervention in response selection and activation as required by the customer organization.

The PSEC-SIM packaging has intentional focus to support incident analysis, decision support and response management. The overall market for incident detection and prevention systems (IDS/IPS) is high, but competition is also strong. Essential differentiators related to attack path analysis along an attack path provide key insights to the security operator.

3.2.3 Packing roadmaps compared to market delivery

It should be obvious that the packaging of the PSEC-SIM Enterprise Edition and Enterprise Response Edition match also the PSEC-BRM versions of the same name. This is intentional as it limits the technical complexity of different market packages leveraging the same technical solution. The market differentiation is important since it allows different market entry points based on perceived customer 'pain points' (e.g., business risk or incident management). As the competitive market is further analysed, the project may come to the conclusion that the Enterprise and Enterprise Response Editions should be marketed as a

converged flow from PSEC-BRM and PSEC-SIM, resulting in a view as shown in the figure below:

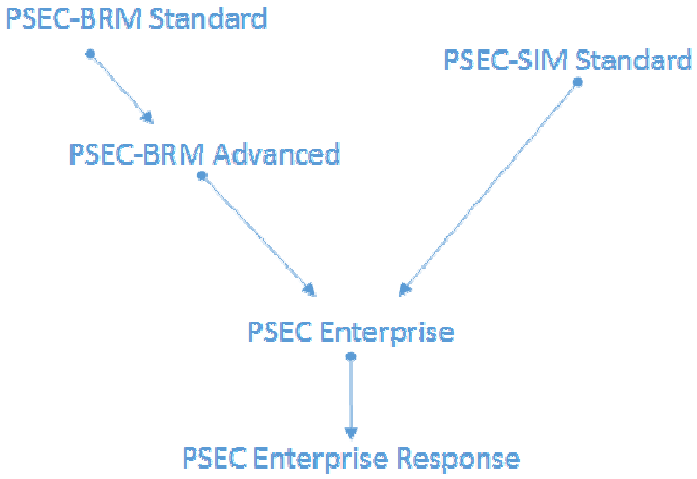

Figure 1: PANOPTESEC (PSEC) marketing packages

3.3 Competitive Market Assessment

The PANOPTESEC packaged outputs described above, place the PANOPTESEC project within two related cyber security product segments, (1) Information Technology Risk Management (ITRM) and (2) Security Information and Event Management (SIEM). To be adequately positioned in these markets, a competitive market assessment is performed against leading products in these segments. As a general approach, the project has completed a comparison of the PANOPTESEC packaged outputs according to the Gartner Magic Quadrant (MQ) surveys of the ITRM and SIEM markets. The Gartner MQ results specific to ITRM and SIEM markets provide concise descriptions of relevant capabilities of market relevant products for comparison. The approach taken in each of the sections below is to compare the PANOPTESEC capabilities to the capability descriptions of each of the products identified in the above mentioned Gartner reports, combined with a comprehensive review of available product data from the identified companies.

For reference, the identified capabilities for each category (ITRM and SIEM), as well as current market capabilities of product vendors, are taken from the following sources:

- Gartner Magic Quadrant for IT Risk Management Solutions, ID: G00276514, Published: 19 May 2016, Analysts: K. Pratap, J. Wheatman; and
- Gartner Magic Quadrant for Security Information and Event Management, ID: G00290113, Published: 10 August 2016, Analysts: M. Cavanagh, O. Rochford, T. Bussa.

3.3.1 Information Technology Risk Management

Figure 2 provides the May 2016 outcomes of the Gartner MQ for ITRM products, identifying the 11 companies for comparison of feature capabilities with PANOPTESEC.

Figure 2: Gartner MQ for ITRM (May 2016)

Table 3 provides a comparison of ITRM feature capabilities across companies and including PANOPTESEC feature capabilities. Vendors for comparison are identified by the following reference IDs:

1. PANOPTESEC;
2. Allgress;
3. Brinqa;
4. ControlCase;
5. EMC (RSA);
6. IBM;
7. LockPath;
8. MetricStream;
9. Modulo;
10. RiskVision;
11. Rsam; and
12. SeviceNow

Table 3: PANOPTESEC comparison to Gartner MQ identified ITRM capabilities and companies

Capability Feature	1	2	3	4	5	6	7	8	9	10	11	12
Policy Management												
Policy authoring, change management and version control	P	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Development and approval workflow	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Mapping policy statement into technology, business and regulatory risk requirements	P	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Control Mapping and Reporting												
Out-of-the-box content for compliance reporting (e.g., ITIL, COBIT, ISO27001, etc)	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Mapping controls to requirements	P	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Security Operations Analysis and Reporting												
Standard connectors to import vulnerability scan data, security configuration data, SIEM data, etc.	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y
Configurable connectors to import other types of data	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y
Support vulnerability remediation workflow	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y
IT Risk Assessment												
IT risk assessment workflow	P	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Survey functions to support data gathering	P	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Risk acceptance process	P	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
IT risk register	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
IT asset management	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Manual control testing workflow/support	N	N	N	Y	N	N	N	P	N	N	Y	N
IT risk metrics and reporting	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Incident Management												
Incident management/loss event capture and analysis	Y	Y	N	Y	Y	Y	P	Y	Y	Y	Y	Y
Support for interdepartmental collaboration	N	Y	N	Y	Y	Y	P	P	Y	Y	Y	Y
Incident management workflow	P	Y	N	Y	Y	Y	P	Y	Y	Y	Y	Y
Incident trend analysis	Y	Y	N	Y	Y	Y	P	Y	Y	Y	Y	Y
Colour coding												
Feature substantially present	Y											
Feature partially present	P											
Feature not present or not apparent	N											

As can be seen from Table 3, the collection of vendors identified by the Gartner MQ ITRM report, provide a comprehensive set of capabilities in-line with current market expectations for feature capabilities to varying degrees. As may be expected, some products demonstrate capabilities clearly matching the ITRM expected scope, while others are less capable. Similarly, as a newly developed prototype, there are features from the ITRM scope that are lacking in PANOPTESEC. However, it appears that the baseline set of features are at least comparable to the general capabilities of the ITRM market scope.

What is not immediately clear by the Gartner MQ report is the ability of these vendor solutions to meet additional features developed under the PANOPTESEC project offering an improved feature set applicable to the ITRM feature scope. Comparison of the same vendor solutions against PANOPTESEC innovative features is provided in Table 4. As can be seen, with the exception of business oriented risk assessment, very few of the top vendors provide the innovative features developed by the PANOPTESEC project. This indicates that PANOPTESEC has strong ability to meet current market needs, while also providing additional feature capabilities. Concerning business oriented risk assessment, it is not surprising that products in the scope of ITRM will have some capabilities for business oriented risk assessment, due to their orientation to support business oriented governance, risk and compliance. However, from the analysis, it does not appear that any of the products are able to support complex interdependency analysis provided by the PANOPTESEC solution.

Table 4: PANOPTESEC feature comparison to Gartner MQ identified ITRM companies

Capability Feature	1	2	3	4	5	6	7	8	9	10	11	12
Attack path generation and analysis	Y	N	N	N	N	N	N	N	N	N	N	N
Mission or business oriented impact or risk assessment	Y	P	P	P	P	P	P	P	P	P	P	P
Automated decision support for vulnerability and incident management	Y	N	N	N	N	N	N	N	N	N	N	N
Automated policy deployment for security risk mitigation	Y	N	N	N	N	N	N	N	N	N	N	N

3.3.2 Security Information and Event Management

Figure 3 provides the May 2016 outcomes of the Gartner MQ for SIEM products, identifying the 14 companies for comparison of feature capabilities with PANOPTESEC.

Figure 3: Gartner MQ for SIEM (August 2016)

Table 5 provides a comparison of SIEM feature capabilities across companies and including PANOPTESEC feature capabilities. Vendors for comparison are identified by the following reference IDs:

1. PANOPTESEC;
2. AlienVault;
3. BlackStratus;
4. EMC (RSA);
5. EventTracker;
6. Fortinet (AccelOps);
7. HPE;
8. IBM;
9. Intel Security;
10. LogRythm;
11. ManageEngine;
12. Micro Focus;
13. SolarWinds;
14. Splunk;
15. Trustwave.

Table 5: PANOPTESEC comparison to Gartner MQ identified SIEM capabilities and companies

Capability Feature	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Collection of event data															
Collect and aggregate event data from multiple sources including log data, netflow data, etc.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	P	Y	Y	Y
Combine event data with context about users, assets, threats and vulnerabilities	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	P	Y	Y	Y
Normalization of data from disparate sources for correlation	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Real-time correlation of events for security monitoring	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Analysis of event data															
Analyze event data in real time for early detection of attacks and data breaches	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Collect, store, investigate and report on log data for incident response, forensics and regulatory compliance	P	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Query and analytics for historical analysis	P	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Colour coding															
Feature substantially present	Y														
Feature partially present	P														
Feature not present or not apparent	N														

As can be seen from Table 5, the collection of vendors identified by the Gartner MQ SEIM report, provide a comprehensive set of capabilities in-line with current market expectations for feature capabilities. Overall, it appears that products within the SEIM market have a comprehensive set of capabilities matching SIEM the market scope.

However, what is not immediately clear by the Gartner MQ report is the ability of these vendor solutions to meet additional features developed under the PANOPTESEC project offering an improved feature set. Comparison of the same vendor solutions against PANOPTESEC innovative features is provided in Table 6. As can be seen, very few of the top vendors provide the innovative features developed by the PANOPTESEC project. This indicates that PANOPTESEC has strong ability to meet current market needs, while also providing additional feature capabilities.

Table 6: PANOPTESEC feature comparison to Gartner MQ identified SIEM companies

Capability Feature	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Attack path generation and analysis	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Mission or business oriented impact or risk assessment	Y	N	N	Y	N	N	N	Y	N	N	N	P	N	N	N
Automated decision support for vulnerability and incident management	Y	N	N	N	N	N	N	N	N	Y	N	P	P	N	N
Automated policy deployment for security risk mitigation	Y	N	N	N	N	N	N	N	N	Y	N	P	P	N	N

4 EXPLOITATION STRATEGY

4.1 Indicative exploitation plans

The PANOPTESEC consortium exploitation plan represents the collective intent of the PANOPTESEC consortium to pursue the results of the project to the maximum extent possible.

To succeed its main goal, the PANOPTESEC project provided a prototype, which implies that the exploitation possibilities are significant. This system will be first used by ACEA, one of the largest Italian public utility companies for power and water supply.

The consortium as a whole and each partner separately has already identified and foresee various ways that the results can be further exploited by the project completion and beyond (please see section 5.3 below). Depending on each partner's profile and business objectives, the exploitation of the results may vary from educational transfer and know-how improvement to developing new technologies, products and services. Active research in the areas of visual analytics, cyber defence / cyber security, data analysis will be leveraged for teaching and further research activities as well as real-world applications and commercial service packaging. It is also envisioned that the PANOPTESEC project results will have implications in various security related standards activities as well as security related policy developments.

4.2 Intellectual property rights principles

PANOPTESEC intends to produce knowledge that can be turned into significant commercial value. The Steering Committee will encourage project partners to protect the knowledge generated and to promote it in standardisation, publications, workshops and conferences. Intellectual Property Rights (IPR) application for new concepts and solutions will be regulated by the concerned participants through the PANOPTESEC consortium agreement, which defines the rules for the ownership and access rights of knowledge.

The PANOPTESEC Project has an established and agreed consortium agreement setting out the rules and requirements for intellectual property ownership, access, confidentiality and responsibilities for protection.

These are the focus areas where involved partners are particularly encouraged and expected to develop and protect intellectual property, including:

- Improved network and security multi-sensor data integration and correlation using a mathematical framework and mixed-initiative problem solving based on Semantic Web technologies;
- Automation of attack awareness and risk assessment via attack modelling taking into account the evolution of systems and services, the emergence of new threat sources and newly discovered system vulnerabilities, and the operational mission priorities;
- Automation of attack awareness and risk assessment via risk quantification through data collection, threat assessment and risk modelling;

- Automation of attack awareness and risk assessment via decomposition of risk quantification into separate proactive and reactive assessment chains;
- Automation of response assistance to provide cyber defence operators with prioritized courses of action recommendations for review and activation;
- Advanced mechanisms to capture and model mission/business process relationships to services and systems based on Semantic Web technologies; and
- Advanced visualization techniques for mission/business process risk display including representation

Within the D&E activities, eventual intellectual property rights applications will be supported, ensuring each partner's claims.

5 PANOPTESEC EXPLOITATION FOR COMMERCIAL PARTNERS

The PANOPTESEC consortium includes three partners which are commercial companies.

5.1 PANOPTESEC Exploitation by RHEA

5.1.1 Partner profile and background

Since 1992, RHEA has been providing space engineering services and products to the international space community including the European Space Agency (ESA) and EUMETSAT. RHEA is the proud supplier of the Mission Operations Information System (MOIS) technology, used in support of over 100 space missions and also a leading provider of concurrent design and engineering systems and services with its flagship product, Concurrent Design Platform™. With headquarters in the Brussels area of Belgium, RHEA is an international organisation with an established presence in Belgium, the Netherlands, Italy, Germany, Spain, Switzerland, the UK, the Czech Republic and Canada.

Since 2004, RHEA has been broadening its service offerings by taking a strategic approach to the delivery of system and software engineering solutions dedicated to the aerospace, defence and security domains with a particular emphasis on space systems engineering, cyber security, critical infrastructure protection and information technology solutions. Part of this strategy has been the creation of the RHEA Security and Crisis Management (SCM) business unit, providing information security services to agency-level organisations throughout Europe. It is the mission of the RHEA security practice to deliver innovative solutions to meet security applications, systems and operations requirements. Most recently, in December 2014, RHEA acquired majority shareholding interest in SixSq, a European leader in Cloud Computing technologies and services.

5.1.2 Exploitation results and strategy

5.1.2.1 Exploitation Results

As a SME industrial partner within the PANOPTESEC consortium, RHEA has already achieved some successful exploitation of PANOPTESEC results and will continue to pursue commercial opportunities for delivery of PANOPTESEC as a productised solution for cyber defence.

Leveraging corporate capabilities and experience developed within the PANOPTESEC project, RHEA has successfully proposed and been awarded a contract with the European Space Agency (ESA) to deliver a “Cyber Security Training Range” at ESA Station in Redu Belgium. The value of the contract is € 480 K and has a mandate to deliver a virtualized technical environment supporting a variety of cyber security related training, research, development and test activities in a relevant space assets simulation context. The project will also deliver a Long Term Perspective, with recommendations for ongoing use of the facility beyond the current project. This provides additional potential for expanding business at RHEA. RHEA experience in delivering the PANOPTESEC emulation environment not only improved corporate capabilities in this area but was also a substantial factor in the successful evaluation of the RHEA proposal as a reference project.

Following the success of the Operational Demonstration Workshops at ACEA in October 2016, RHEA has been approached by several companies interested to have deeper understanding of PANOPTESEC technologies for future exploitation. At this stage it is too early to determine the full scope of the opportunities, however each represents potential for product related sales, embedded product licensing, or technology support services. In this context, commercial interest has been expressed by:

- Leonardo (http://www.leonardocompany.com/en);
- Raytheon (http://www.raytheoncyber.com/);
- Lutech (http://www.lutech.it/?lang=en/);
- Telecom Italia Mobile (https://www.tim.it/); and
- MetaEnergia (http://www.metaenergia.it/).

Even following the official end of the project, RHEA continues to actively support PANOPTESEC demonstrations in collaboration with ACEA, hosed at ACEA premises.

5.1.2.2 Product Packaging and Branding

Following the success of the ESA Cyber Range, RHEA will continue to pursue opportunities in the various core markets, incrementally developing productized versions of the PANOPTESEC solution according to the modular and packaged outputs described in Section 3.2.

As part of project closure activities, RHEA is further refining the packaging approach and developing a branding strategy. Additional market assessments specific to key regional priorities of RHEA are underway with particular focus in Belgium and Italy. In support of this, RHEA has recently hired a new General Manager for RHEA in Italy and augmented the business development team with additional resources in Belgium. In both cases, these additional business development resources have a particular focus towards development of exploitation opportunities for PANOPTESEC outcomes.

The RHEA Group security product branding strategy is intended to capture several core concepts of the PANOPTESEC, while providing a unique brand characteristic of the RHEA Group.

5.1.2.3 Target markets and approach

RHEA will focus exploitation efforts towards the following markets:

1. Space Systems Security: Space systems are more and more recognised as critical infrastructures. These environments have similar requirements for security monitoring other critical infrastructure and national defence environments. RHEA has several initiatives already underway that leverage PANOPTESEC results in the domain of Space Systems Security.

a. European Security Certification Standards for space assets: In response to the ESA GOVSATCOM Precursor Activities, RHEA has submitted a Notice of Intent to submit an Outline Proposal. This proposal presents a recommendation to establish a European Space Security Certification Scheme (ESSCS) and independent security evaluation facility. An independent and mandatory ESSCS would encourage use of ESSCS certified products within the EU, establishing an industrial mandate and market for EU solutions, while improving security of space assets through requirements for 'security-by-design' concepts. This activity should be done in light of the activities of the Cyber Security Coordination Group (CSCG), collectively formed by CEN, CENELEC and ETSI. The CSCG has published a White Paper "Recommendations for a Strategy on European Cyber Security Standardisation" demonstrating there is a need for such standardization. However, the CSCG body is largely concerned with traditional Information and Communications Technologies (ICT) related topics and the White Paper does not address unique challenges of space technologies or systems. In the outline proposal RHEA has recommended use of the above mentioned ESA Cyber Range project as the independent ESSCS evaluation facility. Such a facility will require an expanded space assets cyber emulation environment including a Cyber Integration Test and Evaluation Framework (CITEF). The PANOPTESEC Integration Framework will form the basis of the CITEF;

b. Space Systems and Solutions: ESA are developing a common approach to ground system solution and delivery called the European Ground Station Common Core (EGS-CC). RHEA has been actively involved in the EGS-CC prototyping efforts and is the Belgium Prime for involvement in EGS-CC testing framework. Although operating in different industrial domains, the EGS-CC and the PANOPTESEC Integration Framework share common technologies and approach. This is an intentional step by RHEA to leverage common results between the two projects. The previously mentioned CITEF based on PANOPTESEC will further enhance RHEA capabilities to deliver integration and testing solutions for space systems; and

2. Critical Infrastructure Protection: A primary customer opportunity for PANOPTESEC, RHEA is promoting the concepts to potential public and private utilities companies (energy, water, oil & gas, etc.). Recent media coverage demonstrates growing concern over the issues of cyber-attacks to critical infrastructure[3]. RHEA has intentionally established a Critical Infrastructure Protection Business Strategy targeting this market on a regional basis where infrastructure providers are being approached and presented with PANOPTESEC as packaged solutions. Engagements start with use of PANOPTESEC for Business Risk Management (see Section 3.2), then

[3] Matgen, Le Bussy, Braun, Lambrecht, and Lovens, http://www.lalibre.be/actu/belgique/attentats-d-ici-5-ans-ils-pourraient-prendre-le-controle-d-une-centrale-nucleaire-56f58f4d35708ea2d3e8e878, La Libre.BE, 26/03/2016, last accessed 04/04/2016.

proceed towards expanded offering for Security Incident Management. Regional focus will leverage RHEA office placement in Belgium, Germany, Italy, The Netherlands and the United Kingdom. Specific opportunities within this market include participation in the proposed Multi-sector National Testbed for Critical Infrastructures[4] as part of The Hague Security Delta in The Netherlands. It is intended that RHEA capabilities for delivering a critical infrastructure emulation environment similar to PANOPTESEC emulation environment will be leveraged into the National Testbed. RHEA is also participating in a proposal to the European Space Agency as part of the Integrated Applications Programme (IAP) in which the PANOPTESEC system will be used to secure a crisis management and response infrastructure for industrial accidents according to SEVESO[5] regulations;

3. Cloud Provider Security: RHEA has recently acquired majority interest in SixSq, an innovative provider of technology and solutions for automated provisioning of cloud services. PANOPTESEC is considered a valued added solution for cloud provider environments, offering a large scale capability for continuous security monitoring. Increased capabilities for continuous security monitoring in cloud environments may improve market opportunities for Small-Medium Enterprise (SME) that may otherwise be reluctant to take advantage of cloud provider services. SixSq are actively involved in projects related to security of industrial control systems, critical infrastructure, and secure cloud delivery (H2020 projects: SCISSOR, CYCLONE and PaaSword). The combined technology opportunities of these projects towards increasing cloud provider security and supporting their SME clients is a significant market for RHEA;
4. National Defence Organisations: Due to the evolution of the cyber threat, national defence organisations must pursue advanced solutions to counter the threat. Some already identified business opportunities include the Cyber Situation Awareness Package (CySAP) within the European Defence Agency (EDA) and the Cyber Defence Situational Awareness (CDSA) work package within the NATO Multi-national Cyber Defence Capability Development (MNCD2) project. Leveraging the PANOPTESEC experience, RHEA submitted a proposal on 4 November 2016, to the EDA CySAP project, in collaboration with partner UROME. If successful, the project will involve definition of the System Requirements and Target Architecture of the future CySAP project.

5.1.3 Risks and mitigation strategy

The main risk envisioned for RHEA exploitation of PANOPTESEC is that the technical achievements of the project are too complex or comprehensive for market acceptance of the complete solution. This risk is mitigated by the packaging options identified in Section

[4] The Hague Security Delta, "Securing Critical Infrastructures in the Netherlands: Towards a National Testbed," https://www.thehaguesecuritydelta.com/images/HSD_rapport_Testbed_EN.pdf, 2015, last accessed 04/04/2016.
[5] http://ec.europa.eu/environment/seveso/

3.2. These packaged outputs provide the opportunity to deliver specific components in an incremental way, supporting a staged roadmap of delivery.

Also, as a systems integrator, RHEA is focused on delivery of a robust integration framework as part of the PANOPTESEC solution. This framework is built on a strong system engineering approach supporting commercial release. The modular nature of the framework supports further component refinement or integration of alternate commercial modules according to market demand. This approach provides a solid basis for successful commercial release.

5.1.4 Implementation strategy

The implementation of our exploitation strategy includes the following:

1. Market driven materials: In support of business development activities, RHEA will prepare PANOPTESEC based marketing materials including white papers and case studies under a new product brand. This will prepare customers for interest in the resulting packaged solution and component parts. A combined RHEA-SixSq eGuide "Smart City Cyber Protection for Critical Infrastructures" has already been produced to highlight the use of the SixSq Nuvlabox in the PANOPTESEC project as a cyber security sensor host platform in remote critical infrastructure facilities (e.g. electricity distribution substations);
2. Technology demonstration events: RHEA actively participates in industry conferences and demonstrations in relevant market segments. Trade exhibits within the industry conferences will provide significant opportunity to showcase PANOPTESEC results;
3. Expansion of existing client contracts: As noted above, existing clients (e.g., ESA, EDA and NATO) have significant requirements for cyber defence continuous monitoring solutions. RHEA has already begun promoting PANOPTESEC concepts to existing clients in order to generate interest and new business opportunities and has seen early successes. Although not specifically a cyber security related project, RHEA is leveraging common aspects of the integration framework between the PANOPTESEC and EGS-CC projects; and
4. Active bidding on upcoming opportunities: The ESA Cyber Range project demonstrates early success for RHEA in this area. As noted above, upcoming opportunities fit the PANOPTESEC scope and concepts (e.g., ESA GOVSATCOM and EDA CySAP). RHEA is well positioned to propose a PANOPTESEC-based solution as the winning approach to meet these and similar requirements. RHEA has submitted an Outline Proposal to the ESA GOVSATCOM Precursor Activities on 06/05/2016. RHEA has also submitted a proposal for improving cyber security of space assets as part of the ESA ARTES 5.2 programme and is currently preparing a proposal as part of a consortium towards the ESA IAP for security of infrastructures supporting crisis management.

5.2 PANOPTESEC Exploitation by Alcatel-Lucent (ALBFL)

Due to the ongoing merger between Alcatel-Lucent and Nokia, market exploitation by ALBFL is dependent on overall corporate strategy decisions that are, as yet not fully resolved and a

formal approach is not feasible at this time. The company remains committed to take advantage of the project outcomes through various exploitation channels.

5.3 PANOPTESEC Exploitation by Epistematica Srl

5.3.1 Spin-off

Having regard to the Treaty establishing the European Community, and in particular Article 165 thereof, where it speaks:

(1) When re-launching the Lisbon Strategy in 2005, the Heads of State or Government stressed the key role that better links between public research organisations, including universities, and industry can play in facilitating the circulation and use of ideas in a dynamic knowledge society and in enhancing competitiveness and welfare.

(2) An effort should be made to better convert knowledge into socio-economic benefits. Therefore, public research organisations need to disseminate and to more effectively exploit publicly-funded research results with a view to translating them into new products and services. Means to realise this include in particular academia-industry collaborations – collaborative or contract research conducted or funded jointly with the private sector –, licensing and the creation of spin-offs.

And having regard to the European Commission recommendation on the management of intellectual property in knowledge transfer activities, and Code of Practice for universities and other public research organisations, in order to:

(a) promote the use of publicly-funded research results and maximise their socio-economic impact, consider all types of possible exploitation mechanisms (such as licensing or spin-off creation) and all possible exploitation partners (such as spin-offs or existing companies, other public research organisations, investors, or innovation support services or agencies), and select the most appropriate ones.

(b) develop and publicise a licensing policy, in order to harmonise practices within the public research organisation and ensure fairness in all deals. In particular, transfers of ownership of intellectual property owned by the public research organisation and the granting of exclusive licences should be carefully assessed, especially with respect to non-European third parties. Licences for exploitation purposes should involve adequate compensation, financial or otherwise.

(c) develop and publicise a policy for the creation of spin-offs, allowing and encouraging the public research organisation's staff to engage in the creation of spin-offs where appropriate, and clarifying long-term relations between spin-offs and the public research organisation.

(d) establish clear principles regarding the sharing of financial returns from knowledge transfer revenues between the public research organisation, the department and the inventors.

In accordance with the Panoptesec project Consortium Agreement - PPCA, IPR and access rights chapter, Epistematica decided to create a new company to exploit its own results of the publicly-funded research.

It will be an European simplified company based on the Italian regulatory. The share of the company will be open to the authors, contributors (eg. Tech evangelists) and stakeholders, as well as to the partners of the Panoptesec consortium.

5.3.2 Reason for New Company

Software solutions like RMC, designed and developed by Epistematica to compute reachability matrix with a semantic approach, are not yet in the market.

Epistematica is specialized in research, design and development of solutions based on semantic technologies. It is not a cyber-security or software firm. To take advantage from the research it was decided to create a new company together with domain experts.

The business model of the new company will be digital, fully inside the digital economy paradigm.

5.3.3 General information

5.3.3.1 Name

Renodes

5.3.3.2 Director

Giovanni Rizzello

5.3.3.3 Business

Online sale of proprietary software

5.3.3.4 Product

Renodes – a software solution to automate the discovering of the network logical topology (derived by Panoptesec RMC module)

5.3.3.5 Market

Worldwide

5.3.3.6 Target

All users of the best COTS solutions of the network inventory management

5.3.3.7 Beneficiaries

Not cyber-security specialists for physical and logical network topology visualization and testing; pentesting professionals to make faster ISO/OSI layer 5-6-7 assessment activities

5.3.3.8 Other assets

Epistematica will also confer to the new company another publicly-funded research results from ESA – European Space Agency, coming from RARE project – http://wiki.services.eoportal.org/tiki-index.php?page=RARE+Project. The outcome of the RARE project is a software environment developed in Java for visualization of ontologies and browsing of metadata. In the Renodes suite, it will be used to browse the nodes' properties and to navigate the network's physical and logical topology.

5.3.3.9 Startup strategy

To realize the startup the following steps will be required:

- Analyzing the legal aspects of intellectual property, company constitution and registration (in progress)
- Creating a business plan (in progress)
- Creating a marketing plan (in progress)
- Creating tools and instruments for business activities: web site; e-commerce service for paying download; CRM-based service for technical assistance to the customers; social marketing service for lead generation strategy; insurance and banking services for digital business needs; etc. (in progress)
- Creating the first downloadable products based on open-source technologies with a connector to one of the most important network inventory management software (in progress)
- Fundraising (es. venture capital) for triggering the second business step to implement a new class of products (in progress)
- Developing new products based on property technologies and new connectors (programmed)
- Expanding business on large scale (programmed)

5.3.3.10 Communication plan

To support the startup main strategy, it will be necessary to perform some communication activities below summarised:

- Registering the domain: renodes.net (done)
- Creating a Twitter account of renodes: @LogicalTopology (done)
- Performing a digital marketing campaign for generating buzzing around renodes.eu (in progress)
- Creating a Website: www.renodes.net (in progress)
- Launching the startup in international events (ongoing)

5.3.3.11 Future exploitation activities

RMC module is a “proof of concept” for other applications in different domains.

Epistematica wants to explore new application domains in order to create applications based on the RMC's methodology and technology.

Using strong semantics to represent knowledge and automated reasoning to infer, the applications like RMC are more autonomous than applications based on syntactic technologies. It could better support fully automated business processes, which are business processes of the digital age.

6 PANOPTESEC EXPLOITATION FOR END-USER PARTNERS

The PANOPTESEC consortium includes one partner which represents the end-users of PANOPTESEC-like solutions.

6.1 PANOPTESEC Exploitation by Acea

6.1.1 Partner profile and background

Among the most important Italian public utilities, Acea is an industrial Group which focuses on the consolidation and creation of value from its two main activities, energy and water. Stock market listed since 1999, it deals with the management of energy, environmental and water services: the production, sale and distribution of energy, the development of renewable sources, the disposal and creation of energy from waste, the public and artistic lighting, and an integrated water service (aqueducts, sewerage and purification). Acea has always taken seriously its corporate social responsibility, and pays particular attention to all stakeholders, profitability, service quality and sustainable development. Being a prominent Critical Infrastructure utility, both for water and electricity, the Acea Group has a strong focus on Cyber Security and actively participates in working groups, projects and public events.

6.1.2 Exploitation results and strategy

Acea Group intends to use the PANOPTESEC system to actively monitor and protect its SCADA Command & Control centres and ICT environments to defend them from Advanced Cyber Threats: being the only User Agency of the PANOPTESEC project, Acea Group will use its test bed to validate the results of the system and then move it to the production environment.

Moreover areti (former Acea Distribuzione) confirmed in the budget resource allocation for the year 2017 the extension of the IT and SCADA protection systems to the main electricity distribution sites, closely followed by the integration with the PANOPTESEC system (value: 60K euro investment for 2017, plus ordinary maintenance/licence renewal costs).

6.1.3 Risks and mitigation strategy

The main risks envisioned for Acea exploitation of the PANOPTESEC are related to the interactions with the existing systems and operators, the responsiveness of the system and the quality of the results obtained from it: as an example, if the rate of false positives will be too high (i.e. over the expected results), the cost in terms of time and resources needed to properly analyze, categorize and solve them could not be tolerable and we could be forced to revert to other solutions. To mitigate these risks, Acea team closely monitored the results and performances regularly during the development, avoiding or solving conflicting situations in advance. To avoid any unwanted interaction, a dedicated room is available in ACEA Headquarters to showcase the system functions in a simulated but real protected environment, without introducing any risk in the functional operational context.

6.1.4 Implementation strategy

The implementation strategy includes:

1. After internal validation, testing the PANOPTESEC system in our real-world contexts (i.e. areti, former Acea Distribuzione);
2. Giving access to our partners and other selected parties to our premises for the demonstration of the PANOPTESEC system;
    a. Qualification Review with internal stake holders (within Acea Group) and EAB on 22-23 September and 5 October 2016;
    b. **Operational workshop** Acea HQ 17-28 October 2016 (for details see D.2.3) with more than 90 external qualified stakeholders belonging to sectors/industries such as defence, transport, telecommunication, bank, financial, television, IT/ICT, utility;
    c. Organisation and/or participation to national/international events related to Critical Infrastructure Cyber Protection:
        i. Participation by A. Guarino (ACEA) to the a demonstration workshop of the EU FP7 project "ECOSSIAN" (http://www.ecossian.eu) for the protection of critical infrastructures (Rome, 8 November 2016)
        ii. Round Table with a short presentation by Stefano Liotta (areti) and Andrea Guarino (ACEA) at the "3ª Conferenza nazionale Cyber Security Energia" event organised by EnergiaMedia (Rome, 25 October 2016)
        iii. Presentation by A. Guarino (ACEA) at "Outthink threats" event organised by IBM (Rome, July 2016)
        iv. Presentation by A. Guarino (ACEA) and M. Merialdo (RHEA) at "European Mobility & Endpoint Security User Group" meeting organised by IBM (Rome, 27 May 2016)
        v. Presentation by A. Guarino (ACEA) at "CPX 2016 – Check point Experience" event (Nice, 19 April 2016)
        vi. Presentation by F. Bosco (ACEA) to the EUREAU Commission EU3 (Berlin, 11 February 2016)
        vii. Presentation by A. Guarino (ACEA) at "Cyber Security Energia 2015" event organised by EnergiaMedia (Rome, 24 September 2015)
        viii. Participation in the experts panel of A. Guarino (ACEA) in the "CyberSec 2014" event, organised by Intel Security (Rome, 15 October 2014)
        ix. Presentation by A. Guarino (ACEA) at "First National Conference on Cyber Security for the Energy Sector, 2014", organised by EnergiaMedia and World Energy Council (WEC) (Rome, 3 July 2014)

x. Participation by A. Guarino (ACEA) in the "Security Summit 2014", event organised by AIIC-Clusit (Rome, 18-19 June 2014)

xi. Presentation by A. Guarino (ACEA) at the "IFIP WG 10.4 - 65th Meeting" (Sorrento, 24 January 2014)

xii. Participation by A. Guarino (ACEA) in "Final meeting of the Cyber Group", organised by "Osservatorio Nazionale per la Sicurezza" (OSN) (Rome, 13 December 2013)

xiii. Participation by A. Guarino (ACEA) in the "Workshop in preparation of the First National Conference on Cyber Security for the Energy Sector", organised by EnergyMedia and World Energy Council (WEC) (Rome, 11 December 2013)

3. In addition to the aforementioned events, ACEA will be present and participate to the following forthcoming seminars and workshops for light dissemination and networking:
    a. Red Hat Open Source Day (Rome, 15 November 2016) (https://www.redhat.com/it/about/events/red-hat-open-source-day-2016)
    b. Intel CyberSec 2016 (Rome, 16 November 2016) (https://emea.demand.intelsecurity.com/Intel-Security-Cybersec-2016)
    c. FORTINET Security Day (Rome, 17 November 2016) (https://www.emea-events.com/securityday2016_roma)
    d. European Electronic Crime Task Force (EECTF): "Advanced Persistent Threats: real cases" (Rome, 22 November 2016) (http://www.posteitaliane.it/en/innovation/cyber_security/index.shtml)
4. Actively promoting the PANOPTESEC Project in the context of other FP7 and/or H2020 consortiums and proposals to extend its results to the other connected domains. Acea promoted the PANOPTESEC and disseminated its results and findings to the following EU Projects:
    a. FP7 Security Project ECOSSIAN "European COntrol System Security Incident Analysis Network" (www.ecossian.eu) through the Consortium partner Poste Italiane SpA;
    b. H2020 Project SUCCESS "securing critical energy infrastructures (www.success-energy.eu/) through the Consortium partner ASM Terni SpA;
    c. FP7 C2-SENSE "Interoperability Profiles for Command/Control System and Sensor Systems in Emergency Management" (www.c2-sense.eu) through the Consortium partner Lutech SpA.
5. Dissemination and informal presentation to selected stakeholders:
    a. Utilitalia Commission on Telecommunication informal presentation by F.Bosco (ACEA) (Bologna, 20 October 2016);

b. Presentation by A. Guarino (ACEA) and M. Merialdo (RHEA) to 4RF Limited of the PANOPTESEC System solution (Rome, 27 July 2016);

c. Presentation by A. Guarino (ACEA) and M. Merialdo (RHEA) to General Electric Industrial Communication of the PANOPTESEC System solution (Rome, 26 May 2016).

7 PANOPTESEC EXPLOITATION FOR ACADEMIC PARTNERS

7.1 PANOPTESEC Exploitation by Institut Mines-Telecom

7.1.1 Partner profile and background

This Institut Mines-Télécom is a group of prestigious French engineering schools operating under the aegis of the French Ministry of Industry. It is focusing on the domains of Energy and Information and Telecommunication Technologies, and their applications (e-health, smart cities, green society, cyber-security, etc.). The Institute has 3 main missions:

- Higher education: the institute trains about 13000 students in its 15 schools, including around 9000 engineers (M level) and 1800 PhDs.
- Research and innovation: the Institute leads a strong research activity, with about 1700 ranked publications per year, 450 PhD defences and around 50 patents granted each year.
- Economic development: The institute contributes to about 100 start-ups founded by students or teaching staff, of which 85% are 3 years old or more

Institute Mines-Télécom is thus an active contributor to many of the French “poles de compétitivité” and “Instituts de Recherche Technologique” (IRT) that create networking opportunities and support for business creation and development.

7.1.2 Exploitation results and strategy

As an academic publication, IMT will of course participate in the dissemination of scientific knowledge through publications in conferences and journals, in the information security domain. Our policy is to publish few but solid papers, which can leverage interest in the security community.

Within the framework of PANOPTESEC, IMT is leading and developing an activity related to cyber-attack mitigation. This activity has matured up to the point that IMT has obtained recently a patent on the topic. We will continue to enhance our research to the point where we should be able to ask for more patents on the same topic, as well as be able to demonstrate our technology on use case scenarios to our industry partners. IMT actively seeks to transfer patents to industry, in order to foster development and commercial exploitation.

7.1.3 Risks and mitigation strategy

The main risk envisioned is that we are not successful in acquiring first, and transferring second, the patents that we wish to seek. This may lead to the decision to push some of these patents and the associated software into the public domain, if the cost of maintaining them becomes prohibitive for the Institute.

7.1.4 Implementation strategy

The implementation of our exploitation strategy will be twofold:

- Technology fairs: every year, IMT participates to or organises several technology fairs, either with small businesses or major partners. During these fairs, technologies are presented to interested industry partners in private meetings, and technology transfers are planned.
- "Challenge projet d'entreprendre": every year in March, the school (Télécom SudParis) organises for its students an entrepreneurship challenge, where teams of students analyze a technology, the market, and create business plans. Proposals compete and the prize winners often develop their startup based on the challenge results. Our strategy is to propose this activity to a group of students interested in the domain of ICT security.

7.1.5 Papers and publications

A detailed list of all papers and publications is contained in the companion document, Dissemination Report [D8.1.3].

7.2 PANOPTESEC Exploitation by Universität zu Lübeck (UzL)

7.2.1 Partner profile and background

In 1973, the Universität zu Lübeck (UzL) became an independent scientific institution in the German state of Schleswig-Holstein. UzL offers degree programs in medicine, computer science, engineering, and natural sciences. Interdisciplinary programs encompassing natural sciences, computer science, and medicine offer practical and up-to-date education underpinned by the highest standard in healthcare research. Compared with other universities, the Universität zu Lübeck is small, with just 3,400 students -- but has a good teacher-student ratio. The high standings of our computer science and medicine students point out the high standard of our teaching and education. In addition, Universität zu Lübeck intensively support technology transfer activities to support existing companies as well as new spin-offs. The University functions virtually as an incubator for the emergence of business concepts. The numbers of such University spin-offs have increased considerably in past years and have contributed essentially to the creation of new, highly-qualified workplaces. For this reason, spin-offs are particularly supported by special programs of federal and state authorities. In this frame, the Federal Ministry for Economy and Technology's promotion program EXIST plays a decisive role.

7.2.2 Exploitation results and strategy

As university partner within the PANOPTESEC consortium, UzL exploits PANOPTESEC results for scientific developments and foundational entrepreneurial activities. Fundamental research on theory related to the MIM has been published on major conferences (see the detailed publication list below). Further, theory on data collection and correlation as well as mission impact assessment have been published, and demonstrations of application scenarios were given for participants in applied workshops as well as for industry partners and contacts (see below).

7.2.3 Risks and mitigation strategy

The main risk envisioned for UzL exploitation of PANOPTESEC is that the scientific results obtained are too specific, i.e., are too much tailored to the ACEA use case, and therefore do not transfer directly to other problem domains, such that PANOPTESEC gets wide acceptance in the academic domain. In the publications also other application areas have been investigated (see below for the full list) such that a wide application of PANOPTESEC results can be guaranteed.

7.2.4 Implementation strategy

The implementation of our exploitation strategy includes the following:

1. Publications: Scientific papers submitted to workshops, conferences and journals.
2. Technology demonstration events: UzL participates in industry conferences and demonstrations in relevant market segments, and shows demonstrators indicating the overall applicability and relevance of the problem solutions developed in research projects.

Further, the UzL has progressed towards direct exploitation using industry contacts and demonstrations. The following exploitation reports shows that, in fact, developed components are not tailored towards an ACEA use case, but remain generally applicable.

Presentation of PANOPTESEC Aims, Techniques, and Architecture at CYPP (cypp.de), Sachenstraße 5, Hamburg

March 16th 2016, 10.30-12.30 by Alexander Motzek and Ralf Möller

April 11th 2016, 10.30-12.30 by Mona Lange and Ralf Möller

CYPP is a small company and about to develop a data collection and security assessment software for medium-sized enterprises. They were very much interested in PANOPTESEC in general and the Data Collection and Correlation System in particular. This holds for all data inventories as well as for the low-level correlation system. Their main business model is to provide a security analysis overview tool, with GUI elements pretty much in the spirit of what PANOPTESEC provides as manager-level visualizations (for CYPP the destination platform would be Android or iOS, though). Detailed control room displays as also foreseen in PANOPTESEC are currently not in their focus because, according to CYPP's assessment, this is not what medium-sized enterprises demand, but visualizations were definitely interesting for them.

Business models (MIM) are interesting for CYPP but according to their assessment the perspective of manually providing models might be a show stopper for medium-sized companies. Thus they are very much interested in techniques for automatically collecting models from data, as pursued by UzL. More efforts should be devoted to these issues. Possibly, business functions (tasks) can be kept but, maybe, business processes should be dropped in a CYPP-specific MIM approach. Nevertheless, an additional score for ranking response plans was considered to be interesting. Note that response plans can also be

provided manually using a GUI, and still, ranking principles apply for discussing pros and cons of manually provided alternatives.

CYPP would be very much interested in further contacts. They see the possibility of exploiting PANOPTESEC technology in projects with their customers, with a clear need to adapt the system to customer and context-specific needs. Since PANOPTESEC, according to our claims, would be available in December, CYPP also is interested in referring to PANOPTESEC techniques in project acquisition meetings while they are about develop dedicated software for their market niche.

Several action points were discussed during the meeting. On the one hand, demos would be much appreciated. On the other hand, IPR issues need to be discussed in order to allow CYPP to further consider exploitation of PANOPTESEC results (be it DCC modules or even attack, risk, or response models).

Another action point was to organize a follow-up discussion with the company PLATH GmbH (plath.de) after Easter (personal contacts allow for additional exploitation possibilities for PANOPTESEC). Plath provides sensor equipment, in particular for surveillance applications. Plath members might also be interested in computer forensics and have contacts to LEAs.

7.2.5 Papers and publications

A detailed list of all papers and publications is contained in the companion document, Dissemination Report [D8.1.3].

7.3 PANOPTESEC Exploitation by Centrale Supélec

7.3.1 Partner profile and background

CentraleSupélec is a prestigious French engineering school operating under the aegis of the French Ministry of Education and the French Ministry of Industry and ranked as one of the top in its fields. It is currently organized in a four campuses network located in Châtenay-Malabry, Gif-sur-Yvette, Rennes and Metz. It is focusing on complex systems engineering in the domains of energy, electronics, mechanics, aeronautics, space and information systems. 1000 engineering students (Master of Engineering level) graduate each year. CentraleSupélec also has a strong research activity with 300 research professors and 500 Ph.D. students. It is a member of the Pôle d'Excellence Cyber that regroups renowned French industries and academic partners working in cyber-defense.

7.3.2 Exploitation results and strategy

As an academic partner, CentraleSupélec will participate in the dissemination of scientific knowledge through publications in conferences and journals, in the information security domain. Our policy is to publish solid papers in international conferences and to participate to technical conferences, workshops and technology fairs, which can leverage interest in the security community.

Within the framework of PANOPTESEC, CentraleSupélec is participating in the activities of data collection, intrusion detection and visualization. The first objective of CentraleSupélec is first to integrate its expertise in these three domains in a complete integrated solution.

Then, thanks to experiences performed with this solution on real cases, it will be possible to identify the theoretical limits and practical issues and to improve each component as well as their integration. The second objective of CentraleSupélec is then to be able to provide software components that can be profitably easily integrated to numerous security systems.

7.3.3 Risks and mitigation strategy

The main risks envisioned for CentraleSupélec exploitation of PANOPTESEC is that the scientific and technical achievements of the project do not meet objectives to experiment and validate the resulting solution on a sufficiently significant use case to demonstrate the relevance of the components and of their integration. The mitigation strategy for CentraleSupélec is to use accurate, precise and as standard as possible interfaces to its components to be able to interact with existing technologies. If no standard is available, the data model used in the components should allow easy transformation of the existing data formats.

7.3.4 Implementation strategy

The implementation of our exploitation strategy will be made of three parts:

- Participation in international conferences and workshops to leverage interest of the security community.
- Presentation of the PANOPTESEC project and of its results to the partners of the French Pôle d'Excellence Cyber.
- Participation to technology fairs: every year, CentraleSupélec and INRIA participate to several technology fairs. For instance, CentraleSupélec and INRIA were very active this year in FIC (Forum International de la Cybersécurite) in Lille where it presented results in visualization for cyber-security.

7.3.5 Papers and publications

A detailed list of all papers and publications is contained in the companion document, Dissemination Report [D8.1.3].

7.4 PANOPTESEC Exploitation by UROME

7.4.1 Partner profile and background

UROME unit is made by two main subgroups: distributed and dependable systems group and information visualization group. Both the sub-groups are internationally recognized by their respective communities and have several collaborations with national companies (e.g., IBM, Microsoft) and public administrations and agencies (e.g. Italian national security agency, Minister of the Finance). Recently, most of our efforts have been devoted in the analysis and design of dependable architecture in the Context of Critical Infrastructure protection.

As part of a Research Centre attached to Sapienza University, we have two main missions:

- Higher education: people involved in the CIS are members of Sapienza University of Rome, the main and ancient University of the city that trains thousands of students each year.
- Research and innovation: the research centre has a strong and sustained research activity, witnessed by the high publication rate in high-level peer-reviewed international journals and conferences.

7.4.2 Exploitation results and strategy

From a strategical perspective, being an academic partner, the main exploitation activity of UROME will be devoted to the merger of PANOPTESEC results into its usual communication policy, through articles published in professional and technical press and scientific journals, communications and presentations at research and business conferences (including the IST conferences organized by the EC), trade shows and professional exhibitions.

Furthermore, the use of the results and their publication not only in Italy but also within countries of the European Union will be guaranteed by the institution's large network in the public and private sector.

UROME will exploit its results using its contact network built through several past projects with Public Administrations trough and its experience in developing applied research. This will be also favored by its geographic location (established in Rome, where the Italian Government institutions are also established, and the Italian National Centre for IT in the Public Administration). As a consequence, we expect a high impact of the dissemination of the project results towards the most interested users, especially among public administrations and big companies ready to invest in the cyber defense.

As potential publication venue, UROME is specifically interested in journals, conferences and workshops related to Database, Distributed Systems, Service-oriented Computing, Mobile Computing and Information Visualization.

Given the two assets (Visualization Environment and Query-based High-Level On-line correlation engine, namely QBE) that CIS-UROME established with PANOPTESEC, some exploitation activities have been already carried out and described in the following:

- We transferred basic concepts behind PANOPTESEC into specialized lectures offered to students attending specialized courses of the Master in Engineering in Computer Science offered by our School (e.g. course of Seminars in Distributed Systems and Information Visualization).
- We are setting up a research collaboration with the Academic Centre of Excellence in Cyber Security Research at Imperial College London (Prof. Emil C. Lupu and its group) to further develop and extend the functionalities of QBE.
- Following the successful experience with the spin-off Over Technologies (following from a previous FP7 project), we are investigating the feasibility of a new spin-off.

7.4.3 Risks and mitigation strategy

We do not envision particular risks in the fulfillment of our exploitation plan.

7.4.4 Implementation strategy

Due to our nature of Academic body, the implementation of our exploitation plan falls down in our normal institutional duties and common work.

7.4.5 Papers and publications

A detailed list of all papers and publications is contained in the companion document, Dissemination Report [D8.1.3].

8 CONCLUSIONS

The PANOPTESEC project has identified significant project exploitation opportunities. There are seventeen identified technology outputs (Section 3.1). Most of the components are highly innovative and when delivered as a collective system capability, the PANOPTESEC project achieved consistent high ratings by both external and internal participants to the project demonstration workshops. In summary, Table 7 identifies the set distribution of participation among identifiable outputs and contributions by project partners.

Table 7: Summary of partner exploitation outcomes

Partner	Participation in Project Outputs	Project Output
IMT	2	Strategic Response Decider, Policy Deployer
SUPELEC	2	High-level Online Correlator (both Query Based and Automaton Based)
UROME	6	Reachability Matrix Correlator (non-ontology), Low-level correlator, High-level Online Correlator (both Query Based and Automaton Based), Mission Impact Module, Visual Analytics Environment
UzL	6	Low-level Correlator, Network Dependency Analyzer, High-level Online Correlator (both Query Based and Automaton Based), Mission Impact Module, Visual Analytics Environment
ACEA	1*	All
RHEA	17**	All
ALBLF	3	Attack Graph Generator – Threat Risk Quantifier, Tactical Response Decider, Policy Deployer
EPIST	1	Reachability Matrix Correlator (ontology-based)

The project has conducted a comparison of key features and innovative product capabilities compared to commercial products. The outcome of this analysis demonstrates that the PANOPTESEC solution has a solid capability base among the competing ITRM and SIEM products, while also providing an innovative set of features relevant as improvements to these markets.

The project partners have developed a comprehensive set of exploitation plans, leveraging their respective roles as industrial, academic, research or user agency partners. To varying degrees partners have identified commercial opportunities, leveraging project outputs, including some that have already resulted in increased business revenue. The clear interest expressed by industry is evidence of the relevance and impact of the project.