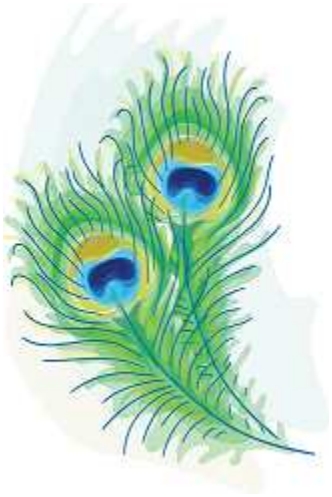

PANOPTESEC

FP7-610416

D5.1.1 – Response System for Dynamic Risk Management Requirements

Work-Package	WP5	Deliverable	D5.1.1
Due Date	27-03-2015	Submission Date	27-03-2015
Main Author(s)	ALBLF		
Contributors	CIS-UROME, IMT, SUPELEC, UoL (formerly TUHH), RHEA		
Version	V2.1	Status	Final
Dissemination Level	PU	Nature	R
Keywords	Risk quantification, likelihood, impact, return on response on investment, attack path, online scenario correlation, policy instantiation.		

Part of the Seventh

Framework Programme

Funded by the EC - DG Connect

EXECUTIVE SUMMARY

In this deliverable, the PANOPTESEC project presents a preliminary Functional Architecture of a *Response System* for the *Dynamic Risk Management* (i.e. *Dynamic Risk Management Response System*), with ambition to go beyond the current state-of-the-art on Dynamic Risk Management systems proposed as scientific or industrial prototypes. Then, the *Specialized Requirements* of this Dynamic Risk Management Response System are established and detailed.

The proposed Dynamic Risk Management Response System will be one of the central-pieces of the Security Management System (i.e. PANOPTESEC system) researched and developed by the PANOPTESEC consortium.

Specialized Requirements for this Dynamic Risk Management Response System which have been established following elicitation and validation processes are specified as a refinement or complement to the Operational Requirements of the PANOPTESEC system (i.e. the Requirements Baseline) described in the deliverable [D2.2.1]. Both Functional and Non-Functional Specialized Requirements are proposed.

Traceability coverage matrices of these Specialized Requirements over the Operational Requirements are given on the Functional and Non-Functional perspectives. This enables verification that the envisaged Dynamic Risk Management Response System within Work Package 5 (WP5) is theoretically and functionally consistent with the project needs related to the *Response System*.

The provided Traceability coverage matrices should help tracking, guiding and evaluating the outcomes of WP5 through the remainder of the PANOPTESEC project.

HISTORY

Version	Date	Name/Partner	Comment
v0.1	01-12-2013	ALBLF	Creation of the document: Proposal of a first Table of Content.
v0.2	26-03-2014	ALBLF	Proposal of an initial high-level functional block diagram representation for section 3. An introductory description of this diagram. And, identification of contributions on functional blocks' description for section 3 awaited from WP5 Partners.
v0.3	19-05-2014	ALBLF, IMT, CIS-UROME	CIS-UROME & IMT & ALUBL: Add the description of the different functional blocks of the high-level functional diagram in section 3. ALUBL: Change of the PANOPTESEC document template. CIS-UROME: Provide a template and first set of functional requirement for the section 4.
v0.4	30-05-2014	IMT	Additional detailed provided on the description of the RORI in section 3. First set of requirements provided in section 4 for the Impact Assessment, Strategic Response Decision, Security Policy Instantiation, and Policy Deployment functions.
v0.5	18-06-2014	ALBLF, CIS-UROME	ALBLF: Additional description of the "(Success) Likelihood" functional block in section3. Slight revision of description of the "Risk Quantification" and "Tactical Response Decision" functional block in section 3. Provision of 17 Functional Requirements for the "Attack Graph Generation" functional block in section 4. Add of a template for coverage matrices of Functional Requirements regarding Operation Requirements in section 5. CIS-UROME: Provision of 11 Functional Requirements for the "High Level Online Correlation" functional block in section 4.
v0.6	30-06-2014	ALBLF, CIS-UROME, IMT, SUPELEC	ALBLF: Additional set of Functional Requirements provided for the "(Success) Likelihood Assessment" block. Initial set of Functional Requirements provided for the "Risk Quantification" block. Modification of a description of the "(Success) Likelihood" functional block in section 3. Slight modification of "Tactical Response Decision" block in section 3. IMT: Several minor corrections and provision of Functional Requirements in section 4 (for the "Impact Assessment" and "Strategic Response Decision" blocks). SUPELEC: Several additional and rewriting of "Attack Graph Generation" and "High Level Online Alert Correlation blocks' Functional Requirements.
v0.7	18-07-2014	ALBLF, TUHH, CIS-UROME, IMT, SUPELEC	ALBLF: Additional set of Functional Requirements provided for the "Threat Impact Assessment" block. Additional set and updates of the set of Functional Requirements provided for the "Risk Quantification" block. Revision of the "Impact Assessment" functional block in section 3. Slight modification in "Attack

			Graph Generation", "Tactical Response Decision" and "Risk Quantification" blocks in section 3. Coverage of AGG, RQU, SLA, TIA, and TRD functional requirements over the operational requirements in section 5. Additional References provides for section 7. Provision of "Background on Dynamic Risk Management" for sub-section 2.2. TUHH: Additional description of "Response Operational Impact Assessment" in the "Impact Assessment" functional block of section 3. Provision with a set of Functional Requirements for the "Response Operational Impact Assessment" in section 4. IMT: Rewriting of the "Strategic Response Decision" blocks for section 3. Several modification and provision of Functional Requirements in section 4 (for the "Impact Assessment" and "Strategic Response Decision" blocks). SUPELEC: Provision of a new "Potential Attack Identification" functional block description for section 3. Several additional and rewriting of "High Level Online Alert Correlation" blocks in section 3. Functional Requirements provided for the new PAI function in section 4. Coverage of the HOC and PAI Functional Requirements over the Operational Requirements for section 5. CIS-UROME: Provision of new and rewriting of Functional Requirements for the "High Level Online Correlation" and the "Potential Attack Identification" blocks in section 4.
v1.0	31-07-2014	PANOPTESEC Consortium	RHEA: Many corrections, rewording, comments, and remarks provided on v0.7. SUPELEC: Several corrections, rewording and comment provided on v0.7. Additional references provided for HOC and PAI descriptions in section 2. Additional coverage of GEN functional requirements provided for section 4. CIS-UROME: Several corrections following RHEA's corrections, rewordings, comments and remarks provided on v0.7. Additional coverage of GEN functional requirement provided for section 4. TUHH: Several corrections following RHEA's corrections, rewordings, comments and remarks provided on v0.7. Additional coverage of ROI functional requirement provided for section 4. IMT: Several answers provided following RHEA's corrections, rewording, comments, and remarks. Additional coverage of RFI, SRD, and SPI functional requirements provided for section 4. ALBLF: Several corrections provided following RHEA's corrections, rewording, comments, and remarks. Final integration of last corrections provided by other Partners. Assessment of the global coverage of WP5 functional requirements over the operational requirements following the provision of last coverage of GEN, ROI, RFI, SRD, SPI. Enhancement of the

			conclusion and Executive Summary.
v1.1	20-02-2015	IMT, ALBLF	IMT: Revision of the Specialised Requirements on the domains RFI, SRD and SPI according to the comments (mainly the first comment) provided on D5.1.1 v1.0 in the 11 December 2014 Review report. ALBLF: Revision of the Specialized Requirements on the domains AGG, RQU, SLA, TIA and TRD according to the comments (mainly the first comment) provided on D5.1.1 v1.0 in the 11 December 2014 Review report. The Requirements were also updated according to a comment on the D4.1.1 for harmonisation purpose (i.e. comment requesting the change of "Main Scenario" in "Main Purpose"). Requirements were also crossed-checked with the new list of Operational Requirements provided for the revised version of the D2.2.1 (provided on Thursday 19 February 2015 on the project SVN server) to verify they are still appropriate. An preliminary methodology Section 2 describing "MUST", "SHOULD" and MAY" terminology is also provided.
v1.2	28-02-2015	UROME, SUPELEC, IMT, UoL ALBLF	UROME: Revision of the Specialized Requirements on the functional domain GEN, and provision of additional Non-Functional Specialized Requirements according to the D2.2.1 Functional Operational Requirements revision and Non-Functional Operational Requirements addition after the comment provided on D2.2.1 v1.0 in the 11 December 2014 Review report. Revision of the Functional Specialized Requirements on the domain HOC according to the comments (mainly the first comment) provided on D5.1.1 v1.0 in the 11 December 2014 Review report. The Requirements were also updated according to a comment on the D4.1.1 for harmonisation purpose (i.e. comment requesting the change of "Main Scenario" in "Main Purpose"). Additional Non-Functional Specialised Requirements were also provided for the functional domain HOC to address the comments (comment #6) provided on D5.1.1 v1.0 in the 11 December 2014 Review report. SUPELEC: Modification proposals of Specialized Requirements for functional domain HOC, and provision of additional Non-Functional Specialised Requirements according to the D2.2.1 Functional Operational Requirements revision and Non-Functional Operational Requirements addition after the comment provided on D2.2.1 v1.0 in the 11 December 2014 Review report. Revision of the Functional Specialized Requirements on the domain PIA according to a comment on the D4.1.1 for harmonisation purpose (i.e. comment requesting the change of "Main Scenario" in "Main Purpose"). Additional Non-Functional Specialised Requirements provided for the functional domain PIA according to the comments (comment #6) provided on D5.1.1 v1.0 in the 11 December 2014 Review report. IMT: Revision of the Specialised Requirements on the domains RFI, SRD and SPI according to comments provided by ALBLF, comments (mainly the first comment) provided on D5.1.1 v1.0 in the 11 December 2014 Review report

			and according to a comment on the D4.1.1 for harmonisation purpose (i.e. comment requesting the change of "Main Scenario" in "Main Purpose"). UoL: Provided additional Non-Functional Specialized Requirements for the domain ROI according to address the comments (comment #6) provided on D5.1.1 v1.0 in the 11 December 2014 Review report. ALBLF: Provision of an enhanced methodology section 2, with stakeholders identification, requirements elicitation analysis, and validation processes. Some additional Non-Functional Specialized Requirements provided for the AGG, RQU, SLA, TIA and TRD functional domains to address the comments provided on D5.1.1 v1.0 in the 11 December 2014 Review report. Additional comment provided on ROI domain Specialized Requirements.
v1.3	09-03-2015	SUPELEC, UROME, ALBLF	SUPELEC & UROME: Common revision of the wording of Functional requirements for the HOC domain to better address the Reviewers comments. Additional Non-Functional requirements were also reworded in common agreement between the SUPELEC and UROME teams. ALBLF: Revision of the Section 5 addressing the coverage of the Specialised Requirements over the Operational Requirements. The tables in Section 5.1 and 5.2 are modified with the new stable set of Functional Operational Requirements dealing with WP5 (i.e. RRS and PRS requirements) provided for the revised D2.2.1 on the 2 March 2015 and validated on 4 March 2015. A new subsection is added to capture: (i) the coverage of Non-Functional Specialized Requirements over the Non-Functional Operational Requirements; and, (ii) the applicability assessment of Non-Functional Operational Requirements to each identified WP5 functional domains.
v1.4	14-03-2015	UoL, UROME IMT, ALBLF	UoL: Additional revisions of the Functional Specialized Requirements for the ROI domain provided to answer the comments (comment #1) provided on D5.1.1 v1.0 in the 11 December 2014 Review report. Some rewording and comments provided in other section of the deliverable. Revision of the coverage of the ROI Specialized Requirements over the new Function and Non-Functional Operational Requirements. Provision of the applicability of the Non-Functional Operational Requirements over the ROI functional domain. UROME: More revision of Specialized Requirements for the HOC and PAI domains provided to address the comments (comment #4 part on "uncertainty") provided on D5.1.1 v1.0 in the 11 December 2014 Review report. Some rewording and comments provided in other section of the deliverable. Reassessment of the coverage of the HOC and PAI Specialized Requirements over the new Function and Non-Functional Operational Requirements. Provision of the applicability of the Non-Functional Operational Requirements over the HOC and PAI functional domains. IMT: A rewording of the introductory section 3.3 to detail and explain more the dichotomy between

			proactive/strategic and reactive/tactical in the Response Assistance stage of the preliminary functional architecture of the DRMRS to address Reviewers comments #4. Additional revision of the Functional Specialized Requirements for the RFI, SRD and SPI domains provided to answer the comments (comment #1) provided on D5.1.1 v1.0 in the 11 December 2014 Review report. ALBLF: Revision of Introduction Section 1 to comply to the PANOPTESEC document template provided by the TMP in January 2015. Enhancement of the Section 2 on Methodology, and addition of the QA criteria and validation process sub-sections. Slight rewording of some Specialized Requirements of the GEN and ROI domains. Revision of the coverage of the AGG, RQU, SLA, TIA and TRD Specialized Requirements over the new Function and Non-Functional Operational Requirements. Add version numbers to all Specialized Requirements to support the requirement management and traceability within the Project. Add new purpose explanations and insights to the introductory part of Section 5.3. Provision the applicability of the Non-Functional Operational Requirements over the AGG, RQU, SLA, TIA and TRD functional domains. Revise the Reference section.
v1.5	21-03-2015	RHEA, EPIST, SUPELEC, UoL, IMT, ALBLF	RHEA & EPIST: Many comments, rewording proposals throughout the document provided after the WPL Review of the QA validation process which occurred between 16/03 and 18/03/2015. SUPELEC: Updates to the coverage matrices for the GEN and PAI requirements in Section 5.1 and 5.2. Provision of the coverage of Non-Functional Specialized Requirement coverage over Non-Functional Operational Requirements for Section 5.3.1. Provision of the applicability of the Non-Functional Operational Requirements to the PAI functional document in Section 5.3.2. Slight modification of the HOC text is also provided in Section 3.1.2. UoL: Rewording of the ROIA Specialized Requirements after the comments provided during the WPL Review. Some rewording in Section 3.2.3 for consistency with the rewording of SRs. IMT: Additional Non-Functional Specialized Requirements provided for RFI, SPI and SRD domains. Rewording provided for Functional SRs of domains RFI, SPI and SRD after the WPL Review. Provision of the coverage of Non-Functional SRs over Non-Functional ORs. Provision of the applicability of the Non-Functional ORs to the RFI, SPI and SRD domains. ALBLF: Rewording of the SRs for the functional domains AGG, RQU, LA, TIA and TRD after the WPL Review comments. Some comments and rewording proposals of the WPL Review addressed in section 2 and Section 5.
v1.6	24-03-2015	UROME, SUPELEC, UoL, ALBLF	UROME: Rewording of the some HOC requirements after the comments provided by RHEA during the WPL Review of the SA validation process. Slight additional modification

			to the HOC functional domain description in the preliminary Functional Architecture (Section 3.1.2). SUPELEC: Provision of the applicability of the Non-Functional Operational Requirement over the PAI functional domain. UoL: Proofread and comments provided on Specialized Requirements for functional domains RQU, LA, and TIA. ALBLF: Stakeholder, actors and user roles slight rewording to comply with D2.2.1 formulation. Figure 1 changed to comply with latest Section 3 rewordings. Rewording of some Specialized requirements of the functional domain AGG, RQU, LA, and TIA to remove the dependency of them on the "ICT system" wording. Slight rewording of parts of Section 3 and Section 5 after comments from RHEA provided during the WPL Review of the QA validation process. Rewording of the Executive Summary, the Conclusion. Additional references provided. Styles changes for D5.1.1 to conform to the Project deliverable template.
v1.7	25-03-2015	RHEA, ALBLF	RHEA: provision of the DRMRS Specialized Requirements tables extracted from the SysML PANOPTESEC design project used for traceability in the Project, which are based on the v1.6 Specialized Requirements provided by WP5 Partners. ALBLF: Integration of the Specialized Requirements tables extracted from the SysML PANOPTESEC design project used for traceability in the Project in the Section 4. Finale edition of the deliverable for QA validation process final phase.
v2.0	27-03-2015	ALBLF	Production of the v2.0 for the submission to European Commission of the revised D5.1.1 as requested in the Review Report of the 11 December 2014 Review #1.
v2.1	27-03-2015	RHEA, ALBLF	RHEA: Some minor additional formatting and grammar comments provided by the QAM during the last QA validation process phase. ALBLF: Some modifications following QAM review comments.

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

ACRONYMS AND DEFINITIONS

Table 1 - Acronym List and Definitions

Acronym	Meaning
ACEA	ACEA S.p.A.
ALBLF	Alcatel-Lucent Bell Labs France
AP	Applicable
CIS-UROME	Universita Degli Studi Di Roma La Sapienza
DRMRS	Dynamic Risk Management Response System
EPIST	Epistematica SRL
ICS	Industrial Control System
ICT	Information and Communication Technology
IMT	Institut Mines-Telecom
NA	Not Applicable
OR	Operational Requirements
PRS	Proactive Response System
QA	Quality Assurance
QAM	Quality Assurance Manager
RHEA	RHEA System S.A.
RRS	Reactive Response System
SR	Specialized Requirements
SUPELEC	Ecole Supérieure D'Électricité
SVN	Subversion repository
UoL	Universität zu Lübeck
WP	Work Package

1. INTRODUCTION

1.1 Context

This deliverable establishes and details the *Functional Requirements* of the *Response System for the Dynamic Risk Management* at the centre of the global Security Management System researched and developed by the PANOPTESEC consortium.

1.2 Purpose

The Purposes of the D5.1.1 deliverable are twofold.

First, to propose a preliminary functional architecture of a *Dynamic Risk Management Response System* (DRMRS) which, as ambitioned by the PANOPTESEC Consortium, goes beyond the current state-of-the-art on Dynamic Risk Management systems proposed as scientific or industrial prototypes.

Then, to establish *Specialized Requirements* of this *Dynamic Risk Management Response System* as a refinement of the Operational Requirements of the global PANOPTESEC Security Management System described in the deliverables [D2.2.1].

1.3 Scope

The deliverable describes the status of the proposed preliminary functional architecture of a *Dynamic Risk Management Response System,* and the detailed list of the *Specialized Requirements* established for it within the PANOPTESEC Consortium, at the time of the issuing of the final version of the D5.1.1 deliverable as scheduled in the Project Description of Work [DoW2013].

The coverage provided by these Specialized Requirements of the Response System regarding the Operation Requirements of the global PANOPTESEC System, and the applicability of Non-Functional Operational Requirements not otherwise established for the DRMRS in the D5.1.1 are identified.

Further management of the evolution of the DRMRS Specialized Requirements, their coverage and traceability during the next phases of design, implementation and experimentations are out of the scope of this deliverable and should be managed within the PANOPTESEC Project using the appropriate system engineering tools and formats established within the project.

***Note*:** Details of the PANOPTESEC Consortium approach and the mapping of the WP5 (WP5) sub-system (i.e. the DRMRS) in the global architecture of the PANOPTESEC system can be found in the Project Description of Work [DoW2013] and the PANOPTESEC system preliminary architecture described in the [D3.1.1] deliverable. Whereas, further details and background on the *Dynamic Risk Management* approach are available in the [D2.1.1] Deficiency Analysis deliverable.

1.4 Document Structure

This document is structured in the following manner:

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

Section 2 *Methodology*: describes the methodology followed by the authors of the D5.1.1 deliverable to establish the preliminary functional architecture of the DRMRS and the list of its Specialized Requirements. .

Section 3 *Dynamic Risk Management Response System generic description*: details the preliminary functional architecture of the DRMRS and establish the various functional domains for the Specialized Requirements.

Section 4 *Specialized Requirements*: details the Specialized Requirements established for the Dynamic Risk Management Response System.

Section 5 *Coverage of Specialized Requirements*: provides the coverage matrices of the Specialized Requirements defined in the D5.1.1 over the Operational Requirement defined in the D2.2.1. It provides also the applicability matrix of the Non-Functional Operational Requirements over the functional domains identified in the preliminary functional architecture of the DRMRS.

Section 6 *Conclusion*: provides the proper conclusions of the D5.1.1 deliverable.

Section 7 *References*: provides a list of references applicable to the D5.1.1 deliverable.

2. METHODOLOGY

The methodology for requirements analysis (RA) follows the established RA procedure for the PANOPTESEC project. The RA procedure is contained in the PANOPTESEC Project Handbook [PH15].

In accordance with the PANOPTESEC Project Handbook, the requirements formulated in this document use several capitalized words with a definite meaning in terms of specification. The words “MUST”, “SHOULD” and “MAY” have the following meanings as described in the [RFC 2119]. Their meanings, extracted from the [RFC2119], are also recalled here after:

- MUST: this word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- MUST NOT: this phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
- SHOULD: this word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- SHOULD NOT: this phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
- MAY: this word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides).

2.1 Stakeholders identification

A group of stakeholders are involved in the frame of the WP5 and D5.1.1, the Dynamic Risk Management Response System and the PANOPTESEC Project. The [D2.2.1] identifies extensively stakeholders’ categories, together with actors that apply in the context of the global PANOPTESEC Project. Several profiles and user roles, which are recalled after, are identified for these stakeholders and apply in the context of the D5.1.1. Some specific actors, which apply more specifically to the DRMRS, are also specified.

WP5 and D5.1.1 stakeholders

- *Solution Provider*: a Partner of the PANOPTESEC Consortium that proposes scientific or technical solutions for which he is skilled and recognized in his community, to fulfill one or several of the objectives of the sub-system (e.g. Dynamic Risk Management Response System) researched, designed and developed in the purview of the Work Package. Within the WP5, UoL, CIS-UROME, SUPELEC, IMT and ALBLF are identified as Solution Providers.
- *User Partner*: a Partner of the PANOPTESEC Consortium which provide to other Partners the operational context and requirements (e.g. use cases, scenarios, experiment dataset and test bed) and control the appropriateness of the solution proposed by Solution Providers to this

operational context and requirements. Within the WP5, ACEA is also involved as the User Partner (i.e. User Partner of the PANOPTESEC Project).

- *Work Package Leader*: a Partner of the PANOPTESEC Consortium that coordinate the work between the other Partners involved within a Work Package, validate the produced results according to the technical objectives of the Work Package as described in the [DoW2013] to ensure technical high quality, and enforce the schedule according to the [DoW2013]. Within the WP5, ALBLF assumes the Work Package Leader role.
- *Deliverable Editor*: a Partner of the PANOPTESEC Consortium that organizes and coordinate the writing of a deliverable between the other Partners within a Work Package, validate the contributions to ensure the technical high quality of the deliverable, and enforce the schedule to respect the due date of the deliverable according to the [DoW2013]. For the D5.1.1, ALBLF assumes the Editor role.

PANOPTESEC Project stakeholders

- *Technical Project Manager*: a Partner of the PANOPTESEC Consortium that manages the technical work between the other Partners involved in the various Work Packages, propose processes that ensure the smooth running of the technical progress, validate the produced results according to the global objectives of the Project as described in the [DoW2013] to ensure technical high quality and consistency, and enforce the technical processes and the technical schedule of the project according to the [DoW2013]. RHEA assumes the Technical Project Manager role.
- *Project Coordinator*: a Partner of the PANOPTESEC Consortium that Coordinate all the aspect of the work between the other Partners involved in the Project, propose processes that ensure the smooth running of the Project within the Consortium and outside the Consortium, validate the produced results according to the global objectives of the Project as described in the [DoW2013] to ensure high quality, consistency and pertinence, and enforce the processes and the schedule of the project according to the [DoW2013]. IMT assumes the Project Coordinator role.

Dynamic Risk Management Response System stakeholders

- *Monitored System Administrator:* A person who, for an organization, is responsible for the inventory, deployment or/and configuration management of hardware and software systems that compose the monitored system(s) on a day to day basis, with the focus to keep the monitored system(s) running and fulfilling their missions. In the context of the D5.1.1, are identifies more specifically two sub-roles.
    - *Network Administrator*: A person who, for an organization, is responsible for the inventory, deployment and configuration management of hardware and software systems that compose the monitored system(s) on a day to day basis, with the focus to keep the monitored system(s) up and running.
    - *Security Administrator*: A person who, for an organization, is responsible for the inventory, deployment and configuration management of hardware and software systems that compose the protection system(s) of the monitored system(s) on a days to day basis, with the focus of keeping the monitored system(s) secure according to rules derived from a security policy established for the monitored system(s) according to defined security objectives and policies of the organization.

- *Business Owner/Manager***:** A person with an executive level function within the organisation interested in understanding the security status of the business (mission) processes and possible business impact due to cyber-attacks. He or she is also interested in improving the security level of the business he of she owns/manages for it to better fulfil its missions.

Beyond the user roles defined in the [D2.2.1] for identified actors in the context of the organization of the PANOPTESEC User Partner. An additional common user role in the security domain is identified for the D5.1.1:

- *Security Officer*: A person who, in an organization, is responsible of the security and the management of security resources for monitored systems supporting missions and businesses of the organization. In particular, in order to achieve his objective, he usually has the responsibility to establish security objectives and a security policy relative to missions and businesses of the organization. A Security Officer is usually responsible for the enforcement of a security policy on monitored systems under its responsibility. In the context of the User Partner of PANOPTESEC, this role is carried out by Business Owners/Managers.

Definitely, a last actor applies also to the DRMRS, even if it is not a stakeholder per-se. The *Threat Agent Actor*, also called shortly in the context of the D5.1.1:

- *Attacker*: a person, system or entity that performs advert actions on the monitored system of an organization that bypass the security policy in order to gain unauthorized information or privileges with the focus of harming the businesses or prevent the organization from achieving one or several of its missions.

2.2 Requirements Elicitation

The process followed by WP5 Partners to establish the Specialized Requirements of a Dynamic Risk Management Response System is based on two main phases/parts:

- Preliminary Functional Architecture establishment
- Specialized Requirement collection

The methodology adopted an iterative process with successive period of proposal for new and revision of Specialized Requirements or Preliminary Functional Architecture modification.

Preliminary Functional Architecture establishment

Based on the list of Operational Requirements (see [D2.2.1]), a preliminary architecture of the global PANOPTESEC system (see [D3.1.1]), and the Deficiency Analysis (see [D2.1.1]), the WP5 Partners established a preliminary functional architecture of a *Dynamic Risk Management Response System* (DRMRS) that defines its global objectives and scope.

The objectives of the establishment of a functional architecture of the researched DRMRS were threefold:

- (i) identification of macroscopic functional modules to cover the scope of the sub-system identified as the objectives of the WP5 in the [DoW2013] and refined during the Work Package 3 PANOPTESEC system preliminary architecture establishment (see [D3.1.1]);

- (ii) identification of WP5 Partners that would act as Prime and address each of the functional modules during the Specialized Requirements collection phase;
- (iii) identification of WP5 Partners that would act as Contributor to each specific macroscopic functional domains of the DRMRS during the Specialized Requirements collection phase;

This preliminary functional architecture of a DRMRS were established and reviewed during a workshop that kicked-off the work of the WP5 in presence of other Work Package Leaders, Solution Provider Partners of the WP5 and the User Partner (WP5 kick-off workshop #1, 11 and 12 March 2014, ALBLF premises, Nozay, France).

This preliminary DRMRS architecture, represented as a functional block diagram (i.e. with an associated description of each functional blocks or module, possibly further decomposed in sub-blocks or sub-modules), were maintained up-to-date during the Specialized Requirement collection phase by the WP5 leader (ALBLF) regarding consistency (i) inside the WP5 with each Partners (ii) outside the WP5, with other Work Package Leaders.

In order to validate the approach proposed and established in the preliminary DRMRS functional architecture, several early mock-up prototyping of various concepts (e.g. Attack Graph or Path generation, vulnerability management, Risk Assessment based on Elementary and Composite Risks, Risk Profiles and break down analysis etc.) were developed, presented and debated during several meetings: (i) within the WP5 between Partners (i.e. WP5 Kick-off meeting between 11 and 12 March 2014), (ii) to other work packages Partners (i.e. Operational Requirements Plenary, 15 and 16 January 2014, WP5 kick-off workshop #1, 11 and 12 March 2014), (ii) to External Advisory Board members (i.e. External Advisory Board meeting #1, 5 May 2014), and outside the PANOPTESEC project (i.e. NATO SAS-106 Symposium, 9 and 10 June 2014, Tallinn, Estonia).

Specialized Requirements collection

Based on the preliminary DRMRS functional architecture and the identification of WP5 Primes and Contributors, a systematic process of collection and review of Specialized Requirements was initiated and instantiated. The process was based on rapid time period of proposal and review on a fortnightly basis, during which dedicated workshops and brainstorming took place between WP5 Partners or between the WP5 Leader and other Work Packages Partners or Leaders to control the consistency across the global PANOPTESEC system and its preliminary architecture. The process was decomposed in several steps:

- A proposal period (usually 8 days), so that WP5 Partners could provide
  - Additional functional domain descriptions;
  - Specialized Requirements in each functional domain;
- Two days of Work Package Leader review and integration, before the publishing a new version of the up-to-date Specialized Requirements document draft.
- A Partners' review and revision period (usually 8 days), in parallel with the proposal period. During this period, revisions of already proposed requirements and possibly evolution of the functional architectures were possible (e.g. after dedicated brainstorming or workshop meetings between the WP5 Leader, a domain Prime and possibly Contributing Partners).

This Specialized Requirement collection process was followed in order to issue a new version/revision/draft of the WP5 Specialized Requirements document (i.e. D5.1.1) on a fortnightly

basis to the WP5 Partners and the Project. This *two weeks process of proposal and review* enabled the early review on drafts of the DRMRS Specialized Requirements.

2.3 Requirements analysis

A specific format for the Specialized Requirement is used. This format follows the format specified in the RA Procedure as defined in the PANOPTESEC Project Handbook and provided by the Technical Project Manager (TPM). The format fulfills the needs of requirement expression, management and traceability in the PANOPTESEC research project. In order to be eligible as a valid Specialized Requirement, each proposal has to provide understandable and convincing text in each of the following fields of the specified format:

1. **id:** A unique identifier, that must be used for the traceability and management of the requirement across the PANOPTESEC project;
2. **Description:** A plaintext description of the requirement. This description must make use of a key word in capital letters used to express the requirement with a formulation that is as unambiguous and precise as possible. The allowed key words are defined below;
3. **Goal:** Used to express the objective of the function addressed by the defined requirement;
4. **MainPurpose:** Used to describe the justification of a corresponding function that would cover the requirement. It may give possible explanation concerning the context of the use of a function that addresses the requirement. Example(s) of the use of the function may be provided as a MainPurpose justification of the need fulfilled by the function.
5. **Importance:** The Importance value describes the importance of a requirement with respect to the stakeholder needs and provides a means to measure the success of the PANOPTESEC project. Importance is rated from 1 to 3. These three values are matched to the statements MAY (1), SHOULD (2) and MUST (3) key words, where the key words are defined by [RFC2119].
6. **Reachability:** The Reachability describes the relative amount of research or development effort that is estimated to fulfill the requirements, rated from 1 to 3. A level 1 reachability rating requires integration of existing components; level 2 reachability rating requires specific development then integration, and level 3 reachability rating requires research, specific development and then integration.
7. **Version:** The Version provides a means to track changes to requirements and enables reference to compare past versions with current versions for traceability.
8. **Type:** Defines the kind of requirement, which can be “Functional” or “Non-Functional”.

The formulation of the ‘**Description**’ field must adhere to good practices for requirements statements including the following:

1. **Clear:** Consists of only a single requirement, easily read and understood by the stakeholders and avoids subjective or open-ended terms;
2. **Complete:** Contains sufficient detail to define the system or software function;
3. **Consistent:** Uses the same formulation structure and has no conflict with or duplication of other requirements;
4. **Uniquely identified:** Has a unique identification number;
5. **Unambiguous:** Must not be susceptible to multiple interpretations;
6. **Important or relevant:** Is either essential or desired to meet stakeholder objectives. The level of importance should be clear to the reader using defined terms [RFC2119];
7. **Reachable or appropriate to implement:** Is possible to achieve with an appropriate amount of effort even where that effort may require a combination of both advanced research and design or implementation activities;
8. **Verifiable (testable):** Stated in such a way that it is possible to evaluate if the requirement has been achieved by the implementation through inspection, analysis, test or demonstration;

9. **Free of implementation details:** Does not prescribe a particular approach to design or implementation.

In a PANOPTESEC Project perspective, two values are also associated with each established requirement: (i) Importance, and (ii) Reachability.

Importance is defined by a numeric value in the '**Importance**' field from 1 to 3, according to the following scale:

- **MAY:** Represents 'Importance' value equal to '1';
- **SHOULD:** Represents 'Importance' value equal to '2'; and
- **MUST:** Represents 'Importance' value equal to '3'.

The '**Importance**' value will be used at the end of the project to assess the success of the PANOPTESEC project. It will also be used all along the project and at especially at the end of each iteration to prioritize research and development: Priority should be given to level 3 (**MUST**) requirements, then to level 2 requirements (**SHOULD**), then to level 1 requirements (**MAY**).

The '**Reachability**' field describes a rough estimate of the level of effort needed to fulfill the requirement. It is rated from 1 to 3, according to the following scale:

- **Level 1:** Reachability requires integration of existing components;
- **Level 2:** Reachability requires specific component or sub-component development and integration;
- **Level 3:** Reachability requires research, specific component or sub-component development and then integration.

2.4 Requirements modelling

There are a variety of methods and mechanisms for modelling requirements in the domain of system and software engineering. The decision is based largely on the scope and complexity of the project, the skills and capabilities of the project team, and the familiarity or availability of specific tools.

In the case of the PANOPTESEC project, the requirements are modelled in SysML within the system engineering repository using the Eclipse-based Papyrus software.

The system engineering repository is contained on a Subversion (SVN) server managed by the University of Lubeck (UoL).

It is the responsibility of the WP3 Leader to ensure requirements models are maintained within the system engineering repository. The WP3 Leader is supported by scientists and engineers from other WPs within the project.

2.5 Requirements traceability and coverage

Requirements traceability refers to the ability to trace the satisfaction of requirements from source, through derivation or refinement, into implementation, test and delivery. This traceability must be bi-directional. That is, the fulfilment of a preliminary objective, stated as a requirement should be traceable to the resulting verified feature or set of features within the system or software solution. Likewise a feature that is defined and verified within a system or software solution should be traceable to a source objective.

Requirements coverage refers to the degree of completeness that higher level requirements have been satisfied by more detailed requirements or by system or software components or sub-components. Complete coverage is the ideal, wherein all requirements are completely covered by lower level requirements or system or software components. In practical terms, this is not always possible. However, it is important for coverage to be demonstrated within design files such that the impact of coverage that is less than 100% can be analyzed and the potential impact of missing coverage understood.

In the case of the PANOPTESEC project, the requirements traceability is management in SysML within the system engineering repository using the Eclipse-based Papyrus software.

The system engineering repository is contained on a Subversion (SVN) server managed by the University of Lubeck (UoL).

It is the responsibility of the WP3 Leader to ensure requirements traceability is maintained within the system engineering repository. The WP3 Leader is supported by scientists and engineers from other WPs within the project.

2.6 Requirements validation

The validation of the Specialized Requirements for the Dynamic Risk Management Response System envisaged within the WP5, rely on mechanisms at different stages of the Specialized Requirement establishment process.

During the Specialized Requirement collection, the established and followed *two weeks process for proposal and review* enabled:

- A preliminary validation of every proposed Specialized Requirements by the WP5 Leader (also deliverable Editor of the D5.1.1 deliverable) on a regular basis, before the publishing in the next draft issued every two weeks;
- A regular review of the up-to-date list of Specialized Requirements by all other WP5 Partners (including the User Partner), so that revision can be requested for the next period in the process.

***Note*:** systematic merger of Partners contributions by the Editor and revision marks (i.e. which kept the originator of the revision using Microsoft Word revision features) were used during the whole process to highlight evolutions between two successive draft revisions of the D5.1.1.

During the Specialized Requirement collection, assessment including the Importance, Reachability and coverage over Operational Requirements expressed in the [D2.2.1] was provided for each proposed Specialized Requirement by the Contributing Partners. This self-assessment was validated by the Work Package Leader and Editor before the issuing of the next D5.1.1 draft revision scheduled in the process.

Note: Workshops or meetings were done for the assessment of Specialized Requirements on functional domains involving several Partners, between the Work Package Leader, the Prime and Contributing Partners.

At the end of the 3 months period during which the Specialized Requirements collection process took place, a QA review process was followed for the final validation of the deliverable by the Consortium and the issuing of a final version of the D5.1.1 deliverable representing the Requirements Baseline (RB) for WP5.

2.7 Requirements management (including change control)

The Requirements Baseline (RB) represents a formal agreement between the stakeholder(s) and the project team. As a formal agreement, the RB must not be changed, except through mutual agreement by the stakeholder(s). Consequently, the RB is a Configuration Item (CI) and any change to the RB must follow the configuration management (CM) and change control (CC) procedure described in the CM Plan. The CM Plan forms a part of the procedures and policies established under the PANOPTESEC Project Handbook.

2.8 Quality assurance

2.8.1 Quality criteria

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

For the purpose of the QA of the D5.1.1, the deliverable MUST be assessed according the following checklists:

- PEER REVIEW (PR) QA CHECKLIST: the D5.1.1 deliverable is a report, it then requires a proper peer review according to the checks defined in this checklist;
- REQUIREMENTS REVIEW (RR) QA CHECKLIST: the D5.1.1 deliverable is also a Requirement document, it then requires the assessment of the checks including in this checklist.

Note: the two QA checklists that the WP5 MUST use during the QA validation process of the D5.1.1 are available on the Project SVN (https://gotika.ifis.uni-luebeck.de/panoptesec/WP01/Project%20Handbook/Quality%20Assurance/QA%20Checklists).

2.8.2 Validation process

For the final validation of work products (i.e. deliverables) within the PANOPTESEC project, a final QA review process MUST be used before the issuing of a final version.

This QA validation process follows the Quality Review Procedure established by the QAM and validated by the Consortium in order to guarantee the high quality level of work products and to validate its adequacy according to the defined quality criteria chosen and defined for each deliverable (see Section 2.8.1). The Quality Review Procedure itself and the selection of the QA Review Committee are described in the PANOPTESEC Project Handbook [PH15]. It is specifically detailed in a PANOPTESEC Quality Review Procedure document available on the Project SVN (https://gotika.ifis.uni-

luebeck.de/panoptesec/WP01/Project%20Handbook/Quality%20Assurance/QA%20Procedure).

The QA validation process is scheduled in the QA Schedule [QAS15] managed by the QAM. And, the detailed results obtained after the process took place are captured and stored in the Project log in a Quality Review Summary Report also available on the Project SVN (https://gotika.ifis.uni-luebeck.de/panoptesec/WP01/Project%20Handbook/Quality%20Assurance/QA%20Reports).

3. DYNAMIC RISK MANAGEMENT RESPONSE SYSTEM GENERIC DESCRIPTION

The functional view of the Response System for the Dynamic Risk Management that should help Security Officers and Administrators to manage their ICT and ICS infrastructures, targeted within the WP5 of the PANOPESEC project, is presented in Figure 1 (using the functional Block diagram formalism).

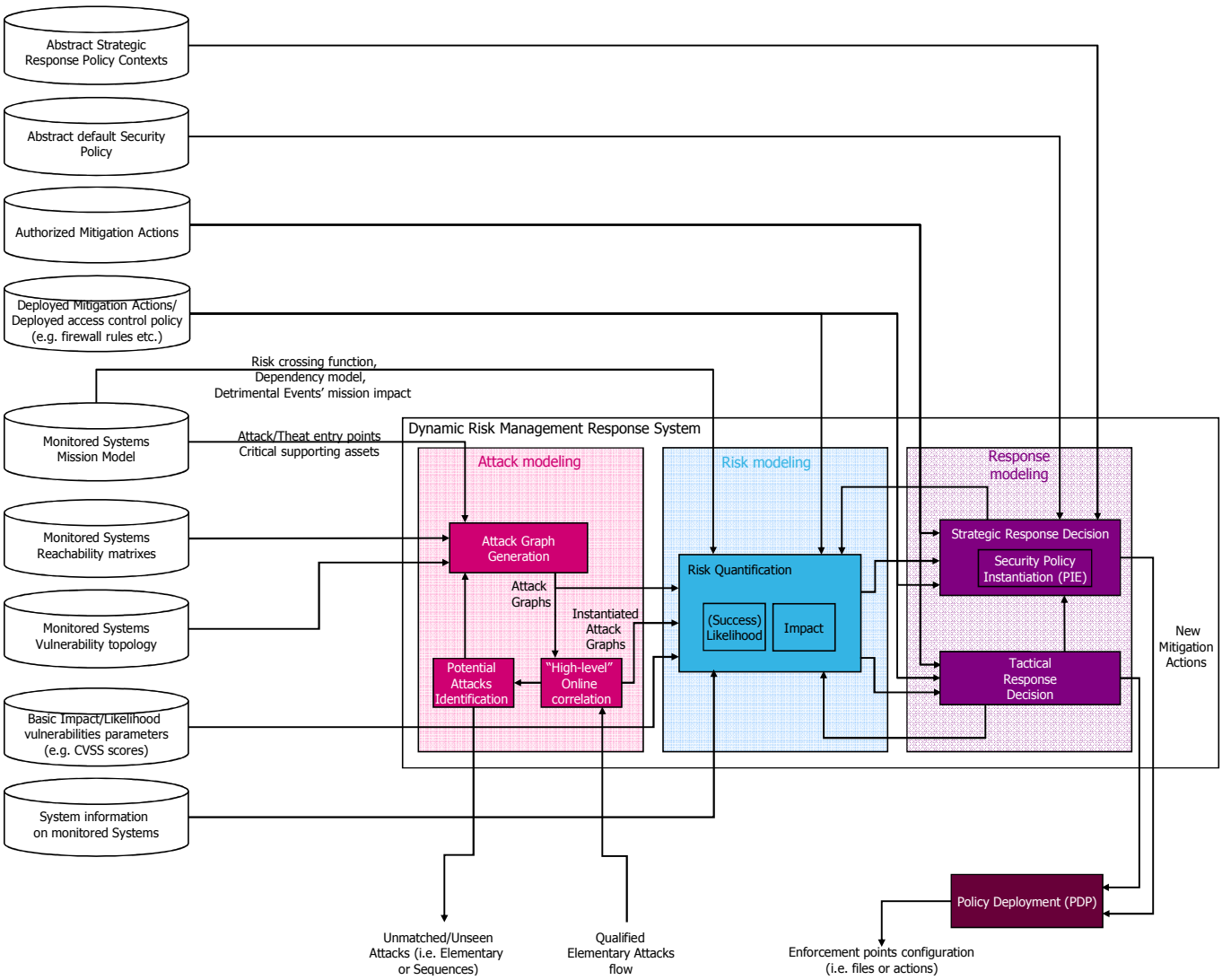

Figure 1 - Risk Management Response System functional block diagram

In this diagram are illustrated the generic high-level functions that enable the three stages of a Dynamic Risk Management which are:

- *Situation Awareness* (exploiting Attack Modeling): a commonly admitted generic definition is given by Mica Ensley in [END1995] as "the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future ". This interprets in our perspective as the regrouped features that enable a manager of monitored systems (i.e. ICT and ICS infrastructures) to grasp the global threats and current ongoing attacks weighing on its systems, business functions, or missions at any time, and project that status into the near future.
- *Risk Assessment* (exploiting Risk Modeling): identifies the features that enable a manager to qualify and quantify the risks of any identified threat or ongoing attack; but, also the possible

impacts and costs on the systems, business function, or missions that should result from the activation and deployment of possible response mechanisms that mitigate these risks.

- *Response Assistance* (exploiting Response Modeling): encompass the features that propose response possibilities to mitigate the identified risks, enable choice of the most suitable response possibilities to reduce the identified risks below an admissible level, and then compute the mitigation actions to be deployed on monitored systems.

3.1 Situation Awareness

3.1.1 Attack graph generation

The first step that enables assessment of the situation of a monitored system has the responsibility to give an awareness of the possible threats that may affect it. Indeed, efficient Information Security relies on an exhaustive identification of the scenarios that may cause unwanted or undesired incidents or events on the monitored system. Security standards relying on Risk Assessment (e.g. ISO27K series [ISO2013], ETSI TVRA [ETSI2006], NIST 800-30 [NIST2011], EBIOS v2 [ANSSI2011]) often define *threat* as the possibility for an identified threat agent or source, to perform adverse actions that exercise a vulnerability on identified assets of an organization. Assets are themselves relying on technical parts of the ICT and ICS infrastructures usually referred to as supporting assets.

A convenient means commonly adopted in the cyber security domain to represent an attack scenario is attack graphs. Various kinds of attack graphs have been proposed in the scientific literature in order to represent at an abstract level (i.e. not a specific occurrence of an attack scenario, but rather a template of a possible multi-steps attack) scenarios composed of several elementary attack steps ([JAJ2006], [SHE2002], [ING2006], [OU2004], etc.).

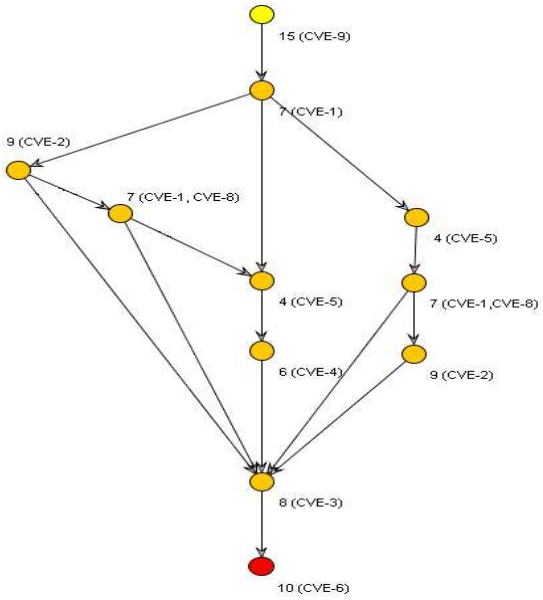

Figure 2 - Example of a topological vulnerability exploit dependency attack graph

In attack graphs, the nodes usually represent attack actions while the edges represent the dependency link or a causality relationship exists between attack actions. Figure 2 shows a fictitious example representing a topological vulnerability exploit dependency attack graph. In this graph, the nodes represent a device of the monitored system, identified by a unique identifier number, which may be attacked by exploiting one or several of its current vulnerabilities, identified by their CVE

identifier. This graph is topological because each node relates to a device of the monitored system. The semantics expressed by such graph is the vulnerability exploit dependency between nodes.

In the Response System envisaged by the PANOPTESEC project, the purpose of the attack graph generation (AGG) function is to compute automatically the most exhaustive list of possible attack scenarios. The researched attack scenarios are those which may lead attackers from identified potential entry points in the ICT and ICS infrastructures to supporting assets, by exploiting successively several vulnerabilities on different devices of the monitored ICT and ICS infrastructures. In order to establish those scenarios, the attack graph generation function should rely on an algorithm which bases its process on an up-to-date knowledge of the network connectivity between each piece of equipment of the monitored system (i.e. the network connectivity represents a list of the possible level four network ports and protocols that allow two devices to communicate in both ways). On another hand, the algorithm should also base its process on the knowledge of an up-to-date vulnerabilities inventory (i.e. a list of all pieces of equipment in the infrastructure with the exhaustive list of its current vulnerabilities).

In the architecture of the envisaged Response System, the attack graph generation is then the main function supporting the proactive chain of treatment that enables generation of an accurate yet up-to-date Situation Awareness of the monitored system.

Challenges exist in the field of attack graph generation. On the modelling perspective, the data format of the connectivity should be designed in order to enable and ease the algorithmic process to generate the list of attack scenarios in a reasonable time. But, the complexity usually derives from tradeoffs between computation time and exhaustiveness of identified attack paths. Moreover, regarding exhaustiveness, all known proposed algorithms are only considering monotonic attack scenarios, or non-backtracking attacks (i.e. attack scenarios for which an attacker never returns to an already compromised device), which is not always the case for the most dangerous attacks. Definitely, in line with the efficiency of the attack graph/path generation, the frequency of the generation, the conditions that may imply re-generation is needed, and the identification of possible optimisation depending on these conditions should also be taken into account.

3.1.2 High-level Online correlation

The aim of High-level Online Correlation function (HOC) is to correlate information about low-level alerts (i.e. alerts generated by sensors and IDSs in the monitored system and pre-processed by the Data Collection and Correlation System), with vulnerabilities of the monitored system itself to provide an accurate estimation of the possible on-going attacks [SMD2013].

To this aim, the HOC function takes mainly the following input on an online perspective: (i) the attack graph of the system and (ii) streams of low-level alerts. From one side, the attack graph provides “static” information about complex attack scenarios and identifies all the possible known attack paths that an adversary may conduct to break the system; on the other side, low-level alerts provide information about what is really happening in the system.

Each low-level alert corresponds to an observation while each node of the attack graph represents an elementary attack action. Therefore a first component of the HOC (called herein the transformation process) is in charge of transforming the attack graph representation into a set of correlation rules [GLO2008] [TVM2004]. This mapping between observation and elementary action is performed once

and offline. The correlation rules define for each elementary action of an attacker (vulnerability exploit) the source and the target identified in the low level alerts. At runtime, these rules are used by the second component of the HOC function (which implementation is usually called a correlation engine). It correlates low level alerts to discover hidden or implicit temporal and spatial relationships defining a possible attack pattern and tries to match such pattern on a known attack path.

The main issues arising in the design and development of a module that implements a HOC function are:

- *Scalability in terms of number of alerts that must be analysed*. The number of alerts generated within the monitored system may be huge due to its size, heterogeneity and complexity. As a consequence, analysing alerts can be seen as a Big Data problem. A common issue working with Big Data is the impossibility to use classical tools of data analysis, as data cannot be stored in a classical relational database; in addition, the solution must be able to provide outputs on-line as soon as alerts arrive. Thus, new solutions based on parallel and on-line computations need to be investigated. Note that the correlation engine is concerned by two scalability issues: it may be impacted both by an increase of the number of low level alerts and also by an increase of the size of the correlation rules.
- *Accuracy of the output*. Attacks to critical infrastructures are becoming more and more frequent and they are often overlapped in time (i.e., multiple attacks from different attackers at different sources may be in place in the same time period) and space (i.e., different attackers may try to compromise the same devices or the same “region” of the monitored system). This makes the application of classical pattern matching techniques far from trivial as multiple patterns may overlap making it difficult to detect them and the large number of possible concurrent alerts may introduce a noise effect in the recognition. The accuracy of the output depends on the mapping between observations and actions done during the transformation process.
- *Accuracy of the IDSs*. It is well known that generating too much information is equivalent to having no information if it cannot be organised and managed appropriately. To this aim, IDS systems are tuned to raise alerts with a certain accuracy to avoid the generation of too many false positives. However, this trade off has a drawback: important alerts may be missed. As a consequence, we have to design a HOC module able to work with potentially incomplete information due to the absence of alerts in the attack pattern to be detected.
- *Possible lack of information about attack patterns*. Attackers are becoming smarter and new types of attack are always possible. As in the previous case, new attacks generate the lack of necessary knowledge to understand what’s going on in the monitored system.

In order to address these issues, within the PANOPTESEC project, we intend to research the use of *pattern matching* and *pattern recognition* techniques. Concerning known attack patterns we plan to design algorithms and heuristics that analyse generated inputs and dynamically estimate the attack(s) that are more likely to be in place. An example of commonly used techniques is the estimation with maximum likelihood. Concerning unknown attack patterns we envisage the investigation of learning-based techniques that exploit the knowledge acquired during the system life time to infer common behaviours to detect anomalous and unknown patterns.

3.1.3 Potential Attacks Identification

The Potential Attacks Identification function (PAI) aims to extract useful information that may help to identify new attack scenarios (after a complementary analysis performed by a system administrator) or to update the set of already known attack paths (after a complementary analysis performed by the AGG module).

The PAI function receives information only from the HOC module. More precisely, during the correlation process, the incoming flow of low-level alerts is automatically subdivided into two subsets. Some alerts do not help the recognition of an ongoing attack scenario (e.g. alerts not belonging to an attack path or alerts included in an attack path but not included in a recent sequence) and we call them “unused alerts”. Otherwise, an alert corresponds to an expected elementary step in at least one of the identified attack paths: it is a “used alert”. Based on this dichotomy the PAI module performs additional investigations.

The PAI function is informed of all unused alerts. Unused alerts can be classified by the PAI module according to different criteria (alert’s type and frequency, alert’s target and frequency, etc.). Among the unused alerts, the PAI can also detect the existence of frequent patterns (e.g. sequences of a few unused alerts). The PAI module is also in charge of identifying the unused alerts that are potentially preceded by a missing alert [CM2002]. This detection can help to discover problems that affect the deployed monitoring devices.

Used alerts may also be of interest for the PAI function. The HOC function must then report to the PAI function any alert that allows progress within the detection of an ongoing attack but does not correspond to a well-identified vulnerability. This information is checked and used to update a knowledge base (new vulnerability or new characteristic of a monitoring device). On another hand, each time a complete attack path is detected, the involved targets should also be transmitted to the PAI function to enrich the knowledge base with identified new entry points or new targets. The information of the knowledge base may be provided back to the Attack Graph Generation function to update the attack graphs accordingly. Note that this accurate discovery of new entry points and new targets can only occur when the correlation engine implementing the HOC function, monitors any potential entry point and target (and not only those that are explicitly mentioned in the attack graph).

The outcomes of the analysis performed by a PAI function may be logged and provided to a system administrator or the AGG function. As one of the major objectives of alert correlation processes is to reduce the number of meta-alerts that have to be analyzed, a module implementing a PAI function must take into consideration avoidance of overwhelming the system (or administrators) with a huge flow of low level alerts that have not been considered during the detection process even if these alerts may help to identify and understand new ongoing phenomena.

The PAI function addresses the challenge of extracting some pertinent and concise knowledge from a stream of unused (and consequently uncorrelated) low level alerts. Furthermore, as some outcomes of the PAI are used by the Attack Graph Generation function to improve the attack graphs and as the updated attack graphs are used later by the HOC function which, in turn, provides information to the PAI function, the resulting cyclic flow of information is original and requires additional research to be mastered safely.

3.2 Risk Assessment

In order to take rational decisions, it is crucial to rely on a *rational metric* which, can be accurately measured or assessed, is unambiguous, and which encompasses the full information available to the decision maker. The objective of this rational metric is to remove and avoid the cognitive-bias which may exist in any decision made by human beings.

In many domains, like economics, energy, bank and insurance, homeland security, or even Defence; Risk is the rational metric commonly used to support the decision making process.

3.2.1 Risk quantification

From the very early thoughts and works on a Risk Theory [HUY1657] [BER1738], the scientific definition of risk has been established as "the expected value (i.e. in the mathematical sense) of a probability function of events". This can be interpreted as the mean value of the consequences of the considered events, weighted by their probabilities. If we denote by e_i the ith event of a set *I* of *n* events, which has a probability of occurring p_i, with a probable consequence C_i, the resulting risk *r* of the events of *I* is valued by the following formula:

$$r = p_1 \cdot C_1 + p_2 \cdot C_2 + \ldots + p_n \cdot C_n = \sum_{i=1}^{n} p_i \cdot C_i$$

Nowadays, several Security Controls Standards defines the Risk, and are applicable to general domains like, economics, health, environment, homeland security, and information and systems security:

- NIST 800-30 [NIST2013] defines the risk as "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence";
- Similarly, ISO27K series [ISO2013] and ETSI TVRA [ETSI2006] define the risk as "potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization".

In the model of Risk that is envisaged for the PANOPTESEC project, we then intend to express the magnitude of a risk in terms of the combination of two dimensions:

- *Likelihood*,
- *Impact*

Those dimensions may be assessed, measured or computed (e.g. based on statistics of previous occurrences of an event) on qualitative or quantitative scales (e.g. Turin scale ref). Based on the values of those dimensions, an evaluation function *f* computes the risk:

$$Risk = f(\, Likelihood, Impact \,)$$

This risk evaluation function can be a 2-d crossing matrix, as proposed by Security Control Standards like the ISO 27K series which provides a risk level in function of the discreet assessment of the two dimensions on qualitative scales. In the case of the PANOPTESEC project, the intent is to research on a quantitative, or hybrid model (i.e. part qualitative and part quantitative) and enable to use any kind of function for *f*.

The purpose of the Risk Quantification function is then to take in charge all the computation of the Risk dimensions defined in the considered model, in order to calculate through the risk evaluation function *f*, on demand and as accurately as possible, the long-term risk values that weigh on the Assets of the organization (i.e. evaluation of risks on a *proactive* perspective). But, its purpose is also to compute the fluctuation of those risk values (i.e. of its dimensions) based on: (1) evolution of the identified missions, businesses and policies of the organisation; (2) variations of the monitored

system (e.g. architectural and topological evolutions, systems' state, new discovered vulnerabilities); (4) threats (e.g. new threat agent detected) and adversaries actions (e.g. progression of attackers on identified attack scenarios) in order to reassess the risks on the *reactive* perspective; (5) responses measures decided or envisaged to counter threats and adversaries' actions.

In order to achieve these goals, the Risk Quantification function should rely on a model that expresses the dependencies between Assets of the organization and identified threats. This model should enable propagation of the Likelihood and Impact dimensions assessed at threat or technical levels, up to the Assets of the organization. Within the PANOPTESEC project our aim is to rely on attack graphs to link the threats and devices of the underlying technical infrastructures that support Assets of the organization (i.e. Supporting Assets). A "dependency model" should provide the link between adverse technical events (i.e. Detrimental Events), and the businesses (or missions) of the organization (i.e. its Assets).

Within the PANOPTESEC project, we also envisage that the Risk Quantification function addresses the computation of the risks on two different perspectives:

- The *proactive* perspective
- The *reactive* perspective

3.2.2 Likelihood assessment

Likelihood is one of the two dimensions of risk. It is mainly relevant to determine "how" the associated risk is delivered. In other words, it depends on the presence of threat agents (i.e. attackers) and the exposure of the monitored system to cyber attacks. State of the art methods rely on previous statistical data to provide an approximate evaluation of the likelihood. If such data is non-existent, which is often the case in the cyber security, then a Security Officer relies mainly on his expertise during a risk assessment process in order to evaluate likelihood values. Obviously, such manual evaluation is inaccurate, cumbersome to establish, and unsuitable for automated process such as those that are envisaged in the PANOPTESEC project. Regarding the two perspectives in this project (i.e. *proactive* and *reactive*), two types of likelihood are calculated and exploited:

- *Likelihood of occurrence*: this type is relevant to the proactive approach. It measures the potentiality of **occurrence** of a **possible** attack scenario. This measurement depends mainly on the monitored systems' state such as its exposure, its topology and existing vulnerabilities. Moreover, thanks to order relation over likelihood values, it allows prioritization of attack scenarios with respect to their potentiality of occurrence. Important to consider with this measurement, is the non-linear aspect of its perception by humans. A characteristic that the likelihood of occurrence quantification has to address at a stage in its computation.
- *Likelihood of success*: this type is relevant in the reactive part. It measures the potentiality of **success** of an **ongoing attack** in the monitored system. Similar to the *likelihood of* occurrence, the *likelihood of success* of an ongoing attack depends on the current state of the system, as well as the (detected) progress of the attack in the system. In other words, the alerts raised by IDS/IPS sensors, which are necessary to determine the progress of an attacker, are needed to calculate the likelihood of success of an ongoing attack scenario occurrence. The closer an attacker is to a critical asset, the higher is the success likelihood. Therefore, the success likelihood allows the systems to

prioritize ongoing attacks in order to address them. Similar to its proactive counterpart, the non-linear aspect of the perception of the likelihood of success has to address at a stage in its computation.

The main challenge to evaluate the likelihood of occurrence of potential attacks is the availability of required information. Particularly, attack graphs are leveraged in order to model potential attack scenarios. Hence, the topology, presence of vulnerabilities and their description, as well as other information related to the technical system's state, are crucial in order to calculate the Likelihood of occurrence. For the success likelihood, in addition to previous information, accurate detection and correlation systems are needed in order to follow the progress ongoing attacks. In particular, detection and correlation systems should overcome false positives and false negatives issues to ensure an accurate evaluation of ongoing attacks. As for the PANOPTESEC project the ambition is to assess the likelihood on a quantitative scale, an important challenge to address is the ability to compare likelihood values within the same perspective, but also between the two perspectives (i.e. proactive and reactive).

3.2.3 Impact assessment

The impact is the second dimension of the risk and is defined as the magnitude of harm that is expected to be perceived by an organization as a result of the consequences from unauthorized disclosure, modification, destruction, unavailability, or loss of information [KIS11].

Two paradigms exist in the Risk Management domain to express the consequence magnitude of detrimental events. On one hand, the impact magnitude may be assessed on a quantitative scale, usually representing financial impacts of detrimental events. On another hand, the impact may be expressed with a qualitative scale. However, qualitative levels of the scale must have a total order relation in order to be able to base decisions on them. An example of a five levels qualitative scale may be the following:

$$Extreme < High < Moderate < Low < None$$

Definitely, the impact of a detrimental event may also be expressed relative to the nature of its consequences. A way of expressing such nature is to bind the consequences on security dimensions. Commonly admitted natures for impacts on Information Systems are: *Confidentiality*, *Integrity* and *Availability (CIA)*.

In the proposed Response System, the purposes of the Impact assessment function are threefold:

- *Threat Impact Assessment*: has to assess the potential impact nature and magnitude caused by identified events feared by the organization (i.e. Detrimental Events) that may occur following the exploitation of possible attack scenarios;
- *Response Operational Impact Assessment*: has to assess the potential impact that efficient Mitigation Actions, in term of mitigation of the assessed risks, may cause on the organization in operational perspective.
- *Response Financial Impact Assessment*: has the goal to provide the assessment of the potential impact that efficient Mitigation Actions, in term of mitigation of the assessed risks, may cause on the organization in a financial perspective.

Regarding the *Threat Impact Assessment*, we intend that the Impact Assessment function evaluates each identified threat (i.e. Detrimental Events) with, (i) its nature expressed on the CIA dimensions, and (ii) its impact magnitude. To assess those characteristics, we intend to rely on identified possible and ongoing attack scenarios and a model of the links that may exist between them and the businesses or missions of the organization (i.e. Assets). Therefore, a proper modelling of the organization's structure and Assets (i.e. its missions or business processes) is essential in order to provide the Impact Assessment with, what we call, a "dependency model" between threats and Assets of the organization. Within the PANOPTESEC project, we envisage to research how this "dependency model" can be derived, from a formal modelling of the organization's structure and Assets, namely the Mission Graph (a part of the Mission Impact Module described within the purview of the Work Package 4 of the PANOPTESEC project [D4.1.1]).

For the *Response Operational Impact Assessment*, we must consider that some Mitigation Actions, while highly effective, might lead to an operational negative side-effect inside the network and therefore onto a mission (e.g. the shut-down of a highly vulnerable server might reduce the risk of it being exploited, however as the mission depends on this server, it highly affects the mission). The Impact Assessment therefore has to assess these operational negative side effects, called the Operational Impact, when given a hypothetical Response Plan (i.e. Response Plan may consist of multiple Mitigation Actions). Similarly in the evaluation of the exposure of a system to threats which may derive from an attack graph, the Operational Impact can be viewed as the exposure of the system to adverse actions due to an Administrator managing the system's Security. The Operational Impact should then provide the impact assessment that the corresponding Response Plan may cause on the organisation's missions or business processes. It should also provide an operational impact assessment at each layer that may be defined in the Mission Impact Module's Mission Graph (see [D4.1.1]). During the PANOPTESEC project, we intend to research on the need to take advantage of any available system information on the monitored or protected systems (e.g. Configuration Files, System Log Files, Traffic Dumps, PLC Dumps, Firewall Rules & Logs, Network Topologies, Security Policy Information, Network Historian Information, roles and responsibilities of involved actors, Alarm Response Policies & Logs) to enhance the accuracy of the Operational Impact of Mitigation Actions and Response Plans.

The purpose of the *Response Financial Impact Assessment* is to support the quantitative model that the PANOPTESEC project intends to use for decision-aided purposes within the Strategic Response Decision function, called the Return On Response Investment (RORI). This RORI index estimates not only the financial impact of security incidents (e.g. intrusions, attacks, errors), but also, the financial impact of implementing a given countermeasure. The RORI index evaluates and selects security countermeasures from a pool of candidates, by ranking them on a trade-off between their efficiency in stopping the intrusion/attack, and their ability to preserve, at the same time, the best service to legitimate users [GON13]. The Response Financial Impact Assessment then has to assess each financial parameter, needed for the computation of the RORI index for a Response Plan composed of multiple Mitigation Actions. The quantification of the RORI parameters only requires accuracy in their relative values (not in absolute values). If all the parameters are estimated by a standard methodology, the RORI evaluation should produce consistent and reproducible results.

3.3 Response Assistance

The concept of Risk is tightly linked to the need to make choices under uncertainties. This question is the central concern of Decision Theory, which is the theoretical foundation on which relies the Response Assistance. Its purpose is to give a rational tool that enables a decision maker to identify the best (or optimal) decision to take in the presence of uncertainties. In prescriptive decision theories, the kind of theory on which most decision support systems base, the decision maker is usually postulated to be ideal. This means that he is considered fully informed, rational, and able to compute with perfect accuracy [ROE2012].

The Response Assistance stage of the DRMRS is a decision support system that can follow two complementary approaches: strategic and tactical response proposals.

Strategic response relies on policy updates prior enforcement of new security requirements over security equipment. Examples of this approach in the literature include [BAR99; MON00; BLA04; ABO05; AUT09; HAC13; GON14]. The use of formal methods in these approaches helps at guaranteeing a global deployment that is free of anomalies. It also provides the necessary means to prove the achievement of requested properties prior to enforcement.

Tactical response is an intermediate level between long-term policy enforcement and short-term implementation of actions from a library of proven tactics. Examples of this approach in the literature include [CUP06; LAB07; KAN10; KAN11]. The goal is to ensure an always formally proved scenario before the concrete deployment. The use of model checking can be used to verify the possibility of temporary topology updates such as transformation of traffic flows (e.g., routing mitigation), filtering of traffic (e.g., access control) and alteration of equipment (e.g., patching).

According to these two established terms in the literature, the PANOPTESEC system will use strategic response as the primary mechanism for the enforcement of proactive mitigation, and tactical response for the enforcement of reactive mitigation. This way, strategic proactive response will fully rely on policy-driven mitigation, for the enforcement of long-term system changes with prior validation by human operators. Tactical reactive response will be in charge of short-term local actions, and can also benefit from a priori definition of security contextual policies that can later be activated and enforced upon the system. The combination of both approaches aims at handling both system vulnerabilities and ongoing attacks. We present in this section the core functionality elements and characteristics of both approaches.

Note that, for clarity reasons, we separate strategic proactive mitigation in two parts: (i) the *Strategic Response Decision* (SRD) function in itself; and, (ii) a sub-function for the specific purpose of *Security Policy Instantiation* (SPI), as depicted in Figure 1. In this representation, SRD conducts the process of computing of a given return on investment index for each mitigation action or response plan. While, SPI is a policy-driven process based on the OrBAC model (cf. deliverable 2.1.1 [D2.1.1] for a description of OrBAC and its detailed expected application within the PANOPTSEC project), which conducts the instantiation of abstract OrBAC policies, via Abstract Strategic Response Policy Contexts, into concrete mitigation policies.

3.3.1 Strategic Response Decision

Strategic Response Decision relies on policy-driven mitigation. It handles identified risks and provides mitigation actions (validated by human operators in the end) on a long-term *proactive* perspective. Multiple mitigation actions are evaluated using a return on response investment (RORI) index [GON13]. The RORI index is a relative security metric that indicates the level of benefit perceived if a given mitigation action is enforced. The input parameters for the RORI calculation are of two kinds: fixed parameters include the Annual Infrastructure Value (AIV), which depends on the system and corresponds to the fixed costs that are expected on the system regardless of the implemented countermeasure; and the Annual Loss Expectancy (ALE), which characterizes the intrusion or attack, and refers to the impact cost that is produced in the absence of countermeasures; variable parameters include the Risk Mitigation (RM), which represents the effectiveness of an action in mitigating the intrusion or attach, and the Annual Response Cost (ARC), which expresses the costs related to a given mitigation action. RORI is calculated according to the following equation:

$$RORI = \frac{(ALE \times RM) - ARC}{ARC + AIV} \times 100$$

The quantification of the parameters composing the RORI model is a task that requires expert knowledge, statistical data, simulation, and risk assessment tools. The ultimate goal is to select the candidate response set that provides the maximal positive RORI index.

The main challenge of using a cost sensitive metric like RORI is accuracy. There are many assumptions taken while analyzing every mitigation action. Results are as accurate as the forecasts of loss event frequencies on which they rely, and today these forecasts use best guesses rather than quantitative models. In addition, a great level of subjectivity is considered while estimating parameters such as benefits and importance of the investment in the RORI model. This latter relies on parameters such as the costs and benefits of a security solution. In general, the costs of countermeasures are rather easily defined, in contrast with their benefits, since it requires predictions of an event that has not yet occurred. However, this issue is of less importance when the ratio is used for relative comparisons.

3.3.2 Security Policy Instantiation

The instantiation of security policies will be performed via the Organization-based Access Control (OrBAC) model [ABO03, MIE05]. OrBAC allows modelling abstract security policies to organizational entities (e.g., organizations, roles, activities, views, contexts), as well as concrete security policies to instantiated entities (e.g., subjects, actions, objects). More information about the OrBAC model and its expected application with the PANOPTSEC project are available in Deliverable 2.1.1 [D2.1.1].

OrBAC contexts are used to define the security policies that apply in a given scenario, for instance, *default context* (i.e., an operational context in the absence of attacks that will set up the permissions and prohibitions by default) and *attack context* (i.e., a prerequisite context that triggers the selection of countermeasures). Such contexts are activated or deactivated according to the received alerts.

Placed outside the scope of the Dynamic Risk Management Response System, a policy deployment component will translate the OrBAC concrete rules into enforcement point configurations. The use of general-purpose transformation functions are expected to guarantee the eventual deployment into security devices such as network access and usage control equipment.

A challenge that is intended to be addressed by the project is the association of the RORI index with strategic mitigation policies approaches (relying on OrBAC) on a proactive perspective. Preliminary works [GON13, GON14] already reported the combination of RORI with OrBAC for the enforcement of strategic mitigation policies but on a reactive perspective (i.e. only based on extraction of data from intrusion detection alerts).

3.3.3 Tactical Response Decision

While the Strategic Response Decision envisages identified risks mitigation on a long-term *proactive* perspective, detection of ongoing 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 attack graph for instance. In these cases, a reprioritization of the risks that should be addressed needs to be performed and mitigation actions have to be taken with this new *reactive* perspective. This is the main function of the Tactical Response Decision, which obviously has to coordinate its decided tactical mitigation actions with the strategic response measures established by the Strategic Response Decision.

The Tactical Response Decision function is then responsible for deciding which of the risks quantified with a reactive perspective (i.e. *reactive risks*) have to be addressed by the Response System. It also has to issue the decision of the mitigation actions chosen to mitigate the reactive risks in the most efficient manner.

For this purpose, the decision should be continuously processed by relying on:

- An up-to-date quantification of the risks at any-time, based on the current state of progression of the identified attackers in the monitored system;
- An identification of the possible mitigation actions, chosen among a library of authorised mitigation actions, which can mitigate the identified and quantified risks. This mitigation should be done by preventing the progress of identified attackers along attack scenarios, as computed/monitored by the High-Level Correlation function;
- An evaluation of the *Return On Response Investment* of the different combinations of possible mitigation actions;
- The assessment of the Operational Impact (i.e. collateral damages) of identified possible mitigation actions to be deployed on the monitored system.

In order to accomplish its function, the Tactical Response Decision will have to consider several issues. Indeed, parameterisation of the function is probably needed. Some thresholds (which may be complex expressions, implying several systems' variables) need to be fixed: first, to define the risk level and value above which it is appropriate to decide tactical response measures; second, to know the targeted level of residual risks. Moreover, as the PANOTESEC system is envisaged as a decision support system, interactive validation of the decisions by human administrators will have to be considered. Definitely, conflicts between the Strategic and Tactical decisions will necessarily occur. The possibility to rely on the same formal policy language (i.e. OrBAC) to express both tactical and strategic responses should be considered, so that conflicts can be managed at the Strategic Response Decision and Security Policy Instantiation levels.

4. SPECIALIZED REQUIREMENTS

The section presents the *Specialized Requirements* of the *Dynamic Risk Management Response System* which is envisaged in the context WP5 of the PANOPTESEC project.

The requirements are organized in several groups, one for each function identified in the preliminary high-level functional architecture described in section 3, and one for the general purpose requirements that are not linked to a specific function but to the global DRMRS.

4.1 General

Functional requirements

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.GEN.R1	The Dynamic Risk Management Response System MUST be able to evaluate the risk deriving from the exploitation of existing system vulnerabilities.	Provide a classification of vulnerabilities according to the level of risk that they represent for the monitored or protected system.	The same vulnerability may affect different devices in the monitored system but, depending on where the device is placed and how it is connected to the rest of the system, the same vulnerability may be or may not be a threat. The PANOPTESEC system MUST help Security Administrators and Officer prioritizing the most urgent vulnerabilities to address based on the risk level they represent for the monitored or protected system.	3	2	2
WP5.GEN.R2	The Dynamic Risk Management Response System MUST be able to process streams of data in (near) real-time.	Acquire relevant information from the low-level correlation process to understand the situation in the monitored or protected system.	IDSes continuously provide a large number of alerts, including false positive and false negative. Such events are pre-correlated at the low-level generating a stream of low-level alerts. Such low-level alerts MUST be finally collected, filtered, aggregated and analysed at a higher level to understand what is really happening in (near) real-time.	3	2	2
WP5.GEN.R3	The Dynamic Risk Management Response System SHOULD be able to suggest efficient Mitigation Actions to an operator of the PANOPTESEC system.	Help Operators to take a decision having all the necessary information on the situation.	Security Administrators and Officer SHOULD be assisted in order to urgently decide which actions are the most appropriate to mitigate an attack and limit the damage on the organization.	2	2	2

Non-functional requirements

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.GEN.R4	Modules implementing the various functions of the Response System for the Dynamic Risk Management SHOULD be designed to be able to scale in terms of performance with respect to the volume of their inputs.	Ensuring availability and performance of the Response System for the Dynamic Risk Management.	Currently, most of the reactive response systems need human intervention. Thus, their reaction time may be in the order of day(s). The PANOPTESEC Dynamic Response System has to react timely (i.e. decreasing the reaction time from days to minutes) to potential on-going attack scenarios. PANOPTESEC modules implementing such Response System should not incur performance degradation with respect to a normal behaviour when handling unusual large volume of alerts (e.g., thousand of events per second).	2	3	2
WP5.GEN.R6	The Dynamic Risk Management Response System SHOULD be able to tolerate failures in any of its components.	Having a fault tolerant Dynamic Response System (i.e., a system able to work even experiencing faults in some of its components).	During the PANOPTESEC system lifetime it may happen that some of its modules stop to work. The module itself has to be able to tolerate such temporary unavailability and should be able to automatically recover form the failure in the order of minutes.	2	2	1
WP5.GEN.R5	Module implementing the various functions of the Response System for the Dynamic Risk Management MUST not adversely impact the monitored or protected systems when experiencing a failure.	Ensure the continuity of the monitored or protected systems in case of a failure or a compromising of the Response System.	Failures are unavoidable events in every environment. The PANOPTESEC system will co-exist together with a running operational environment from which it receives input and on which it can act to limit possible on-going attacks. One or several modules of the Dynamic Response System may stop unexpectedly at any time due to failures or compromising. If this happens, the operational environment must continue to work as if the PANOPTESEC system was not installed.	3	1	2
WP5.GEN.R7	The format of data object exchanged in the system SHOULD be structured (e.g. JSON) and defined according to the PANOPTESEC data model	Making inter-component communication interoperable.	Any PANOPTESEC module may be implemented by a different team using different programming languages and programming styles. However, regardless the internal development style, any module must be able to exchange data with other modules.	2	3	1

4.2 Attack graph generation

Functional requirements

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.AGG.R1	The Attack Graph Generation MUST retrieve the most up-to-date prioritized list of monitored systems (supporting assets) that an organization wants to monitor/protect, from a module of the PANOPTESEC system maintaining this knowledge (e.g. the Mission Impact Module).	Maintain at any time a prioritized list of all the monitored systems (supporting assets) for which the attack paths have to be computed.	Several (i.e. independent or not) systems (i.e. under the same or different administrative domains) may be under monitoring with regard to the security in an organization. Depending on the Assets and assessment from executives of the organization, the monitoring or protection of some of them may be a priori more important than others. This assessment and the list of systems itself may evolve depending on prioritizes and missions of the organization, the Attack Graph Generation must be kept informed of any changes in the list.	3	1	2
WP5.AGG.R2	The Attack Graph Generation MUST retrieve the most up-to-date reachability information for every monitored systems in an organization, in a structured way (i.e. the list of protocols and ports authorized between each pair of nodes of the infrastructure in one direction and the other, including the list of nodes enabling the communication in-between), from a module of the PANOPTESEC system maintaining this knowledge.	Maintain the up-to-date reachability structures for every monitored systems.	During the lifecycle of systems, modification of the possibility for nodes of infrastructures to communicate through networks may occur (e.g. routing modification due to routing protocols when gateways state changes, switching due to the isolation of nodes in the infrastructure, new filtering rules enforcement on firewalls, etc.). It is then necessary to be able to be informed on a regular basis, of those changes in the reachability of each systems under monitoring or protection in an organization.	3	2	2

WP5.AGG.R3	The Attack Graph Generation MUST retrieve the most up-to-date vulnerabilities inventory information for every system to be considered in an organization, in a structured way (i.e. for each node: the list of vulnerabilities, protocols or ports, and the level of privilege required to exploit it; together with, protocols or ports, and level of privilege gained if successfully exploited), from a module of the PANOPTESEC system maintaining this knowledge.	Maintaining a list of vulnerabilities for each node of the monitored systems, with the most up-to-date state of exploitability information.	During the lifecycle of a system, modification of the vulnerabilities existing on nodes of the infrastructure at a given time may occur (e.g. new discovered vulnerabilities, disappearance of patched vulnerabilities, supposed existence of 0-day vulnerabilities on suspect nodes, etc.). It is then necessary to be able to obtain the up-to-date list of vulnerabilities to be considered for each node of the monitored systems, on a regular basis.	3	2	2
WP5.AGG.R4	The Attack Graph Generation MUST retrieve the most up-to-date prioritized list of Entry Points associated to the monitored system, from which attackers may begin an Intrusion, from a module of the PANOPTESEC system maintaining this knowledge (e.g. the Mission Impact Module).	Maintain on a regular basis the up-to-date and prioritized list of potential Entry Points associated to every monitored or protected ICT systems.	During the lifecycle of a monitored system, the assessment of the most probable points in monitored ICT or ICS infrastructures from where attackers may start an intrusion may change (e.g. security expert assessment may evolve, evolution of the infrastructure may create new weaknesses in the architecture like the creation of an invite WiFi DMZ, etc.). It is then necessary to be able to obtain the up-to-date list of Entry Points to be considered for attack path generation, on a regular basis. As the computation of attack paths may be a time consuming task, prioritizing the most probable Entry Points could help in prioritizing the attack paths list establishment.	3	2	2

WP5.AGG.R5	The Attack Graph Generation MUST retrieve the most up-to-date prioritized list of critical devices (Supporting Assets) of every monitored systems that an organization absolutely does not want to see compromised by potential attackers (e.g. devices supporting the most critical Assets of the organization), from the module of the PANOPTESEC system maintaining this knowledge (e.g. the Mission Impact Module).	Maintain regularly an up-to-date and prioritized list of Supporting Assets (i.e. critical devices) that are critical for the organization in every monitored systems.	In monitored systems of an organization, some devices are supporting the delivery of critical services or the storage of critical information. Those devices, usually called Supporting Assets, are those that the organization absolutely does not want to see compromised at all. During the lifecycle of monitored systems, the list of those devices may evolve (e.g. when new critical services are deployed, when evolution of the ICT architecture occurs, when an organization reassess and modify its priorities or missions etc.). It is then necessary to be able to obtain the up-to-date list of those devices to be considered for attack path generation, on a regular basis. Note that, the evolution of those Supporting Assets should be slow or at least with a fixed frequency or planned basis.	3	2	2
WP5.AGG.R6	The Attack Graph Generation MUST compute as accurately as possible, the possible attack paths (i.e. direct and backtracking attack paths), which an attacker could use by exploiting vulnerabilities existing on devices (i.e. nodes) of each monitored system in the organization, from all identified Entry Points up to all known Supporting Assets .	Determine all possible attack paths that may exist in every monitored system.	In order to assess risks on an organisation of possible and ongoing attacks, it is necessary to identify the most exhaustively the possibilities of attackers to intrude in the monitored systems, which would enable them to reach a device supporting an Asset of the organization (i.e. a Supporting Asset). Those intrusions may occur by using a direct attack path (i.e. monotonic attack scenarios that always progress by compromising new nodes of the monitored system at each step) or a backtracking attack path (i.e. a non monotonic attack scenario, in which already compromised nodes may be	3	2	2

			attacked again to enhance an intruder's privileges). Identification of attack scenarios will also enable evaluation of possible corrective actions.			
WP5.AGG.R7	The Attack Graph Generation SHOULD receive at any time the most up-to-date reachability information of a monitored system, in a structured way (i.e. the list of protocols and ports authorized between each couple of nodes of the infrastructure in one direction and the other, including the list of nodes enabling the communication in-between), from the module of the PANOPTESEC system maintaining this knowledge.	Maintain at any time the most up-to-date reachability structure state for a monitored system.	Rapid modification of the possibility for nodes of the infrastructure to communicate through the network may occur (e.g. routing modification due to routing protocols when gateways state changes, switching due to the isolation of nodes in the infrastructure, new filtering rules enforcement on firewalls, etc.). In order to track as accurately as possible the ongoing attacks and try to address them with corrective actions, it is necessary to be informed as soon as possible of these changes by the external module of the PANOPTESEC system maintaining this knowledge.	2	2	2
WP5.AGG.R8	When the reachability of a node within a monitored system has changed, the Attack Graph Generation SHOULD (re-)compute, as accurately as possible, the possible attack paths (i.e. direct and backtracking attack paths), which an attacker could use by exploiting vulnerabilities existing on devices (i.e. nodes), from all identified Entry Points up to all identified Supporting Assets associated to this monitored system.	(Re-)Determine all possible attack paths for a monitored system when changes of its reachability have occurred.	Modification of the reachability occurring at any time may open new possibilities for attackers to exploit existing vulnerabilities and intrude in the monitored system toward reaching a device supporting an Asset of the organization (i.e. a Supporting Asset). Those intrusions may occur using a direct attack path (i.e. monotonic attack scenarios that always progress by compromising new nodes of the monitored system at each step) or a backtracking attack path (i.e. a non monotonic attack scenario, in which already compromised nodes may be attacked again to enhance an intruder's privileges). In order to track as accurately as possible the ongoing	2	1	2

			attacks and try to address them with corrective actions, a (re)-computation of the attack paths should take place as soon as changes in the reachability for a monitored or protected system occur.			
WP5.AGG.R10	The Attack Graph Generation SHOULD receive at any time the most up-to-date vulnerabilities inventory information for a monitored system, in a structured way (i.e. for each node: the list of vulnerabilities, protocols or ports, and the level of privilege required to exploit it; together with, protocols or ports, and level of privilege gained if successfully exploited), from the module of the PANOPTESEC system maintaining this.	Maintain at any time a list of vulnerabilities for each nodes of a monitored system with the most up-to-date state of exploitability information.	New vulnerabilities for devices of a monitored or protected infrastructure may be discovered at any time. And, this may potentially open new possibilities to attackers for intrusions. In order to track as accurately as possible ongoing attacks and try to address them with corrective actions, the Attack Graph Generation should receive new vulnerabilities, as soon as possible, from the external module of the PANOPTESEC system maintaining this knowledge.	2	2	2
WP5.AGG.R10	When the inventory of vulnerabilities for the nodes of a monitored system has changed, the Attack Graph Generation SHOULD (re-)compute, as accurately as possible, the possible attack paths (i.e. direct and backtracking attack paths), which an attacker could use by exploiting vulnerabilities existing on devices (i.e. nodes), from all identified Entry Points up to all identified Supporting Assets associated to this monitored system.	(Re-)Determine all possible attack paths (i.e. attack scenarios) for a monitored system when changes in the inventory of vulnerabilities for one or several of its nodes have occurred.	Modification of the nodes' vulnerabilities inventory of a monitored system may create new possibilities for attackers (i.e. new attack paths) to intrude toward reaching a device supporting an Asset of the organization (i.e. a Supporting Asset). Those intrusions may occur using a direct attack path (i.e. monotonic attack scenarios that always progress by compromising new nodes of the monitored system at each step) or a backtracking attack path (i.e. a non monotonic attack scenario, in which already compromised nodes may be attacked again to enhance an intruder's privileges). In order to track as accurately as possible the ongoing attacks and try to address them with corrective actions, a (re)-computation of	2	1	2

			the attack paths should take place as soon as changes in the inventory of the vulnerabilities for a monitored or protected system occur.			
WP5.AGG.R11	The Attack Graph Generation MAY receive (e.g. from the Potential Attack Identification Module) the list of nodes of a monitored system that have been observed as source nodes of attacks, and which are not currently identified as Entry Points of currently computed possible attack paths.	Maintain at any time a list of additional potential Entry Points that derives from the observation of real attacks on a monitored system.	During the operation of a monitored system, the High Level Online Alert Correlation function that traces the progress of observed attackers along possible attack paths, may receive intrusion alerts from IDS/IPS probes for which the source of the elementary attacks are not currently identified in one of the computed attack paths by the Attack Graph Generation. If these alerts are considered as a “true positives” (e.g. because low level correlation modules of the PANOPTESEC system are responsible for issuing only this kind of attacks to the HOC) these nodes may be new Entry Points for attackers in the system. In order to track as accurately as possible the ongoing attacks and try to address them with corrective actions, the Attack Graph Generation may be informed of potential additional Entry Points, as soon as possible, by the external module of the PANOPTESEC system in charge of extracting this knowledge (e.g. The Potential Attack Identification module).	1	2	2

WP5.AGG.R12	When the list of additional potential Entry Points associated to a monitored system has changed, the Attack Graph Generation MAY compute, as accurately as possible, the possible attack paths (i.e. direct and backtracking attack paths), which an attacker could use by exploiting vulnerabilities existing on devices (i.e. nodes), from all new additional potential Entry Points up to all identified Supporting Assets associated to this monitored system.	Determine all possible attack paths (i.e. attack scenarios) for a monitored system starting from the most up-to-date list of additional potential Entry Points.	New potential Entry Points for attackers in a monitored system may be detected. This may create new possibilities for attackers (i.e. new attack paths) to intrude toward reaching a device supporting an Asset of the organization (i.e. a Supporting Asset). Those intrusions may occur using a direct attack path (i.e. monotonic attack scenarios that always progress by compromising new nodes of the monitored system at each step) or a backtracking attack path (i.e. a non monotonic attack scenario, in which already compromised nodes may be attacked again to enhance an intruder's privileges). Additionally, some of the entries in the potential additional Entry Points list may disappear (e.g. a HOC determined that they are definitely deriving from false-positive IDS/IPS elementary alerts previously considered as true-positive). In order to track as accurately as possible the ongoing attacks and try to address them with corrective actions, a (re)-computation of the attack paths may take place as soon as the additional Entry Points list changes for a monitored or protected system.	1	2	2

WP5.AGG.R13	The Attack Graph Generation SHOULD stop an attack paths generation process on request, before the end of the computation of all attack paths for a monitored system.	Compute attack paths with the most up-to-date input information at any time.	During the computation of attack paths for a monitored system, modification of input of the Attack Graph Generation process spontaneously reported (e.g. change in the reachability, of the vulnerabilities inventory, of additional potential Entry Points etc.), may need to be urgently taken into account. In order to rapidly track the new possibilities of attackers to compromise the system, the Attack Graph generation should be able to stop a current computation process and restart it as soon as possible with the most up-to-date input information required by the attack paths generation.	2	2	2
WP5.AGG.R14	The Attack Graph Generation MUST notify other PANOPTESEC modules about changes in the list of generated attack paths for a monitored system has changed.	Notify, as soon as possible, modules of the PANOPTESEC system requiring it, the most up-to-date prioritized list of all possible attack paths computed for a monitored system.	Other functional blocks of the PANOPTESEC system use the list of attack paths to produce their own results. As the attack path generation process for a monitored or protected system produces regularly a more up-to-date list of attack paths, it is necessary to inform those functional blocks of its availability and that they should take them into account.	3	2	2
WP5.AGG.R15	The Attack Graph Generation SHOULD provide to modules of the PANOPESEC system requesting it , with the most up-to-date prioritized list of attack paths of a monitored system.	Serve on demand modules of the PANOPTESEC system requesting it, with the most up-to-date prioritized list of all possible attack paths computed so far for a monitored system.	Some functional blocks of the PANOPTESEC system may need a list of the most up-to-date attack paths to produce their own results at any given time and, cannot wait until the next scheduled time for the Attack Graph Generation to send them the up-to-date list of attack graphs. In such case, they may need to be able to require on demand to the Attack Graph Generation the current list of the most up-to-date attack paths computed so far.	2	3	2

WP5.AGG.R16	The Attack Graph Generation MAY receive a list of additional previously unidentified vulnerabilities potentially existing on nodes of a monitored system which are not currently identified in the regular vulnerabilities inventory, from a module of the PANOPTESEC system responsible of the establishment of this knowledge.	Maintain at any time an up-to-date list of additional supposedly existing vulnerabilities on nodes of a monitored system.	During the operation of a monitoring system, the High Level Online Alert Correlation that trace in the PANOPTESEC system the progress of observed attackers along possible attack paths, may receive intrusion alerts from IDS/IPS probes for which the target nodes are currently identified as not vulnerable to the kind of elementary attacks related in the alerts. This kind of alerts may be assessed by a module of the PANOPTESEC system to determine if unknown vulnerabilities (e.g. 0-day vulnerabilities) for these target nodes should or should not be considered for the generation of attack paths. If this is the case, the Attack Graph Generation should be able to receive from a module of the PANOPTESEC architecture the supposedly new vulnerabilities with their exploitability characteristics.	1	2	2
WP5.AGG.R17	The Attack Graph Generation MAY compute, as accurately as possible, the additional possible attack paths (i.e. direct and backtracking attack paths), which an attacker could use by exploiting (i) vulnerabilities existing on devices (i.e. nodes) (ii) plus the additional previously unidentified vulnerabilities potentially existing on devices of a monitored system, from all identified Entry Points up to all identified Supporting Assets associated to this monitored system.	Determine additional possible attack paths that may exist in a monitored system taking into account a list of additional supposedly existing vulnerabilities on its nodes.	Possible attack paths may not be computable based on the knowledge of vulnerabilities existing on nodes of a monitored system. This may be because of the existence of unknown vulnerabilities (i.e. 0-day vulnerabilities) on some nodes. In some cases, modules of the PANOPTESEC system may make supposition of the existence of unknown vulnerabilities and their exploitability characteristics on nodes of this system (e.g. based on the processing of specific alerts issues by IDS/IPS sensors, statistical data, etc.). Based on this knowledge, the list of attack paths computed by the Attack Graph	1	3	2

			Generation module may be augmented by additional attack paths.			
WP5.AGG.R20	The Attack Graph Generation MAY request necessary information of exploitability (i.e. for each vulnerability: supposed protocols or ports, and supposed level of privilege required to exploit it; together with, supposed protocols or ports, and supposed level of privilege gained if successfully exploited) for supposedly existing vulnerabilities on nodes of a monitored system, from a module of the PANOPTESEC system responsible of the establishment of this knowledge.	Maintain at any time an up-to-date list of additional supposedly existing vulnerabilities on nodes of a monitored system.	During the operation of a monitoring system, the High Level Online Alert Correlation that trace in the PANOPTESEC system the progress of observed attackers along possible attack paths, may receive intrusion alerts from IDS/IPS probes for which the target nodes are currently identified as not vulnerable to the kind of elementary attacks related in the alerts. This kind of alerts may be assessed by a module of the PANOPTESEC system to determine if unknown vulnerabilities (e.g. 0-day vulnerabilities) for these target nodes should or should not be considered for the generation of attack paths. If this is the case, the Attack Graph Generation will request from a module of the PANOPTESEC architecture, exploitability characteristics of the supposedly new vulnerabilities to be able to take them into account in the attack graph generation process.	1	2	2

Non-functional requirements

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.AGG.R18	The Attack Graph Generation SHOULD determine the possible attack scenarios between an Entry Point and a Supporting Asset in minutes, for a monitored system topology composed of several hundreds of distinct nodes (including routing, firewalling and	Scale the possible attack scenarios generation process to a medium size monitored system (i.e. up to 500 distinct nodes).	During the lifecycle of and operation of a monitored system, the vulnerabilities are usually discovered and published on a daily basis. Moreover, the patching of servers may take several days, or even weeks. To enhance the state-of-the-art on vulnerability management, the	2	3	1

	terminal devices).		assessment of possible attack scenarios on a monitored system should be as fast as possible.			
WP5.AGG.R19	The Attack Graph Generation SHOULD protect the Vulnerability Inventory, the identified Entry Points and Supporting Assets, the Reachability and computed possible attack scenarios of each system it monitors or protect, both within the process memory or during their external storage, from unauthorized disclosure.	Protect the critical information of monitored or protected system during runtime and storage.	The information provided by other modules of the PANOPTESEC system for the purpose of the possible attack scenarios generation, as well as the computed possible attack scenarios are critical for the organisation. This information could be hijacked by attackers to threaten the most important assets of their target. The Module that handles and produces this kind of information should apply software tamper resistant techniques to protect it during the computing process (e.g. obfuscation) or in case of storage of the information (e.g. ciphering) to prevent attackers' attempts to access it.	2	2	1

4.3 High-level Online correlation

Functional requirements

Id	Description	Goal	MainPurpose	Importance	Reachability	Version
WP5.HOC.R1	The HOC module MAY provide a dynamic ranking of potential attack targets.	Provide to the Risk Quantification module an overview of the possible paths that an attacker may be following.	In order to react to on-going attacks, the system must be able to understand what is going on in real time, i.e. which attack paths are being followed by an attacker and the progress over them. This knowledge enables operators to take Situation-aware corrective actions.	3	2	2
WP5.HOC.R2	The HOC module MAY provide a dynamic ranking of potential attack targets.	Provide to the Risk Quantification module an evaluation about the evolution of the attack in terms	Each target may be potentially reached through multiple attack paths. Assessing in real-time the evolution of	1	1	2

		of the topological distance from the compromised node to the target taking into account the attack scenario criticality. Thanks to this distance it is possible to provide the operator with a ranked list of targets.	an attack may bring additional information to an operator that must decide which is the best corrective action and on which attack path to perform them first.			
WP5.HOC.R3	The HOC module SHOULD trigger "unmatched alerts" to the Potential Attacks Identification Module.	Provide the Potential Attacks Identification Module with the list of unused alerts. To Handle the uncertainty represented by the lack of knowledge about emerging attacks or following by the accuracy of the underlying IDS.	A low level alert does not match a correlation rule if (1) the vulnerability field is empty, or (2) the alert does not permit the progression of any correlation rule, or (3) the alert vulnerability is never mentioned in the set of correlation rules derived from the AGG module. In these cases an unmatched alert should be sent to the PAI module. Note that an unmatched alert should be related to a new kind of unknown attack (i.e., not described by the current set of correlation rules used by the HOC).	2	1	2
WP5.HOC.R4	The format of alerts triggered by any module of the monitored system and the information modelled in the attack graph MUST provide some semantically equivalent information (at least source node, target node and exploited vulnerability), in a structured format (e.g., JSON, XML, etc.).	Make possible the potential matching between alerts generated by IDS and the attack actions (e.g., nodes) described in the attack graph.	In order to recognize and understand what is happening in the monitored system, the attack graph must represent actions of the attackers, devices attacked, etc. in a format compliant to the information carried by the alerts.	3	2	2
WP5.HOC.R5	The communications between PANOPTESEC modules SHOULD be asynchronous (i.e., non-blocking communication).	Notify the Risk Quantification module about instantiated attack paths through asynchronous communication modalities (e.g. pub/sub paradigms).	The module receives alerts generated by the IDSes and correlates them with the attack paths. Higher-level alerts are computed and sent to the Risk Quantification module. Given the	2	1	2

			possible high rate flow of low level alerts and the real time requirements, both these communications should be deployed in a non-blocking way.			
WP5.HOC.R6	The HOC module MUST be independent from the underlying IDS, IPS, probes etc.	The module must be able to continue to work even in case of changes in the ICT infrastructure, thanks to the normalization of low level alerts.	The application logic of the HOC module relies on the treatment of normalized low level alerts (that contain source, target and vulnerability information). Thanks to the normalization, these types of information are independent from any IDS, IPS, etc. When some IDSes stop, the lack of information received may impact the recognition of a given scenario. Nevertheless, the HOC module continues to work correctly according to the low level alerts it receives.	3	1	2
WP5.HOC.R7	The module MUST be able to adapt to changes in attack paths.	The HOC module must be able to dynamically handle new attack paths.	Attack paths are continuously evolving and the module must be able to dynamically handle such emerging threats. When a new attack scenario is provided, a new correlation process has to be initialized. During this initialisation, two cases are possible. Either on-going recognitions are ignored (reset of the HOC module) or, when possible, the alerts already observed in the past are taken into account to build the new initial state, which should reflect the previous progresses of the recognition. The choice between the two cases depends on the differences between the old attack paths and the new ones. In the	3	3	2

			case of a major evolution, reset may be the only possible solution.			
WP5.HOC.R8	The module MUST be able to automatically transform the information provided by AGG into correlation rules representing a format usable by the HoC.	The HOC module must be able to automatically transform attack graphs into correlation rules that can be handled by the module itself.	An attack graph corresponds to a set of attack paths, each path can be modelled by a correlation rule. These rules follow a syntax, specific for the correlation engine using them. The transformation process must be an automatic process that does not require human intervention.	3	3	2
WP5.HOC.R9	The module MAY recognize some topological approximate attack paths	The HOC module MUST be able to identify a sequence of low level alerts involved in a correlation rule, where the (1) source node (entry point) of the first low level alert or (2) the target node of the last level alert do not match exactly the correlation rule.	This kind of approximate match will be used by the PAI module to identify new entry points, new targets or new attack paths.	1	2	2
WP5.HOC.R12	Modules implementing the Dynamic Response System SHOULD be able to tolerate uncertainty on the low level alerts generated by the monitoring system (e.g., low level alerts with incorrect embedded information, false negative low level alert etc.), through the recognition of approximate attack paths with missing alerts.	Be able to take into account the possible lack of low level alerts or the lack of knowledge about vulnerabilities.	It may happen that IDSes, probes and so on may not detect some vulnerability exploit in a multi-steps attack. In addition, they may raise low-level alerts, which do not correspond to a real attack step. The PANOPTESEC system should be able to consider the possibility that an attack action (corresponding to a step in an attack path) has happened even if it has not be detected (missing alert), providing an estimation over the attack scenario.	2	2	1

Non-functional requirements

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.HOC.R13	The module SHOULD react to performance degradation	Avoiding memory and CPU bottleneck during the system lifetime.	When the system ages, the HOC module keeps in memory old partial recognitions that can slow down the detection. A periodic purge of recognitions SHOULD be performed. This could be done by periodically deleting old partial recognitions. Note that the suppression of old information may have an impact on the pertinence of the detection. A trade-off has to be defined.	2	2	1
WP5.HOC.R14	The module SHOULD adapt the time required to switch to a new attack graph according to the current rate of the flow of alerts	Depending on the size of the graph, a history of the recently analysed low level alerts SHOULD be replayed or not.	The installation of a new attack graph is followed by the replay of the history of past accepted low level alerts. A trade-off SHOULD be found between the quality of the detection (which is better when more stored alerts in the history are replayed) and the time of replay (which decreases when a smaller part of the history is replayed).	2	2	1
WP5.HOC.R15	The HOC module SHOULD automatically be able to scale in terms of incoming low-level alerts rate.	Keep the HOC performances acceptable even in presence of large amounts of data to evaluate.	During its lifetime PANOPTESEC may experience high low level alert rate. Even in that situation the module should keep on working in reasonable time, with respect to performance requirements.	2	3	1
WP5.HOC.R16	The module SHOULD ensure the security of raised high level alerts	All high level alerts raised SHOULD be stored encrypted	In order to improve the integrity and confidentiality of high level alerts raised by the HOC modules, they are stored in a database in encrypted form.	2	3	1
WP5.HOC.R17	Communication with other PANOPTESEC components SHOULD be encrypted and authenticated.	Keep the data flow information protected against possible eavesdroppers and corruptions.	Communication by secure channels make it possible to avoid situations in which an attacker may inject low-level alerts in the system leading the correlation to wrong results.	2	2	1

4.4 Potential Attacks Identification

Functional requirements

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.PAI.R1	The Potential Attack Identification Module SHOULD be able to identify new phenomena.	Identify unexplained ongoing phenomena that could be the consequence of new unknown attacks.	Some low-level alerts received by the HOC do not allow a progress in the recognition of an ongoing attack. Among these alerts, the PAI module should detect those: - that are frequent: a low level alert (or a sequence of low level alerts) occurs in the monitored system and may be the consequence of a new form of attack; - that are quite similar to some other used alerts (for example the action is the same but the target is different): the configuration of the HOC module is incomplete and must be corrected.	2	2	2
WP5.PAI.R2	The Potential Attack Identification Module SHOULD be able to identify missing alerts identification	To detect a scenario for which all the steps have been seen except one (or a few).	Some low-level alerts received by the HOC do not allow progress in the recognition of an ongoing attack because some preliminary step of the attack scenario has not generated an alert. For example, in a scenario where 2 alerts “a” and “b” must occur in a row, an alert “b” is transmitted by the HOC module to the PAI module if an alert “a” has not been observed before. In such a case, the PAI should check if the scenario “ab” occurred (alert “a” is missing) or not (the alert “b” previously ignored by the HOC module can also be ignored by the PAI module).	2	2	2
WP5.PAI.R3	The Potential Attack Identification Module SHOULD be able to identify new entry points and targets	Inform the AGG module that either new entry point(s) or new target(s) have been involved in attack.	Each time a high-level alert is raised by the HOC module, the provided list of involved nodes is used to identify those that are not yet present in any attack path.	2	2	2
WP5.PAI.R4	The Potential Attack Identification Module SHOULD be able to identify new vulnerabilities	To inform the system administrator that a new vulnerability is potentially present on one node, and that further investigation is needed.	When the HOC uses a low level event to progress in the recognition of a scenario, it emits an unused-alert to the PAI module whenever the vulnerability field of this low level alert is missing.	2	1	2

Non-functional requirements

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.PAI.R5	All alerts raised SHOULD be stored encrypted	Security of raised alerts	In order to improve the confidentiality of the alerts raised by the HOC modules, all alerts stored in a database SHOULD be encrypted.	2	1	1
WP5.PAI.R6	The PAI MAY be optional	Performance of the PANOPTESEC system may be improved if the PAI module is not included.	When confronted to a huge number of alerts, it MAY be useful to disconnect the PAI functionality from the PANOPTESEC system. This component is non critical because it does not participate in the detection of attack multi-step scenarios depicted by the attack graph.	1	3	1

4.5 Risk quantification

Functional requirements

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.RQU.R1	The Risk Quantification MUST retrieve the “dependency model” associated to the organization, from a module of the PANOPTESEC system responsible of the management of this knowledge (e.g. Mission Impact Model).	Maintain the most up-to-date model of dependency links between Assets, Supporting Assets, and Detrimental Events with their Impact natures and values for the organization.	The identified missions or businesses of an organization evolve during its lifetime for many types of reasons (e.g. new projects start or end, new services are offered to customers implying new ICT services or critical Information storage, businesses are abandoned or transferred to other organisations, etc.). These modifications, captured in a “dependency model”, must be captured to assess (or reassess) risks that weight on the organization.	3	2	2

WP5.RQU.R2	The Risk Quantification MAY retrieve the most up-to-date list of mitigation actions deployed in monitored systems of the organization, that controls the access to the systems (e.g. rules of the filtering policy etc.), from a module of the PANOPTESEC system responsible of the establishment of this knowledge.	Maintain regularly the up-to-date list of the deployed mitigation actions in monitored systems of the organization.	During the lifecycle of a monitored system, the deployed filtering policy (i.e. firewalling rules) changes to open new flows (e.g. new ports, protocols or access for new machines) for many reasons (e.g. firewall maintenance, modification of the filtering policy, request to open new flows from technical managers etc.). Even if the modifications of the filtering policy do not expose the monitored systems to new threats or raise the risks for the organization, the contribution to the risks (i.e. residual risk induced) by new or existing open flows (i.e. “accept” firewalling rules) may change. These modifications should be captured to determine (or reassess) the origin of assessed risks that weight on the organization.	1	2	2
WP5.RQU.R3	The Risk Quantification MUST retrieve a prioritized list of identified possible attack paths (i.e. possible attack scenarios), from the module of the PANOPTESEC architecture managing this knowledge (e.g. Attack Graph Generation).	Maintain regularly the up-to-date and prioritized list of possible attack scenarios to be considered for Risk Quantification on a proactive mode.	During the lifecycle and operation of a monitored system, modification of the possible attack scenarios will occur on a regular basis (e.g. new vulnerabilities discovered or patched each day, modification and evolution of the infrastructure, possible deployment of new security policy, new identified Entry Points, changes in some priorities for the organization etc.). These changes must be captured to modify the assessment of risks on the organization.	3	2	2

WP5.RQU.R4	The Risk Quantification MUST retrieve the list of most up-to-date instantiated attack paths, each representing the current progress of one of the currently considered detected attackers along one of the identified possible attack paths (i.e. an ongoing attack scenario), from the module of the PANOPTESEC system managing this knowledge (e.g. the High Level Online Alert Correlation).	Maintain regularly the up-to-date list of ongoing attack scenarios, and attackers, to be considered for Risk Quantification on a reactive perspective.	During the operation of the monitored system, attackers perform several elementary attack actions in sequence to progress toward a target that is considered critical by the organization, because it supports one or several of its Assets. This progression, captured by ongoing attack scenarios, must be taken into account to update the assessment of risks on the organisation on a reactive perspective.	3	2	2
WP5.RQU.R5	When changes in the list of currently evaluated possible attack paths, ongoing attack scenarios, or in the "dependency model" have occurred, the Risk Quantification MUST retrieve: - Likelihood assessment values of potential attack scenarios and Likelihood of success of ongoing attack scenarios for the new list, from the PANOPTESEC module managing this knowledge (e.g. Likelihood Assessment); - Impact assessment values for each Detrimental Event of the currently considered "dependency model", induced by each currently considered possible attack scenarios and ongoing attack scenarios of the new list through the most up-to-date "dependency model", from the PANOPTESEC module managing this knowledge (e.g. Threat Impact Assessment).	Maintain the most up-to-date list of Likelihood assessment values and Impact assessment values of Detrimental Events as soon as changes are detected in possible and ongoing attack scenarios, or the "dependency model", from both proactive and reactive perspectives.	When a new service is deployed (i.e. enters under the monitoring of the PANOPTESEC system), two consequences are produced. First, new or modification of the possible and ongoing attacks, which requires the reassessment of their Likelihood values. Second, new Detrimental Events' possible Impacts to the organization are induced, causing an update of the "dependency model". These consequences must be captured to update the risks weighing on the organization.	3	2	2

WP5.RQU.R6	The Risk Quantification MAY process spontaneous changes in: - Likelihood assessment values of potential attack scenarios and Likelihood of success of ongoing attack scenarios, from the PANOPTESEC module managing this knowledge (e.g. (Success) likelihood assessment); - Impact assessment values for each Detrimental Event, of the currently considered "dependency model", induced by each currently considered possible attack scenarios and ongoing attack scenarios through the "dependency model", from the PANOPTESEC module managing this knowledge (e.g. Impact assessment).	Maintain at any time the most up-to-date list of Likelihood assessment values and Impact assessment values of Detrimental Events as soon as changes are detected in possible and ongoing attack scenarios, or the "dependency model", from both proactive and reactive perspectives.	The exploitability, difficulty and impact characteristics (i.e. as described in CVSS Base and Temporal scores) of a vulnerability existing on several Supporting Assets of monitored or protected systems (i.e. not patched up to now), are updated by the community of experts that manages this knowledge (e.g. the NVD database). No new or modification of possible and ongoing attack scenarios are induced. But, these modifications cause the reassessment of Likelihood values and Impact values for Detrimental Events, which may produce unacceptable risks for the organisation.	1	2	2
WP5.RQU.R7	The Risk Quantification MAY retrieve the risk crossing function to be used to compute a Risk level based on an impact value (e.g. as computed by the Impact Assessment for each Detrimental Event) and, a Likelihood value assessed on a proactive or a reactive perspective (e.g. as computed by the (Success) likelihood assessment) from the PANOPTESEC module that manages this knowledge.	Maintain the most up-to-date risk crossing function to use for computing risk levels based on the Likelihood and the Impact dimensions.	The organization monitoring its systems with a PANOPTESEC system, changes the risk management methodology or approach on which it relies (e.g. changes from the EBIOS [ANSSI2011] to the Mehari [CLUSIF2010] methodology). In the new methodology, it makes use of a new way to compute risk levels based on the two dimensions of Likelihood and Impact.	1	2	2

WP5.RQU.R8	The Risk Quantification MUST Compute the contribution to the Risk levels of each Detrimental Events associated to an Asset of the organization, of each entities identified in the “dependency model” (e.g. Assets, Supporting Assets), each entities of the possible attack scenarios (e.g. devices of monitored systems, vulnerabilities, Entry Points), andeach deployed mitigation action that controls the access to the monitored systems (e.g. rules of the Filtering policy etc.), on a proactive perspective.	Maintain the contribution to the Risk levels of Detrimental Events, of each identified technical entity of the “dependency model”, possible attack scenarios and deployed mitigation actions, on a proactive perspective.	During the lifecycle of the monitored systems of an organization, many kind of changes occurs regularly: new vulnerabilities are discovered each day; modifications of deployed mitigation actions change the exposure of the systems to threats each week; new threats (i.e. additional Entry Points) may be identified; new or modifications to the ICT services priorities for the businesses/missions of the organization, etc. Those periodic changes may result in contributions to the risks for the organization of technical entities of the “dependency model”, possible attack scenarios and deployed mitigation actions, requiring their regular reassessment on a proactive perspective.	3	2	2
WP5.RQU.R9	The Risk Quantification MUST compute the contribution to the Risk levels of each Detrimental Event associated to an Asset of the organization, of each entities identified in the “dependency model” (e.g. Assets, Supporting Assets), each entities of the ongoing attack scenarios (e.g. devices of the monitored systems, vulnerabilities, Entry Points), and each deployed mitigation action that controls the access to the monitored systems (e.g. rules of the Filtering policy etc.), on a reactive perspective.	Maintain the contribution to the Risk levels of Detrimental Events, of each identified technical entity of the “dependency model”, ongoing attack scenarios and deployed mitigation actions, on a reactive perspective.	During the lifecycle of monitored systems of an organization, many kinds of changes regularly occur: attackers perform elementary attacks and progress along their attack scenarios; new vulnerabilities are discovered each day; modifications of deployed mitigation actions change the exposure of the systems to threats each week; new threats (i.e. additional Entry Points) may be identified, etc. Those periodic changes result in contributions to the risks for the organization of technical entities of the “dependency model”, ongoing attack scenarios and deployed mitigation actions, requiring their regular reassessment on a reactive perspective.	3	2	2

WP5.RQU.R10	The Risk Quantification MUST compute Risk levels for each Detrimental Event linked to an Asset of the organisation, based on the risk contribution computed for each entities identified in the "dependency model" (e.g. Assets, Supporting Assets), each entities of the possible and ongoing attack scenarios (e.g. devices of the monitored system, vulnerabilities, Entry Points), and each deployed mitigation action that controls the access to the monitored or protected systems (e.g. rules of the Filtering policy etc.) on both proactive and reactive perspectives.	Maintain the Risk levels of each Detrimental Events of the "dependency model", on both proactive and reactive perspectives.	During the lifecycle of monitored systems of an organization, many kinds of changes regularly occur: attackers perform elementary attacks and progress along their attack scenarios; new vulnerabilities are discovered each day; modifications of deployed mitigation actions change the exposure of the systems to threats each week; new threats (i.e. additional Entry Points) may be identified; new or modifications to the ICT services priorities for the business functions or missions of the organization, etc. Those periodic changes may result in risks for the organization requiring their reassessment on both proactive and reactive perspectives.	3	2	2
WP5.RQU.R11	For each element of a list of possible Mitigation Actions, the Risk levels reduction relative to each Detrimental Event linked to an Asset of the organisation, for both proactive and reactive perspectives, MUST be computed on demand.	Compute on demand the potential risk reduction induced on each Detrimental Event of each Mitigation Actions of a list, on both proactive and reactive perspectives.	A list of the Mitigation Actions that can potentially mitigate a selection of the proactive and reactive risks identified for the organization has been done by another module of the PANOPTESEC system (i.e. Tactical Response Decision or Strategic Response Decision). To decide which of those mitigation actions should be chosen for deployment, their effectiveness in term of risk reduction needs to be assessed and transmitted to the module of the PANOPTSEC system that will manage the final deployment decision.	3	3	2

WP5.RQU.R12	The Risk Quantification MAY process spontaneous changes in the list of mitigation actions deployed in monitored or protected systems of the organization, which control the access to the system (e.g. rules of the filtering policy etc.), received from the module of the PANOPTESEC system responsible of maintaining this knowledge.	Maintain at any time the up-to-date list of the deployed mitigation actions in monitored systems of the organization.	During the lifecycle of a monitored system, the deployed filtering policy (i.e. firewalling rules) changes to open new flows (e.g. new ports, protocols or access for new machines) at any time for many reasons (e.g. firewall maintenance, modification of the filtering policy, request to open new flows from technical managers etc.). The modifications do not expose the monitored systems to new threats or raise the risks for the organization. But the contribution to the risks (i.e. residual risk induced) by new or existing open flows (i.e. “accept” firewalling rules) may change.	1	2	2
WP5.RQU.R13	The Risk Quantification SHOULD process spontaneous changes to the prioritized list of identified possible attack paths (i.e. possible attack scenarios), from the module of the PANOPTESEC system that maintains this knowledge (e.g. Attack Graph Generation).	Maintain at any time the up-to-date and prioritized list of possible attack scenarios to be considered for Risk Quantification on a proactive perspective.	During the lifecycle and operation of a monitored system, modification of the possible attack scenarios occur at any time (e.g. new vulnerabilities are discovered, possible deployment of new security policy, new Entry Points identified, changes in some priorities for the organization etc.). One or several modified or new possible attack paths may cause evolution of risks on the monitored system that should be addressed immediately on a proactive perspective.	2	2	2
WP5.RQU.R14	The Risk Quantification SHOULD process spontaneous changes to the list of instantiated attack paths (i.e. ongoing attack scenarios), from the module of the PANOPTESEC system that maintains this knowledge (e.g. High Level Online Alert Correlation).	Maintain at any time the up-to-date list of ongoing attack scenarios, and attackers, to be considered for Risk Quantification on a reactive perspective.	During the operation of the monitored system, attackers perform rapidly several elementary attack actions in sequence to progress toward a target that is considered critical by the organization (e.g. because it support one or several of its Assets). One or several detected and correlated elementary attacks may cause	2	2	2

			rapid evolution of risks on the monitored system that should be addressed immediately on a reactive perspective.			
WP5.RQU.R15	The Risk Quantification SHOULD (re-)compute the contribution to the Risk levels of each Detrimental Event associated to an Asset of the organization, of each entities identified in the "dependency model" (e.g. Assets, Supporting Assets), each entities of possible and ongoing attack scenarios (e.g. devices of the monitored system, vulnerabilities, Entry Points), and each deployed mitigation action that controls the access to the monitored systems (e.g. rules of the Filtering policy etc.), impacted by changes in Likelihood assessments or Impact contributions (i.e. induced by currently considered possible or ongoing attack scenarios through the "dependency model") or changes in the deployed mitigation actions, on both proactive and reactive perspectives.	Maintain at any time the most up-to-date contribution to the Risk levels of Detrimental Events, for each identified technical entity of the "dependency model", possible and ongoing attack scenarios and deployed mitigation actions, on both proactive and reactive perspectives.	The Risk Quantification receives spontaneously an updated list of possible and ongoing attack scenarios, implying modifications of the assessed Likelihood values and assessed Impact values of Detrimental Events. These spontaneous changes should induce the reassessment of the contribution to the risks for the organization of technical entities of the "dependency model", possible and ongoing attack scenarios and deployed mitigation actions on both proactive and reactive perspectives.	2	3	2
WP5.RQU.R16	The Risk Quantification SHOULD (re-)compute Risk levels for each Detrimental Event linked to an Asset of the organisation impacted by changes in Likelihood assessments or Impact contributions (i.e. induced by currently considered possible or ongoing attack scenarios through the "dependency model") or changes in the deployed mitigation actions, on both proactive and reactive perspectives.	Maintain at any time the most up-to-date Risk levels for each Detrimental Events of the "dependency model", on both proactive and reactive perspectives.	The Risk Quantification receives spontaneously an updated list of possible and ongoing attack scenarios, implying modifications of the contribution to the risks for the organization of technical entities of the "dependency model", possible and ongoing attack scenarios and deployed mitigation actions. Those changes should induce the reassessment of the risks for the organization on both proactive and reactive perspectives.	2	3	2

WP5.RQU.R17	The Risk Quantification MUST notify other PANOPTESEC modules requiring it, the changes in the list of Risk levels for each considered Detrimental Events linked to an Asset of the organisation.	Notify modules of the PANOPTESEC system requiring it, with the changes in the Detrimental Events' Risk levels on proactive and reactive perspectives.	Modules of the PANOPTESEC system should decide which risks are unacceptable (i.e. Strategic Response Decision for the proactive perspective and Tactical Response Decision for the reactive perspective). They must be informed as soon as possible of any change in the assessment of those risks. In order to decide which Mitigation Actions are efficient to manage the unacceptable risks, they also have to be informed of any change in the risk contribution of technical entities of the "dependency model", possible and ongoing attack scenarios and deployed mitigation actions.	3	3	2
WP5.RQU.R18	The Risk Quantification MUST provide to modules of the PANOPESEC system requesting it , the list of Risk levels for each considered Detrimental Events linked to an Asset of the organisation.	Serve on demand modules of the PANOPTESEC system requesting it, with the most up-to-date assessment of Risk levels for each Detrimental Events of the "dependency model", on a proactive or reactive perspective.	Modules of the PANOPTESEC system should decide which risks are unacceptable (i.e. Strategic Response Decision for the proactive perspective and Tactical Response Decision for the reactive perspective). They may request at any time the most up-to-date assessment of those risks. In order to decide which Mitigation Actions are efficient to manage the unacceptable risks, they also may request the most up-to-date assessment of the risk contribution of technical entities of the "dependency model", possible and ongoing attack scenarios and deployed mitigation actions.	3	3	2

WP5.RQU.R21	The dependency model, which is processed by the Risk Quantification, MUST include: - Supporting Assets of the monitored systems, - Assets of the organization (i.e. critical services or information for the businesses of an organization, supported by Supporting Assets of monitored or protected systems), - Detrimental Events that are feared by the organization with the associated nature of the Impact feared by the organization (i.e. on the Confidentiality, the Integrity and the Availability) and an assessed Impact value on the organization (i.e. as it would be assessed in a classical Risk Management process).	Maintain the most up-to-date model of the dependency model links between Assets, Supporting Assets, and Detrimental Events with their Impact natures and values for the organization.	The identified missions or businesses of an organization (i.e. its Assets) rely on technical devices (i.e. Supporting Assets) of the monitored system that may incur attacks causing feared events (i.e. Detrimental Events) which represent a risk for the organisation. To be able to assess which possible or ongoing attack scenarios represent risks for the organisation, the links between the Assets, the Supporting Assets and the Detrimental Events must be expressed in a structured “dependency model”. Hence, the main purpose is to associate attack scenarios to detrimental events.	3	2	2

Non-functional requirements

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.RQU.R19	The Risk Quantification SHOULD comply with a standard ISO27000 series risk assessment methodology.	Comply with already deployed or used risk assessment processes in an organization.	Organizations usually have methodological processes based on an ISO 27000 series compliant methodology for periodically assess the risks on the organisation. Those processes are usually not automated but define important business and technical information (e.g. critical assets and supporting assets), scales for the assessment of the likelihood and the impact of threats (e.g. a risk crossing	2	2	1

			function or matrix). The Risk Quantification should be able to rely on these information, concepts and scales in order to ease the PANOPTESEC system configuration.			
WP5.RQU.R20	The Risk Quantification SHOULD protect the possible and ongoing attack scenarios, the "dependency model" entities (e.g. Assets, Supporting Assets, and Detrimental Events), and the various computed values and levels of risks, both within the process memory and during their external storage, from disclosure to unauthorized module or user.	Protect the critical information of monitored or protected system during runtime and storage.	The information provided by other modules of the PANOPTESEC system for the purpose of the Risk Quantification, as well as the various computed risks are critical for the organisation. This information could be hijacked by attackers to more accurately target the most threatening assets. Modules that handle and produce this kind of information should apply software tamper resistant techniques to protect it during the computing process (e.g. obfuscation) or in case of storage of the information (e.g. ciphering) to prevent attackers' attempts to exploit it.	2	2	1

4.5.1 Likelihood assessment

Functional requirements

Id	Description	Goal	MainPurpose	Importance	Reachability	Version
WP5.LA.R1	The Likelihood Assessment MUST retrieve the most up-to-date prioritized list of identified possible attack paths (i.e. possible attack scenarios) used to compute the likelihood on a proactive perspective, from the module of the PANOPTESEC system maintaining this knowledge (e.g. Attack Graph Generation or Risk Quantification).	Maintain the up-to-date and prioritized list of possible attack scenarios to be considered for likelihood assessment on a proactive perspective.	During the lifecycle and operation of a monitored system, modification of the possible attack scenarios will occur (e.g. new vulnerabilities discovered or patched each day, modification and evolution of the infrastructure, possible deployment of new security policy, new identified Entry Points, changes in some priorities for the organization etc.). To follow the risks evolution on the organization, the Likelihood Assessment	3	1	2

			has to be aware of the changes in possible attack scenarios to compute an up-to-date assessment.			
WP5.LA.R2	The Likelihood Assessment MUST retrieve the most-up-to-date exploitability and difficulty characteristics (e.g. parameters of the Base and Temporal score of CVSS metrics) of the vulnerabilities present in the possible attack paths (i.e. possible attack scenarios) and instantiated attack paths (i.e. ongoing attack scenarios) used to compute the likelihood on proactive and reactive perspectives , from the module of the PANOPTESEC architecture who manages this knowledge.	Maintain the up-to-date exploitability and difficulty characteristics of the list of vulnerabilities participating in possible and ongoing attack scenarios used for likelihood assessment on proactive and reactive perspectives.	During the lifecycle of vulnerabilities, it may happen that the assessment of its exploitability and difficulty performed by security experts changes (e.g. when an exploit program begin to circulate on the Internet). It is then required to guarantee that the vulnerability characteristics used to compute the likelihood on proactive and reactive perspectives are up-to-date.	3	2	2
WP5.LA.R3	The Likelihood Assessment MUST compute the most up-to-date likelihood of compromising of each identified Supporting Asset induced by each identified possible attack paths (i.e. possible attack scenarios) on a proactive perspective.	Compute the most up-to-date likelihood assessment of possible attack scenarios on a proactive perspective.	During the operation and lifecycle of the monitored system, modification in the possible attack scenarios, or change in the assessment of the characteristics of vulnerabilities (e.g. parameters of the Base and Temporal CVSS metrics [CFRA2014]) participating in those attack paths, will periodically occur. Those changes will have an influence on the likelihood assessment of identified possible and ongoing attack scenarios that need to be addressed.	3	1	2
WP5.LA.R4	The Likelihood Assessment SHOULD retrieve the list of the most up-to-date instantiated attack paths (i.e. ongoing attack scenarios, each representing the current progress of one of the detected attackers along one of the possible attack paths) used to compute the	Maintain the up-to-date list of ongoing attack scenarios, and attackers, to be considered for likelihood assessment on a reactive perspective.	During the operation of the monitored system, attackers perform several elementary attack actions in sequence to progress toward a target that is considered critical by the organization, because it supports one or several of its Assets. In order to track the evolution of	2	2	2

	likelihood on a reactive perspective, from the module of the PANOPTESEC system maintaining this knowledge (e.g. the High Level Online Alert Correlation or Risk Quantification).		the risks on the organization, the Likelihood Assessment should keep abreast of the progress of each attacker along possible attack scenarios regularly.			
WP5.LA.R5	The Likelihood Assessment SHOULD compute the likelihood of success, for each currently considered detected attacker, to reach identified Supporting Assets on a reactive perspective (i.e. likelihood of each ongoing attack scenario).	Compute the most up-to-date assessment of the Likelihood of success for ongoing attack scenarios on a reactive perspective.	During the operation and lifecycle of the monitored system, modification in the assessment of the progress of attackers toward devices supporting Assets of the organization occurs frequently (e.g. by performing elementary attack actions). Moreover, change in the assessment of the characteristics of vulnerabilities (e.g. parameters of the Base and Temporal CVSS metrics [CFRA2014]) participating in those attack paths, will periodically occur. To capture those changes the likelihood of success of ongoing attack scenarios should be updated in order to track the evolution of the risks on the organization on a reactive perspective.	2	2	2
WP5.LA.R6	The Likelihood Assessment SHOULD process spontaneous changes to the prioritized list of identified possible attack paths (i.e. possible attack scenarios) used for likelihood computation on a proactive perspective, from the module of the PANOPTESEC system that maintains this knowledge (e.g. Attack Graph Generation).	Maintain at any time the up-to-date and prioritized list of possible attack scenarios to be considered for likelihood assessment on a proactive perspective.	During the lifecycle and operation of a monitored system, modification of the possible attack scenarios occur at any time (e.g. new vulnerabilities are discovered, possible deployment of new security policy, new Entry Points identified, changes in some priorities for the organization etc.). One or several modified or new possible attack paths may represent risks on the organization that should to be addressed immediately on a proactive perspective. The Likelihood Assessment then should be aware immediately of the changes in possible attack scenarios, so that an up-to-date assessment can be made as soon	2	2	2

			as possible for the Risk Quantification.			
WP5.LA.R7	When the list of vulnerabilities involved in possible attack paths (i.e possible attack scenarios) or instantiated attack paths (i.e. ongoing attack scenarios) has changed, the Likelihood Assessment SHOULD retrieve the most-up-to-date exploitability and difficulty characteristics (e.g. parameters of the Base and Temporal score of CVSS metrics) of the vulnerabilities present in those attack paths, from the module of the PANOPTESEC system that maintains this knowledge.	Maintain at any time the up-to-date exploitability and difficulty characteristics of the list of vulnerabilities participating in possible and ongoing attack scenarios used for likelihood assessment on proactive and reactive perspectives.	During the lifecycle and operation of a monitored system, modification of the possible attack scenarios occur at any time (e.g. new vulnerabilities are discovered, possible deployment of new security policy, new Entry Points identified, changes in some priorities for the organization etc.). One or several modified or new possible attack paths may have new vulnerabilities for which the characteristics should be retrieved so that the Likelihood Assessment can be processed for the Risk Quantification.	2	2	2
WP5.LA.R8	The Likelihood Assessment SHOULD receive spontaneous changes to exploitability and difficulty characteristics (e.g. parameters of the Base and Temporal score of CVSS metrics) of vulnerabilities involved in possible attack paths (i.e. possible attack scenarios) or instantiated attack paths (i.e. ongoing attack scenarios) , from the module of the PANOPTESEC system that maintains this knowledge.	Maintain at any time the up-to-date exploitability and difficulty characteristics of the list of vulnerabilities participating in possible and ongoing attack scenarios used for likelihood assessment on proactive and reactive perspectives.	During the lifecycle of a vulnerability, some assessed characteristics of difficulty and exploitability may change (e.g. an exploit program emerge for this vulnerability whereas it was not the case before). The Likelihood of possible attack scenarios or the Likelihood of success of ongoing attack scenarios may change inducing modifications to the priorities of the risks for the organization. The module computing this likelihood and likelihood of success should then be aware of vulnerability characteristics changes as soon as possible.	2	2	2
WP5.LA.R9	When possible attack paths, or the characteristics of the vulnerabilities in those paths have changed, the Likelihood Assessment MUST (re-	(Re-)compute the most up-to-date Likelihood assessment of possible attack scenarios on a	During the lifecycle and operation of a monitored system, modification of the possible attack scenarios occur at any time (e.g. new vulnerabilities are	2	2	2

	)compute the likelihood of compromising of each identified Supporting Asset induced by each of those identified possible attack paths (i.e. possible attack scenarios) on a proactive perspective.	proactive perspective, when changes in the identified possible attack paths have occurred.	discovered, possible deployment of new security policy, new Entry Points identified, changes in some priorities for the organization etc.). One or several modified or new possible attack paths appear, containing new vulnerabilities so that the Likelihood of possible attack scenarios (i.e. proactive perspective) has to be processed again for the Risk Quantification.			
WP5.LA.R10	The Likelihood Assessment MUST process spontaneous changes to the list of instantiated attack paths (i.e. ongoing attack scenarios) to be considered for likelihood computation on a reactive perspective, from the module of the PANOPTESEC system that maintains this knowledge (e.g. High Level Online Alert Correlation).	Maintain at any time the up-to-date list of ongoing attack scenarios, and attackers, to be considered for likelihood assessment on a reactive perspective.	During the operation of a monitored system, attackers perform rapidly several elementary attack actions in sequence to progress toward a target that is considered critical by the organization (e.g. because it support one or several of its Assets). In order to track the evolution of the risks on the organization, the module computing the Likelihood of success of ongoing attack scenarios has to be informed of the progression of attackers along possible attack scenarios as soon as their elementary attacks are detected and correlated (e.g. in instantiated attack paths by the High Level Online Alert Correlation).	2	2	2
WP5.LA.R11	When instantiated attack paths (i.e. ongoing attack scenarios) or the characteristics of the vulnerabilities in those paths has changed, the Likelihood Assessment MUST (re-)compute the likelihood of success of each currently considered detected attacker, to reach identified Supporting Assets on a reactive perspective (i.e. likelihood of each ongoing attack scenario).	Compute the most up-to-date assessment of the Likelihood of success for ongoing attack scenarios on a reactive perspective, when changes in instantiated attack paths have occurred.	During the operation and lifecycle of a monitored system, the progress assessment of attackers toward devices supporting Assets of the organization, is performed as soon as their elementary attacks are detected and correlated (e.g. in instantiated attack paths by the High Level Online Alert Correlation). Moreover, change in the assessment of the characteristics of vulnerabilities	3	3	2

			participating in those attack paths, may occur at any time. To identify a change to stop those ongoing attacks scenarios, the effect of those modifications on the reactive perspective of the likelihood dimension have to be assessed as soon as possible.			
WP5.LA.R12	The Likelihood Assessment MUST notify, modules of the PANOPESEC system requiring it (i.e. Risk Quantification), that changes in the list of Likelihood of potential attack scenarios (i.e. proactive perspective) and likelihood of success of ongoing attack scenarios (i.e. reactive perspective) have occurred.	Notify, as soon as possible, modules of the PANOPTESEC system requiring it, of changes in likelihood values that occurred on a proactive or a reactive perspective.	The likelihood and likelihood of success values deriving from possible and ongoing attack scenarios change at any time for many reasons (e.g. new vulnerabilities discovered or modification in existing vulnerabilities exploitability characteristics). The module of the PANOPTESEC system which should assess the risks for the organization based on likelihood or likelihood of success values (i.e. Risk Quantification) must be informed as soon as possible of any change for the immediate reassessment of those risks.	3	2	2
WP5.LA.R13	The Likelihood Assessment SHOULD provide to modules of the PANOPESEC system requesting it (i.e. Risk Quantification), the changes in Likelihood of potential attack scenarios (i.e. proactive perspective) and likelihood of success of ongoing attack scenarios (i.e. reactive perspective); even if the process of likelihood assessment for every attack paths that changed has not ended.	Serve and demand modules of the PANOPTESEC system requesting it, with the most up-to-date assessed likelihood values on a proactive or a reactive perspective.	The likelihood and likelihood of success values deriving from possible and ongoing attack scenarios change at any time (e.g. new vulnerabilities discovered or modification in existing vulnerabilities exploitability characteristics). A module of the PANOPTESEC system which assess the risks for the organization based on the most up-to-date likelihood or likelihood of success values (i.e. Risk Quantification), may request those values when needed in order to reassess the risks.	2	2	2

Non-functional requirements

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.LA.R14	The Likelihood Assessment SHOULD protect the possible and ongoing attack scenarios, and their computed likelihood and success likelihood values, both within the process memory and during their external storage, from disclosure to unauthorized module or user.	Protect the critical information of monitored or protected system during runtime and storage.	The information provided by other modules of the PANOPTESEC system for the purpose Success Likelihood computation, as well as the various computed likelihood and success likelihood values are critical for the organisation. This information could be hijacked by attackers to more accurately target the assets which are the most easily accessible. Module that handle and produce this kind of information should apply software tamper resistant techniques to protect it during the computing process (e.g. obfuscation) or in case of storage of the information (e.g. ciphering) to prevent its harmful exploitation.	2	2	1

4.5.2 Threat Impact Assessment

Functional requirements

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.TIA.R1	The Threat Impact Assessment MUST retrieve the most up-to-date "dependency model" associated to the organization, from a module of the PANOPTESEC system responsible for maintaining this knowledge (e.g. Mission Impact Model or Risk Quantification).	Maintain the most up-to-date model of dependency links between Assets, Supporting Assets, and Detrimental Events with their Impact natures and values for the organization.	The identified missions or businesses of an organization evolve during its lifetime for many types of reasons (e.g. new projects start or end, new services are offered to customers implying new ICT services or critical Information storage, businesses are abandoned or transferred to other organisations, etc.). These modifications, captured in a "dependency model", may change the induced Impact of identified threats (i.e. possible or ongoing attack scenarios). The module computing the Impact of threats must capture those changes so that the risks that weight on the organization can be followed as soon as possible.	3	2	2
WP5.TIA.R2	The Threat Impact Assessment MUST retrieve a prioritized list of the most up-to-date possible attack paths (i.e. possible attack scenarios), from the module of the PANOPTESEC system that maintains this knowledge (e.g. Attack Graph Generation or Risk Quantification).	Maintain the up-to-date and prioritized list of possible attack scenarios to be considered for Impact Assessment on a proactive perspective.	During the lifecycle and operation of a monitored system, modification of the possible attack scenarios will occur (e.g. new vulnerabilities are discovered or patched each day, modification and evolution of the infrastructure, possible deployment of new security policy, new identified Entry Points, changes in some priorities for the organization etc.). This may have an impact on the Detrimental Events list that may be potentially caused by those possible attack scenarios.	3	2	2

WP5.TIA.R3	The Threat Impact Assessment MUST retrieve the list of the most up-to-date instantiated attack paths, each representing the current progress of one of the currently detected attackers along one of the identified possible attack paths (i.e. an ongoing attack scenario), from the module of the PANOPTESEC system maintaining this knowledge (e.g. the High Level Online Alert Correlation or Risk Quantification).	Maintain the up-to-date list of ongoing attack scenarios, and attackers, to be considered for Impact Assessment on a reactive perspective.	During the runtime of a monitored system, new ongoing attack scenarios are detected regularly (e.g. new attackers may perform elementary attack actions in sequence to progress along, already existing or new, possible attack paths). This may have an impact on the Detrimental Events list that may be potentially caused by those ongoing attack scenarios. This may have an impact on the Detrimental Events list that may be potentially caused by those ongoing attack scenarios.	3	2	2
WP5.TIA.R4	The Threat Impact Assessment MUST retrieve the up-to-date impact characteristics (e.g. from the parameters of the Base score of CVSS metrics [FRA2014]) of the vulnerabilities present in the target node of identified possible attack paths (i.e. possible attack scenarios) and instantiated attack paths (i.e. ongoing attack scenarios), from the module of the PANOPTESEC system that maintains this knowledge.	Maintain an up-to-date list of vulnerabilities participating in the terminal node of possible and ongoing attack scenarios with their Impact characteristics.	During the lifecycle of vulnerabilities, it may happen that the assessment of their impact nature on the Confidentiality, Integrity and Availability dimensions performed by security experts changes (e.g. when an exploit program begin to circulate on the Internet). It is then required to verify that the vulnerability characteristics are up-to-date.	3	2	2
WP5.TIA.R5	The Threat Impact Assessment MUST compute the Impact characteristics (i.e. magnitude values and natures expressed on Confidentiality, Integrity and Availability dimensions) of the list of Detrimental Events induced by the most up-to-date possible attack scenarios (i.e. possible attack paths) or ongoing attack scenarios (i.e. instantiated attack paths).	Maintain the evaluated Impact characteristics of the list of Detrimental Events on proactive and reactive perspectives.	A module of the PANOPTESEC system has to assess the risks on the organization on both proactive and reactive perspectives. It bases its assessment on the evaluation of the potential Impact of events that are feared by the organization (i.e. Detrimental Events) relating to existing possibilities for attackers to penetrate the monitored or protected systems or existing attackers progressing along attack scenarios.	3	2	2

WP5.TIA.R6	The Threat Impact Assessment MUST notify, as soon as possible, modules of the PANOPESEC system requiring it (i.e. Risk Quantification), that changes have occurred in the Impact characteristics (i.e. magnitude values and natures expressed on Confidentiality, Integrity and Availability dimensions) of the most up-to-date list of Detrimental Events on proactive and reactive perspectives.	Notify, as soon as possible, modules of the PANOPTESEC system requiring it, of changes in the Impact characteristics of the most up-to-date Detrimental Events list on proactive and reactive perspectives have occurred.	Modules of the PANOPTESEC system have to address with Mitigation Actions the most critical risks on the organization on both proactive and reactive perspectives (e.g. Tactical Response Decision and Strategic Response Decision). Modifications in the assessed impact of the Detrimental Events list to be considered occur, which raise risks on the organization to an unacceptable level. In order to address them, the module of the PANOPTESEC system that evaluates the risks on the organization must be updated as soon as possible.	3	2	2
WP5.TIA.R7	The Threat Impact Assessment MUST provide to modules of the PANOPESEC system requesting it (i.e. Risk Quantification), the Impact characteristics (i.e. magnitude values and natures expressed on Confidentiality, Integrity and Availability dimensions) of the most up-to-date list of Detrimental Events on proactive and reactive perspectives.	Serve on demand modules of the PANOPTESEC system requesting it, with the Impact characteristics of the most up-to-date Detrimental Events list on proactive and reactive perspectives.	Modules of the PANOPTESEC system have to address with Mitigation Actions the most critical risks on the organization on both proactive and reactive perspectives (e.g. Tactical Response Decision and Strategic Response Decision). Modifications in the assessed impact of the Detrimental Events list to be considered occur, which raise risks on the organization to an unacceptable level. In order to be able to address them, a module of the PANOPTESEC system that has to reassess the risks on the organization, must periodically request the most up-to-date Impact assessment of the list of Detrimental Events to be considered on both proactive and reactive perspectives.	3	2	2
WP5.TIA.R9	The “dependency model” associated to the organization processed by the Threat Impact Assessment MUST at least express	Maintain the most up-to-date model of dependency links between Assets,	The identified missions or businesses of an organization (i.e. its Assets) rely on technical devices (i.e. Supporting Assets)	3	2	1

	in an abstract way the dependency links between: - Supporting Assets of the monitored systems, - Assets of the organization (i.e. critical services or information for the businesses of an organization, supported by Supporting Assets of the monitored or protected systems), - Detrimental Events that are feared by the organization with the associated nature of the Impact feared by the organization (i.e. on the Confidentiality, the Integrity and the Availability) and an assessed Impact value on the organization (i.e. as it would be assessed in a classical Risk Management process).	Supporting Assets, and Detrimental Events with their Impact natures and values for the organization.	of the monitored system that may incur attacks causing feared events (i.e. Detrimental Events) which produce impacts (i.e. a magnitude and a nature assessed on one or several dimensions of Confidentiality, Integrity or Availability) for the organisation. To be able to assess which possible or ongoing attack scenarios may cause impacts to the organisation, the links between the Assets, the Supporting Assets and the Detrimental Events must be expressed in a structured “dependency model”.			

Non-functional requirements

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.TIA.R8	The Threat Impact Assessment SHOULD protect the possible and ongoing attack scenarios, the “dependency model” entities (e.g. Assets, Supporting Assets, and Detrimental Events), and the computed impact characteristics associated to each Detrimental Events, both within the process memory or during their external storage, from disclosure to unauthorized module or user.	Protect the critical information of monitored or protected system during runtime and storage.	The information provided by other modules of the PANOPTESEC system for the purpose Threat Impact Assessment computation, as well as the various computed impact characteristics associated to Detrimental Events are critical for the organisation. This information could be hijacked by attackers to more accurately target the assets with the most harmful impact. Module that handle and produce this kind of information should apply software temper resistant techniques to protect it during the computing process (e.g. obfuscation) or in case of storage of	2	2	1

			the information (e.g. ciphering) to prevent attackers from exploiting it.			

4.5.3 Response Operational Impact Assessment

Functional requirement

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.ROI.R1	The Response Operational Impact (ROI) Assessment MUST be able to process Response Plans at the Network Layer	Process response plans for network-configuration changes (port, ip, protocol blocking) in order to perform an impact assessment on ongoing business process due to taken actions.	A response plan consists of multiple mitigation actions. Such an action might be that a certain port, protocol or IP address is blocked in the complete network or on individual network nodes. However exactly these connections might be needed for another node to work. As this node might affect the overall mission, this affect must be addressed.	3	2	2
WP5.ROI.R2	The Response Operational Impact (ROI) Assessment MUST be able to process Response Plans at the Software Layer.	Process response plans for vulnerability-topology changes (patching, uninstalling). In order to perform an impact assessment on ongoing business process due to taken actions.	A response plan consists of multiple mitigation actions. Such an action might be that a certain vulnerability is patched. The removal (patching) of a vulnerability is similar to removing the affected software, as both put a change to the vulnerability topology. A patch requires in most cases a restart of a system and therefore leads to a (temporal) unavailability of a service or node. The same holds (but with a longer temporal effect) for uninstalling.	3	2	2
WP5.ROI.R3	The Response Operational Impact (ROI) Assessment MAY predict temporal consequences of Response Plans.	Identify and assess temporal consequences of a response plans, where an impact's merit varies over time.	Certain operations might have temporal effects on the mission or network. E.g. a mitigation action might be fully harmless for a certain amount of time. After a certain amount however it drastically harms the business/mission.	1	3	2

WP5.ROI.R4	The ROI Assessment MUST compute the Operational Impact of Response Plans.	Provide an Operational Impact (OI) for a given hypothetical response plan.	For every layer and node inside the Mission Graph (see [D4.1.1]) the before mentioned impacts are addressed as an Operational Impact. This OI is expressed in a finite range of real numbers.	3	1	2
WP5.ROI.R5	The ROI Assessment SHOULD react to changes of system information of monitored ICT and ICS.	The ROI Assessment SHOULD be performed on the most up-to-date system information of monitored ICT and ICS retrieved in a structured way from a module of the PANOPTESEC system maintaining this knowledge.	Multiple data sources are required for addressing the OI (e.g. System Log Files, Traffic Dumps, PLC Dumps, Firewall Rules & Logs, Configuration Files, Network Topologies, Security Policy Information, Network Historian Information, roles and responsibilities of involved actors, Alarm Response Policies & Logs). These data sources are collected and normalized in a central component of the PANOPTESEC project and might change over time.	3	2	2

Non-functional requirements

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.ROI.R6	The Response Operational Impact Assessment (ROIA) SHOULD scale in a non-exponential way with the number of processed mitigation actions and edges in the network connectivity.	By slight modifications of a given network or a response plan to be processed, the expected response time should scale well with the modifications.	The ROIA should be efficient in various network topologies, ranging from: small up to huge; complex networks, as well as sparsely connected; deep networks, as well as highly connected; and wide networks.	2	3	1
WP5.ROI.R7	The Response Operational Impact Assessment (ROIA) SHOULD accept different performance configurations for processing of a response plan.	Allow a configuration of performance relevant variables in the ROIA algorithms, s.t. potential time constraints are fulfillable.	Some requests for response plan evaluations might be time uncritical and an in-depth analysis is desired. In contrary, some requests might be time critical, e.g. during an ongoing attack, and an evaluation must be done as fast as possible.	2	3	1

4.5.4 Response Financial Impact Assessment

Functional requirements

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.RFI.R1	The Response Financial Impact Assessment MUST provide the financial loss (in monetary values) considering both the consequences incurred by attacks as well as those provided by mitigation actions.	Provide to the Strategic Response Decision the financial impact (in currency per year) of the detected attacks and all of their associated mitigation actions.	Provide the financial impact of attacks and responses to security administrators during the mitigation actions selection process.	3	2	2
WP5.RFI.R2	The Response Financial Impact Assessment MUST provide the annual loss expectancy computed for an organisation considering both the severity and likelihood of the attack.	Provide to the Strategic Response Decision the Annual Loss Expectancy (in currency per year) of the detected attack.	Provide the financial impact of intrusions or attacks to security administrators during the mitigation action selection process.	3	2	2
WP5.RFI.R3	The Response Financial Impact Assessment MUST provide the annual response cost computed for an organisation considering all direct and indirect costs associated to the activation or deactivation of a security mitigation action (e.g., cost of deployment, maintenance, collateral damages).	Provide to the Strategic Response Decision the response cost (in currency per year) of each and every mitigation action associated to the detected attack.	Provide the financial cost of the strategic responses to security administrators during the mitigation action selection process.	3	2	2
WP5.RFI.R4	The Response Financial Impact Assessment MUST provide the annual cost computed for an organisation as a consequence of the maintenance of security equipment (e.g. annual cost of antivirus licenses installed on servers, appliances or workstations).	Provide to the Strategic Response Decision the financial cost (in currency per year) of the security infrastructure.	Provide the periodic financial impact of the current protection level for the organisation to Security Officers and security administrators.	3	2	2

WP5.RFI.R5	The Response Financial Impact Assessment MUST provide the risk mitigation level an organisation has as a result of the execution of a security mitigation action, considering the delta of the financial risk, before and after a mitigation action is executed.	Provide to the Strategic Response Decision the risk mitigation level (in percentage) relative to the current threats, of each and every security mitigation action associated to the detected attack.	Provide the financial benefit of the strategic responses to security administrators during the mitigation action selection process.	3	2	2

Non-functional requirements

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.RFI.R6	The Response Financial Impact Assessment SHOULD determine combinations of mitigation actions in minutes.	Scale the possible combinatorial explosion of potential relationships among the mitigation actions available for the protected system.	Provide the financial benefit of combined mitigation actions.	2	3	1
WP5.RFI.R7	Communication with other PANOPTESEC components SHOULD be encrypted and authenticated.	Keep the data flow information protected against possible eavesdroppers and corruptions.	Communicate by a secure channel to avoid situations in which an attacker may lead the evaluation to wrong results.	2	3	1
WP5.RFI.R8	The module SHOULD ensure the security of the resources associated to the evaluation process in terms of storage and computation.	All the resources associated to the evaluation process must be protected from unauthorized actions.	Guarantee the integrity of the evaluation process to avoid situations in which an attacker may lead the evaluation to wrong results.	2	3	1

4.6 Strategic Response Decision

Functional requirements

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.SRD.R1	The Strategic Response Decision MUST evaluate the list of mitigation actions per potential attack, and obtain the	Provide a list of mitigation actions (ordered by their associated return on security	Response strategies need to select mitigation actions among a group of candidates.	3	2	2

	corresponding RORI value.	investment index) that can best mitigate a potential attack.				
WP5.SRD.R2	The Strategic Response Decision MUST request the RORI evaluation for every individual mitigation action with the inputs provided by the impact assessment.	Provide a list of mitigation actions (ordered by their associated return on security investment index) that can best mitigate a potential attack.	Response strategies need to select mitigation actions among a group of candidates.	3	2	2
WP5.SRD.R3	The Strategic Response Decision MUST determine a threshold (e.g., the average of the RORI index for all the evaluated mitigation actions) to be used as a reference point to select candidates to be combined.	Provide a list of combined mitigation actions that can best mitigate a potential attack.	Response strategies need to consider combined mitigation actions to mitigate a potential attack. The selected combination needs to guarantee the highest return on investment.	3	2	2
WP5.SRD.R4	The Strategic Response Decision MUST evaluate combined mitigation actions that can mitigate a potential attack, with respect to their return on security investment index.	Provide a list of combined mitigation actions that can best mitigate a potential attack.	Response strategies need to select the optimal combination of mitigation actions to mitigate a potential attack.	3	2	2
WP5.SRD.R5	The Strategic Response Decision MUST request approval from the security administrator before deploying the mitigation actions.	Receive a confirmation from the security administrator to deploy selected mitigation actions.	Response strategies need to verify conflicts on the selected mitigation actions before their deployment. A confirmation message is necessary to implement the security policy.	3	2	2

Non-functional requirements

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.SRD.R6	The Strategic Response Decision SHOULD evaluate combinations of mitigation actions in minutes.	Scale the possible combinatorial explosion of potential relationships among the mitigation actions available for the protected system.	Provide the financial benefit of combined mitigation actions.	2	3	1

WP5.SRD.R7	Communication with other PANOPTESEC components SHOULD be encrypted and authenticated.	Keep the data flow information protected against possible eavesdroppers and corruptions.	Communicate by a secure channel to avoid situations in which an attacker may lead the decision to wrong results.	2	3	1
WP5.SRD.R8	The module SHOULD ensure the security of the resources associated to the contextual policies in terms of storage and computation.	All the resources associated to the management of contextual policies must be protected from unauthorized actions.	Guarantee the integrity of the contextual policies to avoid situations in which an attacker may lead the decision to wrong results.	2	3	1

4.6.1 Security Policy Instantiation

Functional Requirements

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.SPI.R1	The Dynamic Risk Management Response System MUST use contextual security rules defined in terms of policy violations.	Definition of actions violating the security policy of the monitored system in terms of monitoring and diagnosis.	Use of contextual policies whose rules are enabled/disabled by using information from attack graphs and high-level alerts.	3	2	2
WP5.SPI.R2	Policy instantiation MUST use contextual policy representations for the activation of rules.	Maintain a prioritized list of policy contexts for which the policy instances can be computed.	Policy instantiation for the activation of responses, so that response policy instances are appropriately derived.	1	2	2
WP5.SPI.R3	Policy instantiation MUST use the most up-to-date state of the policy contexts.	Maintain at any time the up-to-date list of policy contexts for which the policy instances must be computed.	Policy instantiation for the activation of responses, so that response policy instances are appropriately derived.	3	1	2
WP5.SPI.R4	Policy instantiation MUST request the state of policy context updates with a constant frequency (i.e. pull mode).	Maintain at any time the up-to-date list of policy contexts for which the policy instances must be computed.	Policy instantiation for the activation of responses, so that response policy instances are appropriately derived.	1	2	2
WP5.SPI.R5	Policy instantiation MUST be able to receive an up-to-date list of policy contexts at any time (i.e. push mode).	Maintain at any time the up-to-date list of policy contexts for which the policy instances must be computed.	Policy instantiation for the activation of responses, so that response policy instances are appropriately derived.	3	1	2

WP5.SPI.R6	Contextual policy representation MAY use reactive evidences from high-level alerts issued by a HOC (or by a SIEM).	Activation of contextual policy rules according to current diagnosis reported by the high-level alerts issued by a HOC (or by a SIEM).	Provide reactive mitigation according to malicious actions reported via high-level alerts issued by a HOC (or by a SIEM).	1	1	2
WP5.SPI.R7	Contextual policy representation MUST use the proactive evidences from the attack graphs constructed via the PANOPTESEC system.	Activation of contextual policy rules according to potential threats reported by the PANOPTESEC system.	Provide proactive mitigation according to potential threats reported via the PANOPTESEC system (e.g. the AGG function).	3	1	2

Non-functional requirements

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.SPI.R8	Communication with other PANOPTESEC components SHOULD be encrypted and authenticated.	Keep the data flow information protected against possible eavesdroppers and corruptions.	Communicate by a secure channel to avoid situations in which an attacker may lead the instantiation to wrong results.	2	2	1
WP5.SPI.R9	The module SHOULD ensure the security of the resources associated to the instantiation of policies in terms of storage and computation.	All the resources associated to the instantiation of policies must be protected from unauthorized actions.	Guarantee the integrity of the policy instantiation process to avoid situations in which an attacker may lead the instantiation to wrong results.	2	3	1

4.7 Tactical Response Decision

Functional requirements

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.TRD.R1	The Tactical Response Decision MUST retrieve the most up-to-date set of authorized mitigation actions that can be deployed in the system, as well as their associated targeted devices (i.e. the devices on which it can be enforced) and scope in the system (i.e. whether a mitigation action on an enforcement	Maintain the most up-to-date set of mitigation actions authorized for composing a tactical response.	During the security management of a monitored system, the list of mitigation actions that may be deployed to address detected ongoing attack scenarios may change (e.g. new enforcement points, like firewalls or IPS, are deployed, management decision to	3	2	2

	point is authorized for tactical only or for both tactical and strategic response)..		cancel the authorization of a mitigation action kind on a tactical perspective). This may have an impact on the mitigation actions chosen and instantiated as a tactical response to mitigate ongoing attack scenarios. The module that manages tactical responses establishment must be aware of these changes as soon as possible to adapt its computation.			
WP5.TRD.R2	The Tactical Response Decision MUST determine the lists of mitigation actions (i.e. response plans, instantiated from the set of authorized mitigation actions) which deployment can reduce the most up-to-date identified risks on the organization from a reactive perspective (i.e. those induced by ongoing attack scenarios).	Determine the most up-to-date lists of mitigation actions which deployment can reduce the risks on the organization for the reactive perspective (i.e. tactical response plans).	Several mitigation action kinds, authorized on a tactical perspective, may be efficient to block the ongoing attack scenarios. Moreover, a specific mitigation action may also be efficient to block several ongoing attack scenarios inducing different risks for the organization. The module computing tactical responses must then retain among these lists of effective mitigation actions, only those that offer a global risk reduction for the organization. It is also possible that several lists of mitigation actions offer the same level of global risk reduction for the organization. A further process may then be applied to choose the list offering the lowest collateral damage (i.e. impact).	3	2	2

WP5.TRD.R3	The Tactical Response Decision SHOULD sort several lists of mitigation actions (i.e. several tactical response plans), based on their possible impact on the organization.	Determine a (sorted) list of tactical response plans that minimize the impact on the system.	Several lists of efficient mitigation actions (i.e. response plans, instantiated/derived from the set of authorized mitigation actions) may provide different level of global risk reduction on the organization. Moreover, several mitigation action kinds, authorized on a tactical perspective, may be efficient to block the ongoing attack scenarios. It is then possible that several group of lists of mitigation actions offer different level of global risk reduction for the organization. A process should then be applied to help choosing the list offering the lowest collateral damage (i.e. impact) on the organisation.	2	3	2
WP5.TRD.R4	The Tactical Response Decision MUST provide to any module of the PANOPTESEC system requiring it, the currently computed list of mitigation actions selected as the best trade-off between the risk reduction and the impact on the organisation for the tactical perspective (i.e. the selected tactical response plan).	Inform modules of the PANOPTESEC system requesting it, which is the currently selected tactical response plan for deployment.	Several effective lists of mitigation actions may exist with several levels of risk reduction and impact on the organisation. When a decision has been taken (e.g. by an administrator) to deploy one of them, the module responsible of the enforcement of the response plans must be communicated this information as soon as possible to deploy it timely before the risk situation has evolve so that the tactical response plan is no more appropriate.	3	2	2

WP5.TRD.R5	The Tactical Response Decision SHOULD retrieve the up-to-date list of ongoing attack scenarios from a module of the PANOPTESEC system that manage this knowledge.	Maintain an up-to-date list of ongoing attack scenarios.	During the lifecycle of a monitored system, attackers are progressing toward Supporting Assets along attack paths by exploiting successively several vulnerabilities in sequence, potentially causing detrimental events. In order to build accurately and timely the lists of mitigation actions that enable to block those attackers and reduce the risks on the organisation on a reactive perspective (i.e. tactical response plans), it is required to know the up-to-date state of ongoing attack scenarios.	2	1	1
WP5.TRD.R6	The Tactical Response Decision MUST retrieve the up-to-date contribution to the risks on the organisation of the up-to-date list of ongoing attack scenarios.	Maintain an up-to-date assessment of the contribution to each risk that weight on the organisation for each ongoing attack scenarios.	An ongoing attack scenario may contribute to several risks on the organization (i.e. may drive to the compromising of several Supporting Assets then causing several Detrimental Events). This information is required in order to choose accurately and timely the lists of mitigation actions that block ongoing attack scenarios (i.e. tactical response plans) and achieve the highest reduce on risks of the organisation on a reactive perspective.	3	1	1
WP5.TRD.R7	The Tactical Response Decision MUST have the possibility to request to an external module of the PANOPTESEC system to select among several lists of mitigation actions (i.e. tactical response plans) the one that offers the best trade-off between the reduction of risks and the impact on the organization.	Select the list of mitigation actions (i.e. tactical response plan) to be deployed.	Several effective lists of mitigation actions may exist with several levels of risk reduction and impact on the organisation. A decision has to be taken (e.g. by an administrator) to select one of them for deployment.	3	2	1

Non-functional requirements

Id	Description	Goal	Main Purpose	Importance	Reachability	Version
WP5.TRD.R8	The Tactical Response Decision SHOULD propose tactical response plans to mitigate an ongoing attack scenarios in minutes, for a monitored system topology composed of several hundreds of distinct nodes (including routing, firewalling and terminal devices).	Scale the mitigation of ongoing attack scenarios to a medium size monitored system (i.e. up to 500 distinct nodes).	During the lifecycle of and operation of a monitored system, attackers exploit several vulnerabilities in sequence towards a critical asset of an organisation to produce huge damages. Those complex attacks may occur in minutes or hours. The assessment of mitigation actions that may possibly address such kind of attack scenarios on a monitored system should be has fast as possible.	2	2	1
WP5.TRD.R9	The Tactical Response Decision SHOULD protect the ongoing attack scenarios, the contribution to the risks on the organisation of each ongoing attack scenarios, the authorized mitigation actions, and the various computed tactical response plans with their associated reduction on the risks and Operational Impact on the organisation, both within the process memory and during their external storage, from disclosure to unauthorized module or user.	Protect the critical information of monitored or protected system during runtime and storage.	The information provided by other modules of the PANOPTESEC system for the purpose of the Tactical Response Decision, as well as the various computed tactical response plans are critical for the organisation. This information could be hijacked by attackers to walk-around or evade the mitigation actions more efficiently. Modules that handle and produce this kind of information should apply software tamper resistant techniques to protect it during the computing process (e.g. obfuscation) or in case of storage of the information (e.g. ciphering) to prevent attackers' attempts to exploit it.	2	2	1

5. COVERAGE OF SPECIALIZED REQUIREMENTS

The section presents the traceability coverage matrix of the *Specialized Requirements* of the *Response System for the Dynamic Risk Management* which is envisaged in the context WP5 of the PANOPTESEC project, compared to the general Operational Requirements of the project identified in deliverable [D2.1.1]. Section 5.1 deals with the coverage of the Functional Proactive Response System Operational Requirements (i.e. PRS) with the *Functional* Specialized Requirements, while the Section 0 deals with the Functional Reactive System Response Operational Requirements (i.e. RRS) coverage by *Functional* Specialized Requirements. Then, the Section 0, express the coverage of Specialized Requirements of the DRMRS that are of the Non-Functional type over the Non-Functional Operational Requirements, and the applicability of Non-Functional Operational Requirements which are not covered by Specialized Requirements.

These matrices, enables to express the coverage, assessed by WP5, of the Specialized Requirements specified for the DRMRS at the time of the publishing of the D5.1.1 over the Operational Requirements defined in [D2.2.1]. These assessments are further inputted and will be managed using the modelling tool (i.e. a SysML project managed in the purview of the Work Package 3) used by the PANOPTESEC Project in order to further analyse and track in a systematic way the impact in term of coverage of Specialized Requirements of the DRMRS, and any modification of them (following the CM and CC procedure, as described in Section 2.3), on the PANOPTESEC System. As a corollary, these assessments also enable to assess the impacted Specialized Requirements following any modification of Operational Requirement of the Requirement Baseline (RB).

The coverage of each functional requirement is assessed on a 2 level scale: if nothing is indicated, it means the Functional Requirement does not cover the Operational Requirement at all; a cross (“X”) means the Functional Requirement covers the Operational Requirement (i.e. partially or totally). On the bottom of the coverage matrixes, the last line presents a self assessment, performed by the authors of the deliverable, whether the Functional Requirements cover totally (“T) or partially (“P”) the Operational Requirements, if all Functional Requirements were considered.

In each coverage matrixes of Section 5.1, 0 and 0, the requirements are organized in several groups, one for each function (i.e. functional domain) identified in the preliminary high-level functional architecture described in Section 3, and one for the general purpose requirements that are not linked to a specific function but to the global Response System.

5.1 Coverage regarding Proactive Response System (PRS) Operational Requirements

Table 2 - Coverage of DRMRS Functional SRs over PRS Functional ORs

		Proactive Response System (PRS) Functional Operational Requirements																	
		PRS01	PRS02	PRS03	PRS04	PRS05	PRS06	PRS07	PRS08	PRS09	PRS10	PRS11	PRS12	PRS13	PRS14	PRS15	PRS16	PRS17	PRS22
General	WP5.GEN.R1	X	X	X	X	X	X	X	X	X									
	WP5.GEN.R2	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	
	WP5.GEN.R3										X	X	X	X	X	X		X	
Attack Graph Generation	WP5.AGG.R1	X	X	X					X	X				X					
	WP5.AGG.R2	X	X	X	X	X				X				X					
	WP5.AGG.R3	X	X	X			X		X	X				X					
	WP5.AGG.R4	X	X	X					X	X				X					
	WP5.AGG.R5	X	X	X					X	X				X					
	WP5.AGG.R6	X	X	X					X	X				X					
	WP5.AGG.R7	X	X	X	X	X				X				X					
	WP5.AGG.R8	X	X	X					X	X				X					
	WP5.AGG.R9	X	X	X			X		X	X				X					
	WP5.AGG.R10	X	X	X					X	X				X					
	WP5.AGG.R11	X	X											X					
	WP5.AGG.R12	X	X						X					X					
	WP5.AGG.R13	X	X	X				X	X	X	X	X		X					
	WP5.AGG.R14	X	X	X				X		X	X	X		X					
	WP5.AGG.R15	X	X	X				X		X	X	X		X					
	WP5.AGG.R16	X	X				X		X					X					
	WP5.AGG.R17	X	X						X					X					
	WP5.AGG.R20	X	X				X		X					X					
High-level Online	WP5.HOC.R1																		
	WP5. HOC.R2																		
	WP5. HOC.R3																		

	WP5. HOC.R4																	
	WP5. HOC.R5																	
	WP5. HOC.R6																	
	WP5. HOC.R7																	
	WP5. HOC.R8																	
	WP5. HOC.R9																	
	WP5. HOC.R12																	
Potential Attack Identifica	WP5.PAI.R1	X	X	X														
	WP5.PAI.R2	X	X	X														
	WP5.PAI.R3	X																
	WP5.PAI.R4	X																
Risk quantification	WP5.RQU.R1	X						X	X	X	X	X		X				X	
	WP5.RQU.R2	X												X				X	
	WP5.RQU.R3	X						X	X	X	X	X		X				X	
	WP5.RQU.R4																		
	WP5.RQU.R5	X						X	X	X	X	X		X				X	
	WP5.RQU.R6	X						X	X	X	X	X		X				X	
	WP5.RQU.R7	X						X	X	X	X	X		X				X	
	WP5.RQU.R8	X						X	X	X	X	X		X				X	
	WP5.RQU.R9																		
	WP5.RQU.R10	X						X	X	X	X	X		X				X	
	WP5.RQU.R11	X						X	X	X	X	X		X				X	
	WP5.RQU.R12																		
	WP5.RQU.R13	X						X	X	X	X	X		X				X	
	WP5.RQU.R14																		
	WP5.RQU.R15	X						X	X	X	X	X		X				X	
	WP5.RQU.R16	X						X	X	X	X	X		X				X	
	WP5.RQU.R17	X									X	X		X				X	
	WP5.RQU.R18	X									X	X		X				X	
	WP5.RQU.R21	X						X	X	X	X	X		X				X	
k — L	WP5.SLA.R1	X						X		X	X							X	

	WP5.SLA.R2	X						X		X	X							X	
	WP5.SLA.R3	X						X		X	X							X	
	WP5.SLA.R4																		
	WP5.SLA.R5																		
	WP5.SLA.R6	X						X		X	X							X	
	WP5.SLA.R7																		
	WP5.SLA.R8	X						X		X	X							X	
	WP5.SLA.R9	X						X		X	X							X	
	WP5.SLA.R10																		
	WP5.SLA.R11																		
	WP5.SLA.R12	X									X							X	
	WP5.SLA.R13	X									X							X	
Impact Assessment Functional Requirements	WP5.TIA.R1	X						X	X	X	X	X		X					
	WP5.TIA.R2	X						X	X	X	X	X		X					
	WP5.TIA.R3																		
	WP5.TIA.R4	X						X	X	X	X	X		X					
	WP5.TIA.R5	X						X	X	X	X	X		X					
	WP5.TIA.R6	X									X	X		X					
	WP5.TIA.R7	X									X	X		X					
	WP5.TIA.R9	X						X	X	X	X	X		X					
	WP5.ROI.R1								X			X							
	WP5.ROI.R2								X			X							
	WP5.ROI.R3								X			X							
	WP5.ROI.R4								X			X							
	WP5.ROI.R5																		
	WP5.RFI.R1	X																X	
	WP5.RFI.R2	X																X	
	WP5.RFI.R3	X																X	
	WP5.RFI.R4	X																X	
	WP5.RFI.R5	X																X	
Sat	WP5.SRD.R1	X									X	X	X		X	X		X	

	WP5.SRD.R2	X									X	X	X		X	X		X	
	WP5.SRD.R3	X									X	X	X		X	X		X	
	WP5.SRD.R4	X									X	X	X		X	X		X	
	WP5.SRD.R5	X									X	X			X	X		X	
Security Policy Instantiation	WP5.SPI.R1																X	X	X
	WP5. SPI.R2																X	X	X
	WP5. SPI.R3																X	X	X
	WP5. SPI.R4																X	X	X
	WP5. SPI.R5																X	X	X
	WP5. SPI.R6																X	X	X
	WP5. SPI.R7																X	X	X
Tactical Response Decision	WP5.TRD.R1																		
	WP5.TRD.R2																		
	WP5.TRD.R3																		
	WP5.TRD.R4																		
	WP5.TRD.R5																		
	WP5.TRD.R6																		
	WP5.TRD.R7																		
Global coverage ("T" for total coverage; "P" for a partial coverage)		P	T	T	T	T	T	T	T	T	T	T	T	T	T	T	P	T	P

The traceability coverage above enable to verification that most of the PRS Functional Operational Requirements are theoretically covered (totally or partially) by the specified Specialized Requirements of the DRMRS. This matrix also enables to remark that some of the Functional ORs of the *Proactive Response System* domain are not covered totally within the WP5. Nevertheless, those not totally covered ORs are relative to the deployment of Mitigation Actions (i.e. PRS16, PRS22), which explains because this function (i.e. Policy Deployer) has been transferred during the Requirement elicitation process to an *Integration Framework*. This Integration Framework should act as a mediation framework and glue between the sub-systems designed in the purview of WP4, WP5, WP6, the monitored systems. It is design in WP3 and presented extensively in deliverables [D3.1.1] and [D3.1.2].

As not all Functional Operational Requirements are totally covered, the coverage assessment of the PRS01 is not total, even if this is due to a transfer of some requirements to another sub-system of the global PANOPTESEC system.

5.2 Coverage regarding Reactive Response System (RRS) Operational Requirements

Table 3 - Coverage of DRMRS Functional SRs over RRS Functional ORs

		Reactive Response System (RRS) Functional Operational Requirements																					
		RRS01	RRS02	RRS03	RRS04	RRS05	RRS06	RRS07	RRS08	RRS09	RRS10	RRS11	RRS12	RRS13	RRS14	RRS15	RRS16	RRS17	RRS18	RRS23	RRS24	RRS25	RRS26	RRS27
General	WP5.GEN.R1	X	X	X	X	X	X	X	X	X														
	WP5.GEN.R2	X	X	X	X	X	X	X	X	X	X	X	X	X			X		X	X				
	WP5.GEN.R3										X	X	X	X			X		X					
Attack Graph Generation	WP5.AGG.R1	X	X					X	X								X						X	
	WP5.AGG.R2	X	X		X	X		X									X						X	
	WP5.AGG.R3	X	X				X	X									X						X	
	WP5.AGG.R4	X	X					X	X								X						X	
	WP5.AGG.R5	X	X					X	X								X						X	
	WP5.AGG.R6	X	X					X	X								X						X	
	WP5.AGG.R7	X	X		X	X		X									X						X	
	WP5.AGG.R8	X	X					X									X						X	
	WP5.AGG.R9	X	X				X	X									X						X	
	WP5.AGG.R10	X	X					X									X						X	
	WP5.AGG.R11	X		X				X									X						X	
	WP5.AGG.R12	X		X				X									X						X	
	WP5.AGG.R13	X	X					X	X	X	X		X				X					X	X	
	WP5.AGG.R14	X	X					X	X	X	X		X				X					X	X	
	WP5.AGG.R15	X	X					X	X	X	X		X				X					X	X	
	WP5.AGG.R16	X		X				X									X						X	
	WP5.AGG.R17	X		X				X									X						X	
	WP5.AGG.R20	X		X				X									X						X	
High-lev	WP5.HOC.R1	X	X	X				X																
	WP5. HOC.R2	X	X	X				X																

	WP5. HOC.R3	X	X	X															X				X
	WP5. HOC.R4	X	X	X	X		X										X					X		
	WP5. HOC.R5	X	X	X																				
	WP5. HOC.R6	X	X	X																				
	WP5. HOC.R7	X	X	X	X		X											X					X	
	WP5. HOC.R8	X	X	X	X												X	X				X	X	
	WP5. HOC.R9	X	X	X																				X
	WP5. HOC.R12	X	X	X	X																			X
Potential Attack Identifica	WP5.PAI.R1	X																	X				
	WP5.PAI.R2	X																	X				
	WP5.PAI.R3	X																	X				
	WP5.PAI.R4	X																	X				
Risk quantification	WP5.RQU.R1	X	X						X	X	X		X						X					
	WP5.RQU.R2	X	X	X	X	X	X	X		X	X		X						X					
	WP5.RQU.R3																							
	WP5.RQU.R4	X	X	X	X	X	X	X	X	X	X		X						X					
	WP5.RQU.R5	X	X	X	X	X	X	X	X	X	X		X						X					
	WP5.RQU.R6	X	X	X	X	X	X	X	X	X	X		X						X					
	WP5.RQU.R7	X	X						X	X	X		X						X					
	WP5.RQU.R8																							
	WP5.RQU.R9	X	X	X	X	X	X	X	X	X	X		X						X					
	WP5.RQU.R10	X	X	X	X	X	X	X	X	X	X		X						X					
	WP5.RQU.R11	X	X							X	X		X						X					
	WP5.RQU.R12	X	X	X	X	X				X	X		X						X					
	WP5.RQU.R13																							
	WP5.RQU.R14	X	X	X	X	X	X	X	X	X	X		X						X					
	WP5.RQU.R15	X	X	X	X	X	X	X	X	X	X		X						X					
	WP5.RQU.R16	X	X	X	X	X	X	X	X	X	X		X						X					
	WP5.RQU.R17	X	X	X	X	X	X	X		X	X		X						X					
	WP5.RQU.R18	X	X	X	X	X	X	X		X	X		X						X					
	WP5.RQU.R21	X	X						X	X	X		X						X					

Likelihood Assessment	WP5.SLA.R1																							
	WP5.SLA.R2	X	X	X	X	X	X	X		X			X						X					
	WP5.SLA.R3																							
	WP5.SLA.R4	X	X	X	X	X	X	X		X			X						X					
	WP5.SLA.R5	X	X	X	X	X	X	X		X			X						X					
	WP5.SLA.R6																							
	WP5.SLA.R7	X	X	X	X	X	X	X		X			X						X					
	WP5.SLA.R8	X	X	X	X	X	X	X		X			X						X					
	WP5.SLA.R9																							
	WP5.SLA.R10	X	X	X	X	X	X	X		X			X						X					
	WP5.SLA.R11	X	X	X	X	X	X	X		X			X						X					
	WP5.SLA.R12	X	X	X	X	X	X	X		X			X						X					
	WP5.SLA.R13	X	X	X	X	X	X	X		X			X						X					
Impact Assessment Functional Requirements	WP5.TIA.R1	X	X						X	X	X	X												
	WP5. TIA.R2																							
	WP5.TIA.R3	X	X						X	X	X	X												
	WP5.TIA.R4	X	X						X	X	X	X												
	WP5.TIA.R5	X	X						X	X	X	X												
	WP5.TIA.R6	X	X								X	X												
	WP5.TIA.R7	X	X								X	X												
	WP5.TIA.R9	X	X						X	X	X	X												
	WP5.ROI.R1								X		X													
	WP5.ROI.R2								X		X													
	WP5.ROI.R3								X		X													
	WP5.ROI.R4								X		X													
	WP5.ROI.R5																							
	WP5.RFI.R1																							
	WP5.RFI.R2																							
	WP5.RFI.R3																							
	WP5.RFI.R4																							
	WP5.RFI.R5																							

Strategic Response Decision	WP5.SRD.R1																							
	WP5.SRD.R2																							
	WP5.SRD.R3																							
	WP5.SRD.R4																							
	WP5.SRD.R5																							
Security Policy Instantiation	WP5.SPI.R1																		X					
	WP5. SPI.R2																		X					
	WP5. SPI.R3																		X					
	WP5. SPI.R4																		X					
	WP5. SPI.R5																		X					
	WP5. SPI.R6																		X					
	WP5. SPI.R7																		X					
Tactical Response Decision	WP5.TRD.R1	X	X							X		X	X											
	WP5.TRD.R2	X								X			X											
	WP5.TRD.R3	X									X		X											
	WP5.TRD.R4	X								X	X		X		X									
	WP5.TRD.R5	X	X							X			X											
	WP5.TRD.R6	X	X							X			X											
	WP5.TRD.R7												X	X	X									
Global coverage ("T" for total coverage; "P" for a partial coverage)		P	T	T	T	T	T	T	T	T	T	T	T	T	T		T	T	T	T		T	T	T

The traceability coverage matrix presented above enables to verification that most of the RRS Functional Operational Requirements are theoretically covered (totally or partially) by the specified Functional Specialized Requirements of the DRMRS. This matrix also enables to remark that some of the Functional ORs of the *Proactive Response System* domain are not covered within the WP5. Comparably to the coverage of the PRS ORs, the uncovered or partially covered ORs are relative to the deployment of Mitigation Actions (i.e. RRS15, RRS24). This lack of coverage is explained because this function (i.e. Policy Deployer) has been transferred during the Requirement elicitation process to a mediation framework now in the purview of the WP3: the *Integration Framework* (see deliverables [D3.1.1] and [D3.1.2]).

As not all Functional Operational Requirements are totally covered, the coverage assessment of the RRS01 is not total, even if this is due to a transfer of some requirements to another sub-system of the global PANOPTESEC system.

5.3 Non-Functional Operational Requirements analysis

In this section, we provide assessment of the coverage of the Non-Functional Specialized Requirements specified in the present [D5.1.1] deliverable according to the exhausted list of Non-Functional Operational Requirements defined in global PANOPTESEC system in the [2.2.1] deliverable. We also provide an applicability assessment of the Non-Functional Operational Requirement over the defined functional domains of the preliminary Functional Architecture of the Dynamic Risk Management Response System researched and designed in the WP5.

As the Non-Functional Specialized Requirements are specified as additional requirements to precise or give some more specific figures or details according to a defined functional domain of the DRMRS, we indicate in section 5.3.1 the coverage of Non-Functional Specialized Requirements according to the Non-Functional Operational Requirements.

The Non-Functional Specialized Requirements are limited and covers sparsely the exhaustive list of Non-Functional Operational Requirements defined in the [D2.2.1]. Nevertheless, most of those Non-Functional Operational Requirements must apply to the DRMRS in the perspective of the development of an advanced prototype or a product (i.e. between TRL7 and TRL9). An additional assessment of the applicability of the defined Non-Functional Operational Requirements is then provided in Section 5.3.2, which indicates the Non-Functional Operational Requirements which should be considered in the perspective of an industrialization of a DRMRS as specified in the WP5 of the PANOPTESEC project.

These assessments complete the traceability of the DRMRS Specialized Requirements, which are stored and managed in a SysML project in the purview of the Work Package 3.

5.3.1 Coverage regarding Non-Functional Operational Requirements

Table 4 - Coverage of DRMRS Non-Functional SRs over Non-Functional ORs

		GEN				AGG		HOC				PAI		RQU		LA	TIA	ROI		RFI			SPI			SRD		TRD	
		WP5.GEN.R7	WP5.GEN.R6	WP5.GEN.R5	WP5.GEN.R4	WP5.AGG.R18	WP5.AGG.R19	WP5.HOC.R16	WP5.HOC.R15	WP5.HOC.R14	WP5.HOC.R13	WP5.PAI.R6	WP5.PAI.R5	WP5.RQU.R20	WP5.RQU.R19	WP5.SLA.R14	WP5.TIA.R8	WP5.ROI.R7	WP5.ROI.R6	WP5.RFI.R6	WP5.RFI.R7	WP5.RFI.R8	WP5.SRD.R6	WP5.SRD.R7	WP5.SRD.R8	WP5.SPI.R6	WP5.SPI.R7	WP5.TRD.R9	WP5.TRD.R8
Compatibility	CMP001																												
	CMP002																												
	CMP003																												
	CMP004																												
	CMP005	X																											
	CMP006	X																											
	CMP007																												
	CMP008																												
	CMP009	X																											
Maintainability	MNT001																												
	MNT002																												
	MNT003																												
	MNT004																												
Performance	PRF001				X													X		X			X						
	PRF002																												
	PRF003																												
	PRF004				X	X												X	X									X	
	PRF005																												
	PRF006				X				X	X	X	X						X											
	PRF007				X				X	X	X	X						X		X			X						
	PRF008																												

Portability	PRT001																											
	PRT002																											
	PRT003																											
	PRT004																											
	PRT005																											
	PRT006																											
Reliability	RLB001																											
	RLB002																											
	RLB003																											
	RLB004		X																									
	RLB005																											
	RLB006																											
	RLB007			X																								
	RLB008									X																		
	RLB009																											
	RLB0010																											
	RLB0011																											
	RLB0012																											
	RLB0013																											
	RLB0014																											
Security	SEC001						X	X							X	X	X											X
	SEC002																					X			X		X		
	SEC003																				X			X		X			
	SEC004																				X			X		X			
	SEC005																					X			X		X		
	SEC006						X								X	X	X					X			X		X		X
Usability	USG001																												
	USG002																												
	USG003																												

5.3.2 Applicability of Non-Functional Operational Requirements to the DRMRS

The following table assess whether some of the global Non-Function Operational Requirements defined for the global PANOPTESEC system are applicable to a functional domain of the Dynamic Risk Management Response System researched and designed in the WP5. In the following table, we assess the applicability of each Non-Functional Operational Requirement on a two value scale:

- "NA" for *Not Applicable*, means the Non-Functional Operational Requirement is totally inapplicable to the considered functional domain;
- "AP" for *APplicable*, means the Non-Functional Operational Requirement applies to the considered functional domain;

Table 5 - Applicability of Non-Functional ORs for DRMRS functional architecture domains

		GEN	AGG	HOC	PAI	RQU	SLA	TIA	ROI	RFI	SRD	SPI	TRD
Compatibility	CMP001	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	CMP002	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	CMP003	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	CMP004	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	CMP005	AP	NA	AP	AP	NA	NA	NA	NA	NA	AP	NA	NA
	CMP006	AP	NA	AP	NA	NA	NA	NA	NA	NA	AP	NA	NA
	CMP007	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	CMP008	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	CMP009	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
Maintainability	MNT001	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	MNT002	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	MNT003	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	MNT004	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
Performance	PRF001	AP	AP	AP	AP	AP	AP	AP	AP	NA	NA	NA	AP
	PRF002	AP	NA	AP	NA	NA	NA	NA	NA	NA	NA	NA	NA
	PRF003	AP	NA	AP	AP	NA	NA	NA	NA	NA	NA	NA	NA
	PRF004	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	PRF005	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	PRF006	AP	NA	AP	NA	AP	AP	AP	AP	AP	AP	AP	AP
	PRF007	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	NA
	PRF008	AP	NA	NA	NA	NA	NA	NA	AP	AP	AP	AP	AP

Portability	PRT001	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	PRT002	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	PRT003	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	PRT004	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	PRT005	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	PRT006	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
Reliability	RLB001	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	RLB002	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	RLB003	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	RLB004	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	RLB005	AP	NA	AP	AP	NA	NA	NA	NA	AP	AP	AP	NA
	RLB006	AP	NA	AP	AP	NA	NA	NA	NA	AP	AP	AP	NA
	RLB007	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	RLB008	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	RLB009	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	RLB0010	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	RLB0011	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	RLB0012	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	RLB0013	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	RLB0014	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
Security	SEC001	AP	AP	AP	AP	AP	AP	AP	AP	NA	NA	NA	AP
	SEC002	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	SEC003	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	SEC004	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
	SEC005	AP	AP	NA	NA	AP	AP	AP	AP	AP	AP	AP	AP
	SEC006	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
Usability	USG001	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
	USG002	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
	USG003	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA

6. CONCLUSION

6.1 Significant results achieved

In this document, we presented the preliminary high-level Functional Architecture for the Dynamic Risk Management Response System of Monitored Systems, as it is envisaged by the Partners of the WP5 of the PANOPTESEC Project.

A list of Specialized Requirements for each identified function of the DRMRS has been proposed. And, the coverage of those Specialized Requirements over the Operational Requirements previously identified within WP2 of the PANOPTESEC project, has been provided for the PRS and RRS relevant domains (i.e. *Proactive Response System* and *Reactive Response System*).

The traceability coverage matrices in Section 5 enable verification that most of the Operational Requirements are theoretically covered (totally or partially) by the proposed DRMRS. But, they also enable to remark that some of the Operational Requirements of the PRS and RRS domains are not fully covered within the WP5. Nevertheless, those uncovered Functional Operational Requirements are relative the deployment of Mitigation Actions (i.e. PRS16, PRS22, RRS15, and RRS24). This lack of coverage is explained because this function (i.e. Policy Deployer) has been transferred during the Requirement elicitation process to a mediation framework now in the purview of the WP3: the *Integration Framework* (see deliverables [D3.1.1] and [D3.1.2]).

6.2 Recommendations

These matrices also constitute the basis to input the coverage of SRs using a modelling formalism (i.e. SysML) and a tool (i.e. Papyrus) for the systematic management of the PANOPTESEC Requirement Baseline within the Work Package 3. It then should enable the further analysis and traceability in the remainder of the project during the design, implementation and validation phases.

These Specialized Requirements should constitute a reference for the WP5 and the PANOPTESEC Project that ensures that the PANOPTESEC Consortium share a common understanding of the objectives of the WP5. The Specialized Requirements should help in the following of the Project to identify and detail the software components, with consistent and well-defined interfaces (i.e. internal and external ones) in the D5.1.2 and other Work Packages design documents. These requirements should be used to trace, guide (i.e. prioritize, decide) and evaluate the outcomes of the WP5 in the remainder of the PANOPTESEC Project.

6.3 Deliverable validation

The content of this deliverable has been validated at several levels. First, internal WP5 validation (i.e. both by WP5 Primes and the WPL) of the content has been carried out all along the writing process on a periodic basis. Then, a two Review phases QA validation occurred before the publishing of the final version of the D5.1.1 deliverable.

7. REFERENCES

[DoW2013] PANOPTESEC Consortium – *"Annex I - Description of Work"* – European Union Seventh Framework Programme, DoW of the PANOPTESEC project, Grant Agreement no: 610416, 19 Sep 2013.

[D2.1.1] PANOPTESEC Consortium - *"Deficiency Evaluation"* - Project deliverable D2.1.1, version 1.0, April 30th, 2014.

[D2.2.1] PANOPTESEC Consortium - *"Operational Requirements Analysis"* - Project deliverable D2.2.1, version 2.0, March 27th, 2015.

[D3.1.1] PANOPTESEC Consortium - *"System High-Level Preliminary Design"* - Project deliverable D3.1.1, version 1.0, April 30th, 2014.

[D4.1.1] PANOPTESEC Consortium – *"Data Collection and Correlation Functional Requirements"* – Project deliverable D4.1.1, version 1.2, October 31th 2014.

[D4.1.2] PANOPTESEC Consortium – *"Data Collection and Correlation Component Design"* – Project deliverable D4.1.2, version 1.0, October 31th 2014.

[PH15] PANOPTESEC Consortium – "PANOPTESEC Project Handbook" – Project internal document, version 0.1, March 27th 2015.

[QAS15] PANOPTESEC Consortium – "PANOPTESEC QA Schedule" - Project internal document, available online at https://gotika.ifis.uni-luebeck.de/panoptesec/WP01/Project%20Handbook/Quality%20Assurance/QA%20Schedule

[ETSI2006] ETSI, TISPAN, Methods and protocols - *"Method and proforma for Threat, Risk, Vulnerability Analysis"* - ETSI TS 102 165-1, v4.2.1, Dec. 2006, available online at http://portal.etsi.org/mbs/Referenced%20Documents/ts_10216501v040201p.pdf.

[ISO2013] ISO/IEC International Standard - *"Information technology - Security techniques - Information security management systems - Requirements"* - ISO/IEC 27001:2013, Version 25 Sep. 2013

[NIST2013] National Institute of Standards and Technology – *"Information Security - Guide for Conducting Risk Assessments"* - Computer Security Division, Information Technology Laboratory, NIST Special Publication 800-30, Revision 1, Sep 2013, available online at http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

[ABO03] Abou-El-Kalam, A., Baida, R., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miège, A., Saurel, C., Trouessin, G. - "Organization Based Access Control" - In: IEEE 4th International Workshop on Policies for Distributed Systems and Networks. (2003) 120–131.

[ABO05] Abou-El-Kalam, A., Briffaut, J., Toinard, C., and Blanc, M. - *"Intrusion Detection and Security Policy Framework for Distributed Environments"* - In *Collaborative Technologies and Systems* (2005), pages 100–106, Missouri, USA.

[ANSSI2011] ANSSI, Agence nationale de la sécurité des systèmes d'information – *"EBIOS - Expression des Besoins et Identification des Objectifs de Sécurité"* - Sous-direction assistance, conseil et expertise, Bureau assistance et conseil, January 25th 2011, France, avialable online at http://www.ssi.gouv.fr/IMG/pdf/EBIOS-1-GuideMethodologique-2010-01-25.pdf.

[AUT09] Autrel, F., Cuppens, F., Cuppens-Boulahia, N. – *"Reaction Policy Model Based on Dynamic Organizations and Threat Context"* - In *23rd Annual IFIP WG 11.3 Working Conference* (2009), pages 49-64, Montreal, Canada.

[BAR99] Bartal, Y., Mayer, A., Nissim, K., and Wool, A. – *"Firmato: A novel firewall management toolkit"* - In *IEEE Symposium on Security and Privacy* (1999), pages 17–31, Oakland, USA.

[BER1738] Daniel Bernoulli - *"Exposition of a New Theory on the Measurement of Risk"* – In Econometrica, Vol. 22, No. 1. , pp. 23-36, Jan, 1954; from Daniel Bernoulli – *"Specimen Theoriae Novae de Mensura Sortis"* - Commentarii Academiae Scientiarum Imperialis Petropolitanae, Tomus V [Papers of the Imperial Academy of Science in Petersburg, Vol. V], pp. 175-192, 1738; available online at http://links.jstor.org/sici?sici=0012-9682%28195401%2922%3A1%3C23%3AEOANTO%3E2.0.CO%3B2-X.

[BINZEL2000] Binzel, Richard P. – *"The Torino Impact Hazard Scale"* – in Elsevier *Planetary and Space Science*, Volume 48, Issue 4, Pages 297–303, April 1st, 2000.

[BLA04] Blanc, M., Clemente, P., Courtieu, P., Franche, S., Oudot, L., Toinard, C., and Vessiller, L. - "Hardening large-scale networks security through a metapolicy framework" - In *3rd Workshop on the Internet, Telecommunications and Signal Processing* (2004), pages 132-137, Adelaide, Australia.

[CFRA2014] Joshua Franklin, Charles Wergin, Harold Booth – "CVSS Implementation Guidance" – NIST, Computer Security Division, Information Technology Laboratory, NISTIR 7946, Apr 2014, available online at http://dx.doi.org/10.6028/NIST.IR.7946.

[CLUSIF2010] CLUSIF, CLUb de la Sécurité de l'Information Français – *"MEHARI 2010 - Fundamental concepts and functional specifications Mehari"* - Methods Commission, August 2010, avialble online at http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Principles-Specifications.pdf.

[CM2002] Frédéric Cuppens and Alexandre Miège – "Alert correlation in a cooperative intrusion detection framework" - In Proceedings of the IEEE Symposium on Security and Privacy, pages 202–215, 2002.

[CUP06] Cuppens, F., Autrel, F., Bouzida, Y., Garcia-Alfaro, J., Gombault, S., Sans, T. – "Anti-correlation as a criterion to select appropriate counter-measures in an intrusion detection framework" - *Annals of Telecommunications* (2006)*, 61(1-2):197-217*.

[END1995] Endsley, Mica R. - *"Toward a theory of situation awareness in dynamic systems."* - Human Factors: The Journal of the Human Factors and Ergonomics Society, vol. 37, no. 1; March 1995, pp 32-64.

[GLO2008] Jean Goubault-Larrecq and Julien Olivain – "A smell of orchids" - In Runtime Verification, volume 5289 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2008.

[GON13] Gonzalez Granadillo, Gustavo - *"Optimization of Cost-based threat response for Security Information and Event Management (SIEM) systems"* - PhD thesis, Télécom SudParis and University Pierre et Mary Curie, 2013.

[GON14] Gustavo Gonzalez Granadillo, Malek Belhaouane, Hervé Debar, Grégoire Jacob - *"RORI-based countermeasure selection using the OrBAC formalism"* – International Journal of Information Security, ISSN 1615-5262 Int. J. Inf. Secur. DOI 10.1007/s10207-013-0207-8, Springer 2014, 13:63-79.

[HAC13] Hachem, N., Garcia-Alfaro, J., Debar, H. – "An Adaptive Mitigation Framework for Handling Suspicious Network Flows via MPLS Policies" - In *18th Nordic Conference on Secure IT Systems* (2013), pages 297-312, Ilulissat, Greenland.

[HUY1657] Huygens, Christiaan – *"The values of all chances"* - In "Games of Fortune; Cards, Dice, Wagers, Lotteries, &c - Mathematically Demonstrated", Printed by S. Keimer for T. Woodward, near the Inner-Temple-Gate in Fleetstreet, London, UK, 1714; from Christiaan Huygens' *"De Ratiociniis in Ludo Aleae"* which was published in Latin in 1657; available online at http://www.math.dartmouth.edu/~doyle/docs/huygens/huygens.pdf.

[ING2006] K. Ingols, R. Lippmann, and K. Piwowarski – *"Practical attack graph generation for network defense"* - In proceedings of the 22nd Annual Computer Security Applications Conference (ACSAC '06), Washington, D.C.: IEEE Computer Society, pp. 121–130, 2006.

[JAJ2005] S. Jajodia, S. Noel, and B. O'Berry – *"Topological analysis of network attack vulnerability"* - In V. Kumar, J. Srivastava, and A. Lazarevic, editors, Managing Cyber Threats: Issues, Approaches and Challenges, chapter 5. Kluwer Academic Publisher, 2005.

[KAN10] Kanoun, W., Cuppens-Boulahia, N., Cuppens, F., Dubus, S. – "Risk-Aware Framework for Activating and Deactivating Policy-Based Response" - In 4th International Conference on Network and System Security (NSS 2010), pages 207-215, Melbourne, Australia.

[KAN11] Kanoun, W. – "*Intelligent Risk-Aware System for Activating and Deactivating Policy-Based Response.* Ph.D thesis, Université européenne de Bretagne (2011).

[KHE10] Kheir, Nizar - *"Response Policies and Countermeasures: Management of Service Dependencies and Instrusion and Reaction Impacts"* – Ph.D thesis, Ecole Normale Supérieure des Télécommunications de Bretagne, France, 2010.

[KIS11] Kissel, Richard - *"Glossary of key information security terms"* - National Institute of Standards and Technology, U.S. Department of Commerce, 2011.

[KOS11] Kosutic, Dejan - "*Is it possible to calculate the Return on Security Investment (ROSI)?"* - In http://blog.iso27001standard.com/2011/06/13/is-it-possible-to-calculate-the-return-on-security-investment-rosi/, 2011

[LAB07] Laborde, R., Kamel, M., Barrére, F., and Benzekri, A. – "Implementation of a Formal Security Policy Refinement Process in WBEM Architecture" - *Journal of Network and Systems Management* (2007), 15(2):241-266.

[LOC04] Lockstep Consulting - *"A Guide for Government Agencies Calculating ROSI" - Technical Report*, http://lockstep.com.au/library/return_on_investment, 2004.

[MIE05] Miège, Alexandre -*"Definition of a formal framework for specifying security policies. The OrBAC model and extensions"* - PhD thesis, Ecole Nationale Superieure des Télécommunications, Paris, 2005.

[MON00] Mont, M. C., Baldwin, A., and Goh, C. – "POWER prototype: towards integrated policy-based management. In *Network Operations and Management Symposium* (2000), pages 789–802, Honolulu, HI, USA.

[OU2004] X. Ou, S. Govindavajhala, and A. W. Appel. – *"MulVAL: A logic-based network security analyzer"* - In 14th USENIX Security Symposium, Baltimore, MD, USA, August 2005.

[RFC2119] Bradner, Scott - "Key words for use in RFCs to Indicate Requirement Levels" – IETF, Networking Working Group, RFC2119, Best Current Practice (BCP 14), March 1997, available online at: https://www.ietf.org/rfc/rfc2119.txt

[ROE2012] Roebuck, Kevin – "Decision Theory: High-impact Strategies - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors" - Emereo Publishing, 2012.

[SHE2002] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing – *"Automated generation and analysis of attack graphs"* - In Proceedings of the 2002 IEEE Symposium on Security and Privacy, Oakland, California, USA, pages 254–265, 2002.

[SMD2013] Saeed Salah, Gabriel Maciá-Fernández, and Jesús E Díaz-Verdejo – "A model-based survey of alert correlation techniques" - Computer Networks, 2013.

[TVM2004] Eric Totel, Bernard Vivinis, and Ludovic Mé – "A Language Driven Intrusion Detection System for Event and Alert Correlation" - In Proceedings of the 19th IFIP International

Information Security Conference, pages 209–224, Toulouse, August 2004. Kluwer Academic.