FP7-610416-PANOPTESEC

Dynamic Risk Approaches for Automated Cyber Defence

D6.1.1: Visualization Component Requirements

Work-Package	WP6	Deliverable	D6.1.1
Due Date	27-03-2015	Submission Date	27-03-2015
Main Author(s)	Marco Angelini, Giuseppe Santucci (CIS-UROME)		
Contributors	All project participants		
Version	V2.0	Status	Final
Dissemination Level	PU	Nature	R
Keywords	Functional and non-functional Requirements, Visualization, Visual Analytics, D2.2.1		

Part of the Seventh

Framework Programme

Funded by the EC - DG Connect

EXECUTIVE SUMMARY

The overall goal of WP6 - Visual Analytics and Display - is to design, develop, and validate an innovative visual analytics environment for analysing and monitoring the PANOPTESEC system model, the attack model, and the actual and historical cyber defence related network data. In addition to that, the visualization component has to show the automatic decisions proposed by the proactive and reactive systems, together with the matching between the actual network state and the closest attack model. The final goal of the visualization component is to support different user roles to accomplish their tasks, ranging from the network administrator activities to the top management decisions.

This deliverable describes the functional and non-functional requirements for the visualization component, refining the operational requirements, the non-functional requirements, and the user roles described in [D2.2.1]. In particular, the deliverable characterizes the user skills, information needs, and tasks to group of user activities in four main groups that are used to categorize the visualization component requirements. This categorization has allowed for collecting requirements in a more structured and focused way and will foster the modularity of the visualization component design and implementation.

Requirements are organized in a hierarchical fashion and are prioritized according to their importance and reachability (see [D2.2.1], Section 2.3). Requirements have been collected using the user centered methodology (UCD) described in [D2.2.1], Section 2, and validated by assessing them against a checklist of possible issues (see [D2.2.1], Section 2.6) and checking their coverage with respect to the operational requirements.

These functional requirements will constitute a reference for the WP6 PANOPTESEC work package to design the visualization component that, according to the result of this deliverable, will encompass four subsystems.

HISTORY

Version	Date	Name/Partner	Comment
0.1	25-08-2014	Giuseppe Santucci/CIS-UROME	First draft with table of content, and operational requirements
0.5	22-09-2014	Giuseppe Santucci/CIS-UROME Nicolas Prigent/SUPELEC	Refinement of table of content, refinement of operational requirements, added list of functional requirements with coverage of operational requirements
0.8	6-10-2014	Giuseppe Santucci/CIS-UROME Marco Angelini/CIS-UROME Nicolas Prigent/SUPELEC	Refinement and review of functional requirements. Expansion of functional requirements in sub-requirements
1.0	16-10-2014	Giuseppe Santucci/CIS-UROME Nicolas Prigent/SUPELEC	Trimming of functional and sub-requirements. Incorporating some partners' comments and contributions.
1.0a	30-10-2014	Giuseppe Santucci/CIS-UROME Nicolas Prigent/SUPELEC Douglas Wiemer/RHEA	Revising names and trimming requirements. Incorporating some partners' comments and contributions. FINAL VERSION – SUBMITTED TO THE COMMISSION
V1.1	1-03-2015	Giuseppe Santucci/CIS-UROME	First draft for the new version due on 27-03-215
V1.2	05-03-2015	Giuseppe Santucci/CIS-UROME	Initial creation of the document in the correct template.
V1.3	06-03-2015	Giuseppe Santucci/CIS-UROME	Revised versioning numbering, improved executive summary, methodology, draft of user characterization
v1.4	12-03-2015	Giuseppe Santucci/CIS-UROME	Revised requirement template. Added first version of non-functional requirements.
V1.5	13-03-2015	Giuseppe Santucci/CIS-UROME	Full characterization of user roles/skill/ and system activities
V1.6	13-03-2015	Giuseppe Santucci/CIS-UROME	Added functional requirements for executive level. New coverage matrix

V1.7	15-03-2015	Giuseppe Santucci/CIS-UROME	Added functional requirements for handling historical data. New coverage matrix. Document ready for the first QA cycle.
V1.8	19-03-2015	Giuseppe Santucci/CIS-UROME Doug Wiemer/RHEA Alexander Motzek	Comments, typos fixing. Improved Document history (including releases of the previous document). Incorporating reviewer comments on functional requirements.
V1.8.1	21-03-2015	Giuseppe Santucci/CIS-UROME	Comments, typos fixing. Incorporating reviewer comments on non-functional requirements.
V1.9	21-03-2015	Giuseppe Santucci/CIS-UROME	Comments, typos fixing.
V2.0	26-03-2015	Giuseppe Santucci/CIS-UROME	Added Conclusions. Document ready for the second QA cycle.

TABLE OF CONTENTS

LIST OF TABLES

ACRONYMS AND DEFINITIONS

Table 1: Acronym List

Acronym	Meaning
ACEA	ACEA S.p.A.
ADD	Attribute-Driven Design
ALBLF	Alcatel-Lucent Bell Labs France
ANM	System analysis and administration
ARM	Reactive security response managing
CDSA	Cyber defence situation awareness
CIS-UROME	Università Degli Studi Di Roma La Sapienza
EPIST	Epistematica SRL
GEN	General
HLM	High Level Monitoring
ICT	Information and Communication Technology
IDS	Intrusion detection system
IMT	Institut Mines-Telecom
Infovis	Information Visualization
MON	Monitoring
QA	Quality assurance
QR	Quality review
RHEA	RHEA System S.A.
ROI	Return of investment
SCADA	Supervisory Control And Data Acquisition
SDLC	Software development life cycle
SUPELEC	Ecole Supérieure D'Électricité
UCD	User-centered design
UoL	Universität zu Lübeck
VA	Visual Analytics

1 INTRODUCTION

1.1 Context

The PANOPTESEC system is a cyber-defence decision support system aiming at demonstrating a risk based approach to automated cyber defence. The high degree of innovation of the system, the complexity of the managed data, and the different user roles and tasks pushes for challenging requirements for the visual user interface of the systems, in terms of ad-hoc visualizations, adaptation, scalability, and interaction modalities. Collecting and detailing such requirements is central to the PANOPTESEC system and is the focus of this deliverable.

1.2 Purpose

This deliverable has two main purposes:

1. To group user roles and tasks described in [D2.2.1], Section 5, in homogenous activity classes, useful for grouping requirements for the visualization component and leading to a modular architecture;
2. Establishing and detailing the functional and non-functional requirements of the visualization component.

This deliverable will then be used all along the project to drive the visualization component design and implementation.

1.3 Scope

The scope of this deliverable includes the description of user task, roles, and skill with respect to the identified four main activity classes, the description of the identified visual functional and non-functional requirements, showing their coverage with respect to the visual operational requirements described in [D2.2.1], Section 7.5.

1.4 Document Structure

This D6.1.1 deliverable is structured in the following manner:

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

Section 2 Methodology: describes the methodology followed in the development of the deliverable

Section 3 Characterizing visual requirements according to User tasks, skills, and roles: groups functional requirements according to user roles.

Section 4 Functional requirements: lists the functional requirements for the Visualization component.

Section 5 Non-functional requirements: lists the non-functional requirements for the visualization component.

Section 6 Coverage of Operational Visualization Requirements: shows the dependencies among functional requirements and operational requirements.

Section 7 Conclusion: summarizes the findings, results and recommendations.

2 METHODOLOGY

For requirements collection and validation this deliverable uses the user-centered design (UCD) methodology described on [D2.2.1], Section 2. According to the underlying spiral life cycle model, several iterations have been completed and others will take place along the rest of the project. The specificity of the visualization component and its key role in the PANOPTESEC system have been taken into account by classifying user roles according to the visualizations and interaction modalities they were needing. Moreover, the early prototyping of some visualization components, either by working prototypes or mock-ups, has contributed to actively involve the users in requirement collection and validation and in the early design activities.

2.1 Information collection

The main source of information for this document are the visual operational requirements [D2.2.1] that provides a high level description of the user skill, characteristics, and needs (functional and non-functional). Other source of information are the PANOPTESEC Description of work and the analysis of deficiency [D2.1.1].

2.2 Information analysis

The analysis started from visual operational requirements and user scenarios described in [D2.2.1]. The available information has been analysed considering user roles, skills and visual operational requirements, identifying visual functional requirements useful for uniform groups of user activities according to their informative needs and tasks. Along this phase, during several meetings at the ACEA premises, ACEA technicians and managers have collaborated with WP6 researchers in defining, validating, and refining both user group activities classification and functional and non functional requirements.

2.3 Synthesis of results

This report defines four main user activity groups (Section 3) and five classes of visual requirements (Section 4), one general and four corresponding to the four groups of activities defined on Section 3. Moreover, relevant non-functional requirements (Section 5) have been selected according to [D2.2.1] Section 5.

According to [D2.2.1] two values, importance and reachability, have been associated to each requirement. As its name implies, the Importance value describes the importance of a requirement with respect to the success of the PANOPTESEC project. Importance is rated from 1 to 3. These three values can be matched to the MAY (1), SHOULD (2) and MUST (3) key words according to RFC 2119 [Bra97]. 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 to prioritize research and development.

In addition to that, visual functional requirements are arranged in a hierarchical fashion. The adopted naming convention is the following:

Root requirement **x**:	WP6.<requirement class name>.R**x**
Sub requirement **y** of root requirement **x**:	WP6.<requirement class name>.R**x**.SR**y**

where <requirement class name> ranges on GEN (general), ANM (system analysis and administration), MON (system monitoring), ARM (Reactive security response managing), HLM (high-level monitoring).

The whole process has produced 20 root functional requirements, 66 sub requirements, and 17 non functional requirements.

Each requirement is described with:

- **Requirement id**: a unique identifier, that must be used for the traceability and management of the requirement across the PANOPTESEC project;
- **Version**: it provides a means to track changes to requirements and enables reference to compare past versions with current versions for traceability;
- **Description**: A plaintext description of the requirement;
- **Goal**: it expresses the objective of the function addressed by the defined requirement;
- **Main purpose** : gives possible explanation on the context of use of a function that addresses the requirement;
- **Importance**: The priority or importance of the requirement for the PANOPTESEC project defined with three levels: “3” (MUST) means critical for the project; “2” (SHOULD) means important; and “1” (MAY) means unimportant (i.e., nice to have);
- **Reachability**: The Reachability describes the relative amount of research or development effort that is estimated to fulfil 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.

2.4 Validation

User activities grouping has been validated by ACEA people during their definition of user scenarios through several meetings and discussions.

Requirements (functional and non-functional) have been validated by selected members of ACEA and PANOPTESEC participants, using the methodology described in [D2.2.1], Section 2.6, using a Quality Review (QR) conducted using the quality criteria established in [D2.2.1]. According to the specific nature of the visualization component, a demonstration of existing prototypes or mock-ups has been given to the participants to the QR.

Any contradictory issues have been discussed according to their nature:

1. Internal technical issues have been discussed and solved within WP6 researchers and PANOPTESEC partners;
2. Issues involving Acea (e.g., ambiguities, contradictions, etc.) have been solved interacting with Acea users.

Results coming from such activities have been propagated on requirements and the two steps have been iterated until step 1 was not raising significant issues.

The coverage of operational requirements has been analysed and assessed by associating each functional requirement to the satisfied operational requirement(s), producing the coverage matrix reported on Section 6.

3 CHARACTERIZING VISUAL REQUIREMENTS ACCORDING TO USER TASKS, SKILLS, AND ROLES

According to PANOPTESEC operational requirements [D.2.1], users have been classified using six roles:

1) **Security Operator:** Primary users of the PANOPTESEC system. Operators have both proactive and reactive responsibilities. Proactive functions include reviewing vulnerabilities within the monitored system, reviewing potential mission impact, review and selection of mitigation actions and their execution. Reactive functions include reviewing indications of suspected cyber attacks, reviewing potential mission impacts, review and selection of mitigation actions and approval of execution;
2) **Network Operator:** In some instances, the approved mitigation actions executed by PANOPTESEC will require intervention on the part of Network Operator staff to implement the chosen mitigation action (e.g., implementation of patches or making changes to system configuration changes);
3) **PANOPTESEC System Manager:** Involved in setup and configuration of the data sensors interface with the PANOPTESEC system as well as any pre-configuration or configuration changes needed by the PANOPTESEC system (e.g., input the list of pre-approved mitigation actions);
4) **SCADA Operator:** Users involved in management of the SCADA devices and environment;
5) **ICT Operator:** Users involved in management of the ICT devices and environment;
6) **Business Owner:** Executive level function within the organisation and interested in understanding the security status of the business (mission) processes and possible business impact due to possible or ongoing cyber-attack;

In the following subsections, we classify user skills and information needs with respect to visual requirements, grouping them in homogeneous classes.

3.1 User skills and information needs

User roles 1, 2, and 3 have similar skills and information needs. They understand the different network topology layers (1,2,3) and have a good knowledge of the hardware and the software that is used within the ACEA environment. They know the problems raised by vulnerabilities, the associated risk, the critical assets, and the impact on the mission. Their tasks include the maintenance of the network, the assessment of proactive mitigation action, the monitoring of the network in terms of instantiated attack paths, device failures, risk and mission impact. If a response plan is triggered by the PANOPTESEC system a security operator that is monitoring the system is called to make decisions on the actual response plan. To accomplish this task he needs to be quickly provided with information supporting cyber situation awareness that, according to [Bar10], encompasses seven main aspects:

1) Be aware of the current situation. This aspect includes recognizing that an attack is occurring and identifying it (e.g., instantiated attack paths);
2) Be aware of the impact of the attack. This aspect includes the assessment of current impact and the assessment of future impact (e.g., through vulnerability analysis);
3) Be aware of how the situation evolves (e.g., inspecting a timeline showing the progress of an attack);

4) Be aware of attack behaviour, identifying attack trends and intents (out of the PANOPTESEC scope);
5) Be aware of why and how the current situation is caused, doing causality analysis and forensics (mostly out of the PANOPTESEC scope);
6) Be aware of the quality and trustworthiness of the collected situation awareness (mostly out of the PANOPTESEC scope);
7) Assess plausible futures of the current situation, understanding attackers' skills and goals (out of the PANOPTESEC scope) and internal vulnerabilities and available mitigation actions.

To accomplish this, the security operator requires information about several complementary aspects: the understanding of the network status (addressing aspect 1); the consequences that the actual situation has on the mission supported by the monitored system (addressing aspect 2), browsing the evolution of the situation (addressing aspect 3), the instantiated attack paths (partially addressing aspect 4), and the anticipated mission impact (partially addressing aspect 7).

Moreover, visual information must to be presented to the user in "real time", i.e., respecting a time constraint between the time a critical information is sent to visualization component (e.g., the triggering of a response plan) and its visual rendering and user alerting. According to the ACEA technicians, a delay up to four seconds is in line with their security objectives. This time constraint does not include the time needed to compute the information, activity that is out of the scope of the visualization component.

User roles 4 and 5 are more device oriented: they have still a good understanding of the ACEA environment but they are specialized in dealing with specific devices. They are required to fix issues on the target machines, and the basic information they need is the location of the machine, the issue they have to deal with and the mitigation actions selected by the Security Operator.

User role 6 is a non-technical role. Users belonging to this role deal with high-level decision making and planning. They need aggregated and simple information about risk, mission impact, and financial impact, e.g., RORI (return of investment).

3.2 User groups and system visual interfaces functionalities

In order to group requirements in homogeneous classes we consider the following macro activities that are in a many-to-many relationship with user roles: a macro activity represents a set of standard operations that may involve many user roles; conversely, a user role may be involved in many macro activities.

1. **System analysis and administration**. This activity foresees to inspect the network structure, examine vulnerabilities and attack paths, proposed patches, feed the system with required information, examine potential business or mission impacts, manage the proactive security response, reviewing and selecting mitigation actions, etc. User roles involved in this activity are:
    - PANOPTESEC System Manager – involved in setup and configuration of the data sensors for the PANOPTESEC system;
    - Security Operator – reviewing vulnerabilities, assessing potential mission impact, reviewing and selecting mitigation proactively proposed according to the business risk;

- Network Operator – involved in implementation of patches and making changes to system configurations;
- SCADA Operator: involved in implementation of patches and making changes to SCADA devices;
- ICT Operator: involved in implementation of patches and making changes to ICT devices;

2. **System monitoring**. This activity refers to the monitoring of the network actual state in terms of risk, mission impact, topology (layer 3) and geography, in order to propose mitigation actions and share information about the situation. User roles involved in this activity are:
   - Security Operator – monitoring the risk level, network behaviour, alerts, mission impact and geographical situation, and managing the risk, sharing information and communicating with other operators;
3. **Reactive security response managing.** This activity consists of observing the mission impact of the ongoing attack, inspecting the proposed response plan, approving or denying the execution of the response plan and selecting single mitigation actions for observing the effect of the running execution plan and its impact on the mission, and where possible, stopping its execution if something is wrong. User roles involved in this activity are:
   - Security Operator – monitoring the impact of the attack and of the response plan in order to make quick, reactive decisions;
4. **High-level system monitoring**. This is an executive activity, needing high-level information for both long term, strategic decisions and immediate decisions targeted to mitigate a risk that may have serious consequences on business functions. In order to make high-level decisions, users involved in this activity need aggregated information about risk, mission impact, and financial impact. User roles involved in this activity are:
   - Business Owner: – monitoring the status of the system from a non-technical perspective and making long-term and short-term decisions.

4 FUNCTIONAL REQUIREMENTS

Functional requirements are grouped according to five classes, one describing the general characteristics of the visual component and the other four reflecting the macro activities presented in the previous section:

1. General (GEN);
2. System and network analysis and administration (ANM);
3. Actual status monitor (MON);
4. Reactive security response managing (ARM);
5. High Level Monitoring (HLM).

For each category, we define one or more root functional requirements that are derived from the operational requirements [D2.2.1]; root requirements are further refined in sub requirements.

4.1 General (GEN)

Requirement id	WP6.GEN.R1	Importance	Reachability
Version	1	3	3
Description	All the Visualizations presented to the user MUST be synchronized, propagating the user actions on element(s) belonging to one visualization (e.g., selecting a node of the network) to all the other visualizations that contain that element(s).		
Goal	To allow operators to get cyber defence situation awareness (CDSA) using multiple coordinated visualizations.		
Main Purpose	To allow the user for exploring the same data from different perspectives, exploiting multiple coordinated visualizations that are driven by user inputs.		

Requirement id	WP6.GEN.R1.SR1	Importance	Reachability
Version	1	3	1
Description	The visualization component MUST include a means for scrolling large images as part of basic visual interactions.		
Goal	To handle screen limitations through scrolling.		
Main Purpose	The purpose of this requirement is to facilitate the user interaction when dealing with large image or visualizations.		

Requirement id	WP6.GEN.R1.SR2	Importance	Reachability
Version	1	3	1
Description	Visualizations MUST include a zooming in and zooming out as part of basic interactions.		
Goal	To handle screen limitations through zooming.		
Main Purpose	The purpose of this requirement is to facilitate the user interaction when dealing with large image or visualizations.		

Requirement id	WP6.GEN.R1.SR3	Importance	Reachability
Version	1	3	3
Description	Visualizations MUST support a semantic zooming when appropriate or required interaction.		
Goal	To handle screen limitations through zooming.		
Main Purpose	The purpose of this requirement is to facilitate the user interaction when dealing with large image or visualizations.		

Requirement id	WP6.GEN.R1.SR4	Importance	Reachability
Version	1	3	2
Description	Visualizations MUST have the capability to present the user with focus plus context, showing a visualization overview and details at the same time, when appropriate to the required interaction.		
Goal	To prevent that the user loses the interaction control while browsing large images.		
Main Purpose	The purpose of this requirement is to facilitate the user interaction when dealing with large image or visualizations.		

Requirement id	WP6.GEN.R1.SR5	Importance	Reachability
Version	1	3	2
Description	Visualizations MUST support brushing popping out numerical details, as part of basic interaction.		
Goal	To provide the user with a simple means for getting additional information.		
Main Purpose	The purpose of this requirement is to facilitate the user interaction when dealing with large image or visualizations		

Requirement id	WP6.GEN.R1.SR6	Importance	Reachability
Version	1	3	2

Description	Visualizations MUST support both selecting and moving among different layers, when appropriate to the required interaction.		
Goal	To handle screen limitations through layered visualizations.		
Main Purpose	The purpose of this requirement is to facilitate the user interaction when dealing with large image or visualizations.		

Requirement id	WP6.GEN.R1.SR7	Importance	Reachability
Version	1	2	2
Description	Visualizations SHOULD use animation to prevent change blindness when appropriate to the required interaction.		
Goal	To drive the user attention on relevant events.		
Main Purpose	The purpose of this requirement is to avoid the user loosing relevant events or visualization changes.		

Requirement id	WP6.GEN.R1.SR8	Importance	Reachability
Version	1	2	2
Description	Visualizations SHOULD use other media (e.g., sound) to prevent inattentive blindness when appropriate to the required interaction		
Goal	To drive the user attention on relevant events.		
Main Purpose	The purpose of this requirement is to avoid the user loosing relevant events or visualization changes.		

Requirement id	WP6.GEN.R1.SR9	Importance	Reachability
Version	1	3	3
Description	Visualizations MUST allow the selection of a subset of the displayed data when appropriate to the required interaction.		
Goal	To provide the user with advanced analysis techniques based on parallel and		

	coordinated views and apply Visual Analytics techniques. In particular, selecting a subset of the data has the main goals of: a) to focus the analysis on such subset, discarding the other data on the actual b) to highlight the selected data on the actual visualization and in all the coordinated views, or c) to start a suitable Visual Analytics algorithm on such a subset. The underlying assumption is that one single visualization on a fixed set of data is not enough and the system has to provide multiple views on the same data, allowing for analysing the same problem from different perspectives. To this aim it is quite useful to allow the user to restrict the set of data he is observing to focus on specific data and/or apply algorithms on it.		
Main Purpose	To allow the user for exploring the same data from different perspectives, exploiting multiple coordinated visualizations that are driven by user inputs.		

4.1.1 WP6.GEN.R2

Requirement id	WP6.GEN.R2	Importance	Reachability
Version	1	2	1
Description	The visualization system SHOULD allow the operator to dispatch human security operations among users.		
Goal	To share insights, comments, suggestions, requested actions.		
Main Purpose	This requirement allows for sharing knowledge and both proposed and requested actions.		

Requirement id	WP6.GEN.R2.SR1	Importance	Reachability
Version	1	2	1
Description	The visualization system SHOULD allow the operator to select screenshots of the observed situation together with the relevant data that generated the screenshot.		
Goal	To reuse analysis patterns.		
Main Purpose	To select visual information for further reuse.		

Requirement id	WP6.GEN.R2.SR2	Importance	Reachability
Version	1	2	1
Description	The visualization system SHOULD allow the operator to annotate selected screenshots.		
Goal	To enrich analysis patterns		
Main Purpose	To annotate visual information for further reuse.		

Requirement id	WP6.GEN.R2.SR3	Importance	Reachability
Version	1	2	1
Description	The visualization system SHOULD allow for saving screenshots for further reuse.		
Goal	To reuse insights, comments.		
Main Purpose	This requirement allows a better collaboration among the different actors		

	involved in the system. As an example, a user that is monitoring the actual state of the network can spot some specific events, sending them to the users that are in charge of the system administration/analysis.		

Requirement id	WP6.GEN.R2.SR4	Importance	Reachability
Version	1	2	1
Description	The visualization system SHOULD support a means to select some actions that need operator intervention to be executed; actions can be: • Required • Proposed		
Goal	To select proposed or needed security actions.		
Main Purpose	This requirement allows a better collaboration among the different actors involved in the system.		

Requirement id	WP6.GEN.R2.SR5	Importance	Reachability
Version	1	2	1
Description	The system SHOULD present the user with a list of authorized people to select the target(s) of the actions selected through WP6.GEN.R2.SR5 requirement.		
Goal	To inform relevant people about proposed and/or needed security actions.		
Main Purpose	This requirement allows a better collaboration among the different actors involved in the system. As an example, a user that is monitoring the actual state of the network can spot some specific events that requires a mandatory action (e.g., unit X is not working: can you check whether this is due to a hardware/physical connection failure?), or that rise the need of some long term administration activity (e.g., increasing the computational power or better balancing the load among servers to decrease the		

	occupation of a specific server).		

4.1.2 WP6.GEN.R3

Requirement id	WP6.GEN.R3	Importance	Reachability
Version	1	2	3
Description	The visualization system SHOULD enable timeline-based comparison of the status of the monitored system.		
Goal	To inspect past events, forensic.		
Main Purpose	To store and retrieve past events and configurations, with the purpose of comparing the actual situation with the past or to monitor the progress of an attack.		

Requirement id	WP6.GEN.R3.SR1	Importance	Reachability
Version	1	2	2
Description	The visualization system SHOULD create snapshots of the system status.		
Goal	To produce a lightweight visual history.		
Main Purpose	The availability of snapshots allows for quickly and visually reviewing recent situations, favouring a more fluid interaction.		

Requirement id	WP6.GEN.R3.SR2	Importance	Reachability
Version	1	2	1
Description	The visualization system SHOULD allow the user to browse past states using time-stamps associated at events, configurations, user actions, etc.		
Goal	To provide the user with a complete visual history, for analysis and forensic		
Main Purpose	To review past situations with all needed details.		

4.2 System analysis and administration (ANM)

4.2.1 WP6.ANM.R1

Requirement id	WP6.ANM.R1	Importance	Reachability
Version	1	3	3
Description	The visualization system MUST display the graph based network topology (Layer 3) of the managed network.		
Goal	To allow user to analyse the logical structure of the network together with contextualized information.		
Main Purpose	To provide the user with the graph of the managed system that is the entry point for analysing relationships between nodes and other relevant security pieces of information.		

Requirement id	WP6.ANM.R1.SR1	Importance	Reachability
Version	1	2	2
Description	The visualization system SHOULD display the network topology (Layer 3) over a geographical map.		
Goal	To allow the user to correlate nodes with their geographical position.		
Main Purpose	The correlation node-geographical position can reveal issues specific to a geographical area.		

Requirement id	WP6.ANM.R1.SR2	Importance	Reachability
Version	1	2	3
Description	It SHOULD be possible to hierarchically subdivide the geographical map into sub areas of interest, when appropriate to the required interaction.		
Goal	To allow the user to correlate the risk status information of each node with more specific geographical areas.		
Main Purpose	To explore the correlation nodes-geographical areas allows for understanding how network problems		

	map on geographical locations.		

Requirement id	WP6.ANM.R1.SR3	Importance	Reachability
Version	1	2	2
Description	The visualization system SHOULD provide the capability to display the network topology at Layer 2.		
Goal	Analyse the structure of the network from a topological point of view (layer 2).		
Main Purpose	Layer 2 visualization allows the operator to inspect the connection among nodes and to locate possible physical failures (e.g., an interrupted wire, or a thunderstorm disturbing a radio connection).		

Requirement id	WP6.ANM.R1.SR4	Importance	Reachability
Version	1	1	2
Description	The visualization system MAY provide the capability to display the network topology at Layer 1.		
Goal	Analyse the structure of the network from a topological point of view (layer 1).		
Main Purpose	Layer 1 visualization allows the operator to inspect the physical connection among nodes, the transmission medium, used protocols and to locate possible physical failures (e.g., an interrupted wire, or a thunderstorm disturbing a radio connection).		

4.2.2 WP6.ANM.R2

Requirement id	WP6.ANM.R2	Importance	Reachability
Version	1	3	2
Description	The visualization system MUST display the mission graph, allowing the operator to designate critical system.		
Goal	To analyse the mission business entities and their relationships with technical devices.		
Main Purpose	The visual relationship between technical devices and mission business entities helps the users in making decision about the approval of mitigation actions.		

Requirement id	WP6.ANM.R2.SR1	Importance	Reachability
Version	1	3	2
Description	The visualization system MUST show the relationships between nodes, services, and business entities**.**		
Goal	To analyse the mission business entities and their relationships with the services that implement them and the ICT devices on which such services are deployed.		
Main Purpose	The help the security officer understand critical devices that are crucial for running business entities.		

Requirement id	WP6.ANM.R2.SR2	Importance	Reachability
Version	1	3	2
Description	The visualization system MUST allow the operator to designate system as identified mission critical.		
Goal	To highlight critical system.		
Main Purpose	The security officer loads different configuration of mission model and selects the critical systems. Different mission scenarios can be instantiated and the system can be evaluated based on the new mission requirements		

Requirement id	WP6.ANM.R2.SR3	Importance	Reachability
Version	1	3	2
Description	The visualization system MUST allow the operator to enter a mission impact description of identified mission critical.		
Goal	To describe critical system.		
Main Purpose	The security officer loads different configuration of mission model and comments the critical systems. Different mission scenarios can be instantiated and the system can be evaluated based on the new mission requirements		

4.2.3 WP6.ANM.R3

Requirement id	WP6.ANM.R3	Importance	Reachability
Version	1	3	2
Description	The visualization system MUST display the network nodes vulnerabilities, distinguishing between exploitable and non exploitable and displaying details on them.		
Goal	To analyse the possible entry points of a cyber attack.		
Main Purpose	The visual representation of vulnerabilities helps the users in locating critical nodes (possibly suggesting patches to be applied or signalling that a patch is not available) and making decision about the approval of mitigation actions.		

Requirement id	WP6.ANM.R3.SR1	Importance	Reachability
Version	1	2	2
Description	The visualization system SHOULD display an aggregated indicator regarding the vulnerability state of each node. This indicator MUST take into account level of dangerousness of possible exploitable vulnerabilities and conveys this information to the user. The indicator MUST be integrated in the topology visualization and must be instantiated on different detail level based on the composition of the network, like: • Nodes • Sub-networks • Assets		
Goal	To allow the user to quickly identify the possible exploitable nodes, sub-networks or assets		
Main Purpose	To allow the security officer to analyse the status of critical nodes in search of vulnerabilities to patch.		

Requirement id	WP6.ANM.R3.SR2	Importance	Reachability
Version	1	2	2
Description	The visualization system SHOULD display a detailed report about vulnerabilities when a user selects a single node. The informative tab MUST contain the list of vulnerabilities present, the associated level of dangerousness or exploitability, the corrective measure (if present) and the impact of the corrective measure (e.g., if the patch requires to shutdown the node)		
Goal	To allow the user to further investigate the status of a previously identified exploitable node		
Main Purpose	To allow the security officer to inspect in detail identified exploitable node in search of corrective measures to eliminate critical vulnerabilities.		

Requirement id	WP6.ANM.R3.SR3	Importance	Reachability
Version	1	2	2
Description	The visualization system SHOULD display an aggregated list of vulnerabilities present in the network and allow the user, by selecting one of them, to highlight all the nodes that are affected by that vulnerability.		
Goal	To allow the user to quickly identify the nodes that are affected by a particular vulnerability		
Main Purpose	To allow the security officer to inspect the aggregated list of vulnerabilities, identify the most dangerous or the most spread and inspect how much critical the affected nodes are.		

4.2.4 WP6.ANM.R4

Requirement id	WP6.ANM.R4	Importance	Reachability
Version	1	3	2
Description	The visualization system MUST display the list of attack graphs with their likelihood. This information MUST be visualized in accordance to the logical topology of the network, with a visual indicator used to convey the likelihood associated (e.g., high blinking effect for attack graph with high level of likelihood)		
Goal	Provide the security officer a higher level of awareness about the most dangerous attack paths		
Main Purpose	The visual representation of attack paths, together with their likelihood and the associated risks, helps the users in making decision about the approval of Mitigation actions.		

4.2.5 WP6.ANM.R5

Requirement id	WP6.ANM.R5	Importance	Reachability
Version	1	3	2
Description	Visualization system MUST allow the user to inspect and activate the list of authorised mitigation actions.		
Goal	Allowing user to inspect the system and authorize mitigation actions and activate them.		
Main Purpose	Strategically authorizing mitigation actions for different foreseen attack scenarios.		

Requirement id	WP6.ANM.R5.SR1	Importance	Reachability
Version	1	2	2
Description	Visualization system SHOULD to display the expected change in the risk associated with each mitigation action.		
Goal	Allowing user to understand the risk level reduction of each Mitigation Action.		
Main Purpose	Strategically select Mitigation actions based on the different risk level reduction.		

Requirement id	WP6.ANM.R5.SR2	Importance	Reachability
Version	1	2	2
Description	Visualization system SHOULD display, for a mitigation action the associated mission impact.		
Goal	Allowing user to inspect the trade-off of a Mitigation Action between risk reduction and mission impact.		
Main Purpose	Selecting Mitigation Action based on their trade-off.		

Requirement id	WP6.ANM.R5.SR3	Importance	Reachability
Version	1	2	2

Description	Visualization system SHOULD allow ordering of a list of Mitigation actions according to their risk reduction level.		
Goal	Allowing user to see Mitigation actions from the highest risk reduction level to the smallest or vice versa.		
Main Purpose	Inspecting Mitigation actions w.r.t. risk level reduction.		

Requirement id	WP6.ANM.R5.SR4	Importance	Reachability
Version	1	1	2
Description	Visualization system MAY allow ordering of a list of Mitigation actions according to their mission impact.		
Goal	Allowing user to see Mitigation actions from the smallest mission impact to the highest or vice versa.		
Main Purpose	Inspecting Mitigation actions w.r.t. mission impact.		

Requirement id	WP6.ANM.R5.SR5	Importance	Reachability
Version	1	2	2
Description	Visualization system SHOULD allow the user to inspect all the details associated with each mitigation action.		
Goal	To allow a user to have a better understanding of the mitigation action he is interacting with.		
Main Purpose	Before authorizing a specific mitigation action the user inspects its detail.		

Requirement id	WP6.ANM.R5.SR6	Importance	Reachability
Version	1	3	2
Description	The visualization system MUST enable operator activation of operator selected mitigation actions.		
Goal	To enable operator to activate mitigation actions.		

Main Purpose	Select and activate mitigation actions.		

4.2.6 WP6.ANM.R6

Requirement id	WP6.ANM.R6	Importance	Reachability
Version	1	2	2
Description	The visualization system SHOULD display aggregated historical data about cyber security incidents.		
Goal	To allow the users to analyse significant past events.		
Main Purpose	The user wants to analyse the efficacy of executed Mitigation actions helping him in making decision about the approval of Mitigation actions.		

Requirement id	WP6.ANM.R6.SR1	Importance	Reachability
Version	1	2	3
Description	The visualization system SHOULD display the history of Deployed Mitigation actions about cyber security incidents.		
Goal	To allow the users to analyse past Mitigation actions efficacy.		
Main Purpose	The user wants to analyse the efficacy of past executed Mitigation actions improving his capability in making decision about selecting Response plans and authorizing Mitigation actions.		

Requirement id	WP6.ANM.R6.SR2	Importance	Reachability
Version	1	2	3
Description	The visualization system SHOULD display the aggregated asset based historical data about: • compromised nodes (in terms of exploited vulnerabilities); • compromised services (in terms of services associated with compromised nodes) ;		
Goal	To allow the users to have an overview of most attacked nodes and services.		

Main Purpose	The user wants to get knowledge about the most attacked services and nodes.		

4.2.7 WP6.ANM.R7

Requirement id	WP6.ANM.R7	Importance	Reachability
Version	1	3	2
Description	The visualization system MUST allow inspecting and importing system configuration, and entering comments.		
Goal	To allow the users to configure the system in a batch fashion.		
Main Purpose	To allow the user to setup the systems, specifying specific domain data and parameters.		

Requirement id	WP6.ANM.R7.SR1	Importance	Reachability
Version	1	1	1
Description	The visualization system MAY allow importing data ontology information.		
Goal	To allow the users to configure the system		
Main Purpose	This functionality supports system initialization.		

Requirement id	WP6.ANM.R7.SR2	Importance	Reachability
Version	1	1	1
Description	The visualization system MAY provide the capability to input mission impact information.		
Goal	To allow the users to comment the mission model		
Main Purpose	To allow the users to comment the mission model		

Requirement id	WP6.ANM.R7.SR3	Importance	Reachability
Version	1	1	2
Description	The visualization system MAY allow operator input of mission impact information.		
Goal	To allow the users to configure the		

	mission impact.		
Main Purpose	This functionality supports mission impact modification.		

4.2.8 WP6.ANM.R8

Requirement id	WP6.ANM.R8	Importance	Reachability
Version	1	3	3
Description	The visualization system MUST display the steady risk level and its impact on the mission.		
Goal	To understand how mission critical systems are affected by the risk.		
Main Purpose	The visual relationship between network nodes, risk, and mission critical systems helps the users in making decision about the approval of mitigation actions.		

Requirement id	WP6.ANM.R8.SR1	Importance	Reachability
Version	1	2	3
Description	The visualization system SHOULD display the list of the mission critical systems ranked by their relevance and linked to the network topology.		
Goal	To understand the relative importance of the mission critical systems and identify the corresponding services and nodes.		
Main Purpose	The visual relationship between network nodes, risk, and mission critical systems helps the users in making decision about the approval of mitigation actions.		

Requirement id	WP6.ANM.R8.SR2	Importance	Reachability
Version	1	3	3
Description	The visualization system MUST display how the actual steady risk level affects each mission critical systems.		
Goal	To decompose the overall steady risk level in its mission critical system contributions.		
Main Purpose	To analyse the mission critical system that are characterized by the highest risk levels.		

Requirement id	WP6.ANM.R8.SR3	Importance	Reachability
Version	1	3	3
Description	The visualization system MUST display, for each critical system, the relationship between the risk and the estimated mission impact.		
Goal	To decompose the overall mission impact in its mission critical system contributions.		
Main Purpose	To analyse the mission critical system that are characterized by highest impact levels.		

4.3 System monitoring (MON)

4.3.1 WP6.MON.R1

Requirement id	WP6.MON.R1	Importance	Reachability
Version	1	3	3
Description	The visualization system MUST display the graph based topology (Layer 3) of the managed network.		
Goal	To allow user to monitor the logical structure of the network together with contextualized information: e.g., node type and vulnerabilities.		
Main Purpose	To provide the user with the graph of the managed system that is the entry point for analysing relationships between nodes and other relevant security pieces of information.		

Requirement id	WP6.MON.R1.SR1	Importance	Reachability
Version	1	2	2
Description	The visualization system SHOULD to display the network topology over a geographical map.		
Goal	To allow the user to correlate the mission risk status information of each node with its geographical position.		
Main Purpose	To explore the correlation nodes-geographical areas allows for understanding how network problems map on geographical locations.		

Requirement id	WP6.MON.R1.SR2	Importance	Reachability
Version	1	3	3
Description	It SHOULD be possible to hierarchically subdivide the geographical map into sub areas of interest, when appropriate to the required interaction.		
Goal	To allow the user to correlate the risk status information of each node with more specific geographical areas.		

Main Purpose	To explore the correlation nodes-geographical areas allows for understanding how network problems map on geographical locations.		

Requirement id	WP6.MON.R1.SR3	Importance	Reachability
Version	1	1	2
Description	The visualization system SHOULD provide the capability to display the network topology at Layer 2.		
Goal	Analyse the structure of the network from a topological point of view (layer 2).		
Main Purpose	Layer 2 visualization allows the operator to inspect the connection among nodes and to locate possible physical failures (e.g., an interrupted wire, or a thunderstorm disturbing a radio connection).		

Requirement id	WP6.MON.R1.SR4	Importance	Reachability
Version	1	3	2
Description	The system MUST show in real-time the dynamic risk related to each node or area, on-demand or automatically, if needed.		
Goal	Continuous monitoring of the risk level in each node and area and give the possibility to react to ongoing attack.		
Main Purpose	Automatic detection of node and area with high-risk level or manual inspection to check the mission impact of a node or an area.		

Requirement id	WP6.MON.R1.SR5	Importance	Reachability
Version	1	3	2
Description	The visualization system MUST highlight the portion of the network having high risk level, in terms of the dynamic risk associated with the actual attack path(s).		

Goal	To provide an overall understanding of the risk level of the generated attack paths.		
Main Purpose	A node may be under attack or reachable by an attack path and therefore its risk level is high and can lower the level of the mission if attacked.		

4.3.2 WP6.MON.R2

Requirement id	WP6.MON.R2	Importance	Reachability
Version	1	3	3
Description	The visualization system MUST display the list of Instantiated attack paths together with their associated dynamic risk.		
Goal	To foresee the possible incoming attack paths.		
Main Purpose	The visual representation of the instantiated attack paths makes the user aware of the possibility of an incoming attack.		

Requirement id	WP6.MON.R2.SR1	Importance	Reachability
Version	1	2	3
Description	The visualization system SHOULD display a ranked list of Instantiated Attack paths based on their probability (as computed by the WP5 HOC module), together additional information regarding the potential risk connected to the attack graphs.		
Goal	To quickly understand the structure of the ongoing attack and its impact.		
Main Purpose	The security officer can monitor the evolution of a potential attack and quickly evaluate the risk connected in real-time		

Requirement id	WP6.MON.R2.SR2	Importance	Reachability
Version	1	1	3
Description	The Instantiated attack graph MAY be represented both network (layer 3) and geographical visualizations, and a visual indicator will be used to communicate their probability.		
Goal	To quickly understand the structure of the ongoing attack and its impact.		

Main Purpose	The security officer can monitor the evolution of a potential attack and quickly evaluate the risk connected in real-time, relating it to both network and geographical level.		

Requirement id	WP6.MON.R2.SR3	Importance	Reachability
Version	1	3	3
Description	The visualization system MUST display a representation of the Risk associated with the Instantiated attack graphs.		
Goal	To quickly understand the evolution of risk level for the resources of the network		
Main Purpose	The user is allowed to inspect different instantiated attack graphs and for each of them the resulting effects on the risk level will be shown. The security officer can monitor the evolution of a potential attack and quickly evaluate the risk connected to each resource of the network in real-time, for different instantiated attack graphs		

Requirement id	WP6.MON.R2.SR4	Importance	Reachability
Version	1	2	3
Description	The visualization system SHOULD display alerts triggered by changes the instantiated attack graphs each time a significant variations occur.		
Goal	Alert the security officer on possible new menaces/variations-specializations of already followed ones		
Main Purpose	To allow the security officer to monitor the ongoing attack and being alerted each time new instantiated attack paths are available. Due to strictly time limit, the user has to be guided in the analysis		

	by the system, that will alert the user if: • Some instantiated attack paths presented has been cut out by lower probability • A new best fitting (i.e., with higher probability) instantiated attack graph is present on top of the list Continuously changing visualization has to be avoided and or mitigated with suitable animations.		

Requirement id	WP6.MON.R2.SR5	Importance	Reachability
Version	1	1	2
Description	The visualization system MAY allow the user to highlight single attack graph displayed with respect to the others represented for both similarity index and likelihood index. At the beginning the top results will start highlighted		
Goal	Allow the security officer to specialize and focus the analysis on the relevant attack graphs		
Main Purpose	In analysis and maintenance phase, the security officer highlight different attack graphs in order to compare them or emphasize correlation between chosen attack graph and actual status		

4.3.3 WP6.MON.R3

Requirement id	WP6.MON.R3	Importance	Reachability
Version	1	3	2
Description	The visualization system MUST display the anticipated mission impact due to the dynamic risk level.		
Goal	To monitor the operational level of the system w.r.t. the mission.		
Main Purpose	The visual representation of the mission impact makes the user aware of operational level of the system w.r.t. its mission.		

Requirement id	WP6.MON.R3.SR1	Importance	Reachability
Version	1	3	2
Description	The visualization system MUST display aggregated indicators about the mission.		
Goal	To monitor the aggregated operational level of the system with respect to the selected mission.		
Main Purpose	The security officer is able to quickly check the level of service offered with respect to the selected mission. The aggregation has to come by the resources that are tied to the different assets defined by the mission model. Moreover, an indicator about the whole fitting of the actual situation with respect to the envisioned level of mission has to be provided		

Requirement id	WP6.MON.R3.SR2	Importance	Reachability
Version	1	2	2
Description	The visualization system SHOULD to represent associations between nodes of the network (e.g., server, router, etc.) and assets relevant for the mission (e.g., payment service, energy distribution service, etc.).		

Goal	To monitor the operational level of the system with respect to the selected mission asset by asset, and make the security officer able to focus analysis on best/worst behaving assets		
Main Purpose	The security officer is able to identify operational level of single assets and further investigate the worst behaving ones. The visualization can be coordinated or over imposed on the topology of the network. Selection of a mission asset has to highlight all the nodes connected with it, while selection of a node has to return the associated assets		

4.3.4 WP6.MON.R4

Requirement id	WP6.MON.R4	Importance	Reachability
Version	1	3	2
Description	The visualization system MUST display the dynamic risk.		
Goal	To monitor the dynamic risk.		
Main Purpose	The visual representation of the actual risk makes the user aware of operational level of the system.		

Requirement id	WP6.MON.R4.SR1	Importance	Reachability
Version	1	3	2
Description	The visualization system MUST display the dynamic risk at network level.		
Goal	To monitor the actual risk associated with network items.		
Main Purpose	The visual representation of the actual risk makes the user aware of the portion of the network that exhibits the highest risk level.		

Requirement id	WP6.MON.R4.SR2	Importance	Reachability
Version	1	2	2
Description	The visualization system SHOULD display the dynamic risk at asset level.		
Goal	To monitor the actual risk associated with the enterprise's assets.		
Main Purpose	The visual representation of the actual risk makes the user aware of the assets that exhibits the highest risk level.		

Requirement id	WP6.MON.R4.SR3	Importance	Reachability
Version	1	2	2
Description	The visualization system SHOULD display the correlation between the nodes that exhibit the risk and the associated assets and vice versa.		

Goal	To inspect correlations between network based and asset based risks.		
Main Purpose	The visual correlation increases the user understanding about the relationships between network failures and impact on the mission.		

4.3.5 WP6.MON.R5

Requirement id	WP6.MON.R5	Importance	Reachability
Version	1	3	2
Description	The visualization system MUST display the incoming alerts and notifications.		
Goal	To quickly focus the user attention on specific, potentially dangerous events.		
Main Purpose	While the user is monitoring the system his attention is quickly driven toward new, relevant events.		

Requirement id	WP6.MON.R5.SR1	Importance	Reachability
Version	1	2	2
Description	While visualizing an alert the visualization system SHOULD rise the user attention with preattentive means and or alternate communication channels (e.g., audio), in a way that is proportional to the alert importance.		
Goal	To quickly switch the user attention toward incoming alerts.		
Main Purpose	While the user is monitoring the system his attention is quickly driven by preattentive or alternate means toward new, relevant events.		

Requirement id	WP6.MON.R5.SR2	Importance	Reachability
Version	1	3	2
Description	The system MUST show the description of alerts, including: • severity; • type (from a predefined domain); • the physical part of the network involved in the alert; • actual and future consequences; • required actions.		
Goal	To quickly make aware the user of the		

	alert meaning.		
Main Purpose	While the user is monitoring the system his attention moves quickly to new incoming alerts, analyses it and makes the appropriate decisions.		

4.4 Reactive security response managing (ARM)

4.4.1 WP6.ARM.R1

Requirement id	WP6.ARM.R1	Importance	Reachability
Version	1	3	3
Description	The visualization system MUST display the dynamic risk and anticipated mission impact.		
Goal	To inspect the actual impact level associated with both the ongoing attack and the Mitigation Action.		
Main Purpose	The visual representation of the actual impact makes the user aware of the mitigation action efficacy.		

Requirement id	WP6.ARM.R1.SR1	Importance	Reachability
Version	1	2	3
Description	The visualization system SHOULD display the dynamic risk with a preattentive visual means.		
Goal	Make the user aware of the impact level with a user-friendly representation.		
Main Purpose	The visual representation of the actual impact makes the user aware of the mitigation action efficacy.		

Requirement id	WP6.ARM.R1.SR2	Importance	Reachability
Version	1	2	2
Description	The visualization system SHOULD display the actual mission Impact using a preattentive visual means (e.g., a suitable colour scale).		
Goal	To allow the user for quickly understanding the Mission Impact and the affected services and assets.		
Main Purpose	The visual representation of the actual impact makes the user aware of the attack progress and Response plan efficacy.		

4.4.2 WP6.ARM.R2

Version	1	3	2
Description	The visualization system MUST display the actual response plan, allowing the user to make decisions on it.		
Goal	To inspect the enriched response plan details and temporal evolution.		
Main Purpose	The representation of the actual response plan details makes the user aware of the single mitigation action efficacy.		

Requirement id	WP6.ARM.R2.SR1	Importance	Reachability
Version	1	2	3
Description	The visualization system SHOULD display the list of deployed mitigation actions since the enriched response plan has been started.		
Goal	Make user aware of the deployed mitigation actions belonging to the actual Enriched Response plan.		
Main Purpose	The user analyses the Enriched Response plan evolution and efficacy.		

Requirement id	WP6.ARM.R2.SR2	Importance	Reachability
Version	1	3	3
Description	The visualization system MUST enable the operator to activate the proposed response plan.		
Goal	To control the proactive mitigation plan.		
Main Purpose	To allow the user to either confirm or stop a mitigation plan		

Requirement id	WP6.ARM.R2.SR3	Importance	Reachability
Version	1	3	3
Description	The visualization system MUST enable the operator to select and activate a mitigation action.		

Goal	To manually activate mitigation actions.		
Main Purpose	To manually use mitigation actions reactively proposed.		

4.4.3 WP6.ARM.R3

Requirement id	WP6.ARM.R3	Importance	Reachability
Type	Functional	3	1
Description	The user MUST be able to ask the system to stop the actual deployed response plan.		
Goal	To manually ask stop the tactical response.		
Main Purpose	If the user detects that the deployed response plan is deviating from the expected results he asks the system to stop it.		

4.5 High Level Monitoring (HLM)

4.5.1 WP6.HLM.R1

Requirement id	WP6.HLM.R1	Importance	Reachability
Type	Functional	3	2
Description	The visual system MUST visualize aggregated high-level information.		
Goal	To provide information for the executive management.		
Main Purpose	To allow managers to quickly understand the status of the system.		

Requirement id	WP6.HLM.R1.SR1	Importance	Reachability
Version	1	3	2
Description	The visualization system MUST display an aggregated information about the risk.		
Goal	Make executive user aware about the actual system security.		
Main Purpose	To allow managers to quickly understand the security level of the system		

Requirement id	WP6.HLM.R1.SR2	Importance	Reachability
Version	1	3	2
Description	The visualization system MUST display an aggregated information about the mission impact.		
Goal	Make executive user aware about the actual mission impact.		
Main Purpose	To allow managers to quickly understand the consequence of the actual network impairment.		

Requirement id	WP6.HLM.R1.SR3	Importance	Reachability
Version	1	2	2
Description	The visualization system SHOULD display an aggregated information about financial trends and impacts (e.g., Roi).		

Goal	Make executive user aware about the financial advantages or disadvantages of mitigation actions.		
Main Purpose	To allow managers to make decisions on how to use effectively the budget available for increasing the system security		

5 NON-FUNCTIONAL REQUIREMENTS

5.1 Performance and Efficiency Requirements

Requirement id	WP6.PRF.R1	Importance	Reachability
Version	1	3	3
Description	The visualization component MUST display the changes in the monitored system according to the time constraint of 2 seconds between the notification of a change in the state of the system and its visualization.		
Goal	To visualize new data about the system status according the time constraint of 2 seconds.		
Main Purpose	To provide the operator with a quick visual information of system status changes.		

Requirement id	WP6.PRF.R2	Importance	Reachability
Version	1	2	3
Description	The visualization component SHOULD be able to scale up to 10,000 nodes.		
Goal	To scale to large-medium networks.		
Main Purpose	To scale to large-medium networks.		

5.2 Compatibility Requirements

Requirement id	WP6.CMP.R1	Importance	Reachability
Version	1	3	2
Description	The visualization component MUST be WEB Browser based.		
Goal	To make the visualization platform able to deal with different from operating systems.		
Main Purpose	To increase the component compatibility with respect to external applications and operating systems.		

Requirement id	WP6.CMP.R2	Importance	Reachability
Version	1	3	2
Description	The visualization component MUST export data and images according to standard		

	formats (e.g., txt, png, jpg, etc.).		
Goal	To easily export data from the visualization component to other applications.		
Main Purpose	To increase the component compatibility with respect to external applications.		

Requirement id	WP6.CMP.R3	Importance	Reachability
Version	1	3	2
Description	The visualization component MUST use the exchange protocols and data formats adopted by the PANOPTESEC architecture.		
Goal	To interoperate with the PANOPTESEC integration framework.		
Main Purpose	To insure the component compatibility with the PANOPTESEC system.		

Requirement id	WP6.CMP.R4	Importance	Reachability
Version	1	2	2
Description	Data sources used by the visualization component SHOULD use JSON and/or XML formats.		
Goal	To easily feed visualization software with supported data format.		
Main Purpose	To increase the component compatibility with respect to external applications.		

5.3 Usability Requirements

Requirement id	WP6.USG.R1	Importance	Reachability
Version	1	2	2
Description	The visualization component SHOULD present different views, each being suitable to the tasks and information needs of each identified user role.		
Goal	To present the user with the data and interaction modalities suited for the task at hand.		
Main Purpose	To provide the different user groups with the right views and interaction modalities		

Requirement id	WP6.USG.R2	Importance	Reachability
Version	1	2	2
Description	The visualization component SHOULD include the up to date visualization techniques, making use of preattentive channels for the most critical tasks.		
Goal	To simplify and speed up the visual user interaction.		
Main Purpose	To reduce the user cognitive load while using the system.		

Requirement id	WP6.USG.R3	Importance	Reachability
Version	1	2	2
Description	The visualization component SHOULD be reactive enough (e.g., minimum five frames per second) to ensure a fluid interaction in most of the standard operations.		
Goal	To simplify and speed up the visual user interaction.		
Main Purpose	To reduce the user cognitive load while using the system.		

5.4 Reliability Requirements

Requirement id	WP6.RLB.R01	Importance	Reachability
Version	1	2	2
Description	Unit testing (black box and white box) SHOULD be applied to all main modules. A regression test must be run after each bug fixing.		
Goal	To reduce the defect rate.		
Main Purpose	To increase the component reliability with respect to the number of residual internal errors.		

Requirement id	WP6.RLB.R02	Importance	Reachability
Version	1	2	2

Description	Recovery time from external and internal failures (e.g., network errors, missing data, crash due to not fixed errors, etc.) SHOULD be less than 2 minutes.		
Goal	To quickly resume the operational state if a blocking error occurs.		
Main Purpose	To recover from blocking situations in a short time.		

5.5 Security Requirements

Requirement id	WP6.SEC.R01	Importance	Reachability
Version	1	2	2
Description	All the communications with other modules that involve sensitive data SHOULD be encrypted (e.g., https)		
Goal	To protect sensitive data across the network.		
Main Purpose	To protect sensitive data across the network.		

Requirement id	WP6.SEC.R02	Importance	Reachability
Version	1	2	1
Description	All the communications with other modules that SHOULD use a secure authentication protocol		
Goal	To avoid unauthorized accesses to the system.		
Main Purpose	To avoid unauthorized accesses to the system.		

5.6 Maintainability Requirements

Requirement id	WP6.MNT.R01	Importance	Reachability
Version	1	2	3
Description	Architecture and programs SHOULD be documented in a standard way (e.g., using ad hoc templates)		
Goal	Increase the software readability.		
Main Purpose	To facilitate modification in the software.		

Requirement id	WP6.MNT.R02	Importance	Reachability
Version	1	3	3
Description	Architecture and programs MUST be modular		
Goal	To reduce modification propagation and to simplify unit test activities.		
Main Purpose	Reduce time and effort for maintenance activities.		

5.7 Portability Requirements

Requirement id	WP6.PRT.R01	Importance	Reachability
Version	1	2	2
Description	The visualization system SHOULD be compatible with the most used WEB browsers (e.g., Mozilla Firefox, Chrome, Internet Explorer, etc.)		
Goal	To easily use the component on different WEB browsers and operating systems.		
Main Purpose	To easily use the component on different WEB browsers and operating systems.		

Requirement id	WP6.PRT.R02	Importance	Reachability
Version	1	2	2
Description	The visualization component SHOULD be developed in a language that is portable between most current operating systems (e.g., JAVA, JAVAscript)		
Goal	To facilitate the reuse of the software through standard programming languages.		
Main Purpose	To facilitate the reuse of the software through standard programming languages.		

6 COVERAGE OF OPERATIONAL VISUALIZATION REQUIREMENTS

Table 2 shows the coverage of operational requirements. Each operational requirement (columns) is covered with one or more functional requirements (rows), which belong to general, analysis, monitoring, attack response, and high-level monitoring groups. All the functional requirements are totally covered.

Table 2: Coverage of operational visualization requirements

			Viz1	Viz2	Viz3	Viz4	Viz5	Viz6	Viz7	Viz8	Viz9	Viz10	Viz11	Viz12	Viz13	Viz14	Viz15	Viz16	Viz17	Viz18	Viz19	Viz20	Viz21	Viz22	Viz23	Viz24	Viz25	Viz26	Viz27	Viz28	Viz29	Viz30
GEN	WP6.Gen.R1		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
		WP6.Gen.R1.SR1	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
		WP6.Gen.R1.SR2	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
		WP6.Gen.R1.SR3	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
		WP6.Gen.R1.SR4	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
		WP6.Gen.R1.SR5	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
		WP6.Gen.R1.SR6	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
		WP6.Gen.R1.SR7	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
		WP6.Gen.R1.SR8	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
		WP6.Gen.R1.SR9	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	WP6.Gen.R2		x																											x		
		WP6.Gen.R2.SR1	x																											x		
		WP6.Gen.R2.SR2	x																											x		
		WP6.Gen.R2.SR3	x																											x		
		WP6.Gen.R2.SR4	x																											x		
		WP6.Gen.R2.SR5	x																											x		
	WP6.Gen.R3																								x	x	x					
		WP6.Gen.R3.SR1																							x	x	x					
		WP6.Gen.R3.SR2																							x	x	x					

			Viz1	Viz2	Viz3	Viz4	Viz5	Viz6	Viz7	Viz8	Viz9	Viz10	Viz11	Viz12	Viz13	Viz14	Viz15	Viz16	Viz17	Viz18	Viz19	Viz20	Viz21	Viz22	Viz23	Viz24	Viz25	Viz26	Viz27	Viz28	Viz29	Viz30
ANM	WP6.ANM.R1									x																					x	x
		WP6.ANM.R1.SR1								x																						
		WP6.ANM.R1.SR2																														
		WP6.ANM.R1.SR3	x																												x	
		WP6.ANM.R1.SR4																														x
	WP6.ANM.R2		x																x	x	x											
		WP6.ANM.R2.SR1	x																x													
		WP6.ANM.R2.SR2																		x												
		WP6.ANM.R2.SR3																			x											
	WP6.ANM.R3										x												x	x								
		WP6.ANM.R3.SR1									x												x	x								
		WP6.ANM.R3.SR2									x												x	x								
		WP6.ANM.R3.SR3									x												x	x								
	WP6.ANM.R4											x																				
	WP6.ANM.R5													x	x			x														
		WP6.ANM.R5.SR1												x																		
		WP6.ANM.R5.SR2												x																		
		WP6.ANM.R5.SR3												x																		
		WP6.ANM.R5.SR4												x																		
		WP6.ANM.R5.SR5													x			x														
		WP6.ANM.R5.SR6													x																	
	WP6.ANM.R6		x																													
		WP6.ANM.R6.SR1	x																						x	x	x					
		WP6.ANM.R6.SR2	x																						x	x	x					
	WP6.ANM.R7								x																							
		WP6.ANM.R7.SR1							x																							
		WP6.ANM.R7.SR2							x																							
		WP6.ANM.R7.SR3							x																							
	WP6.ANM.R8			x	x			x																								
		WP6.ANM.R8.SR1		x	x			x																								
		WP6.ANM.R8.SR2		x	x			x																								
		WP6.ANM.R8.SR3		x	x			x																								

			Viz1	Viz2	Viz3	Viz4	Viz5	Viz6	Viz7	Viz8	Viz9	Viz10	Viz11	Viz12	Viz13	Viz14	Viz15	Viz16	Viz17	Viz18	Viz19	Viz20	Viz21	Viz22	Viz23	Viz24	Viz25	Viz26	Viz27	Viz28	Viz29	Viz30
MON	WP6.MON.R1		x			x				x																					x	
		WP6.MON.R1.SR1	x																													
		WP6.MON.R1.SR2	x																													
		WP6.MON.R1.SR3	x																												x	
		WP6.MON.R1.SR4	x			x																										
		WP6.MON.R1.SR5	x																													
	WP6.MON.R2		x																													
		WP6.MON.R2.SR1	x																													
		WP6.MON.R2.SR2	x																													
		WP6.MON.R2.SR3	x																													
		WP6.MON.R2.SR4	x																													
		WP6.MON.R2.SR5	x																													
	WP6.MON.R3		x				x																						x			
		WP6.MON.R3.SR1	x				x																									
		WP6.MON.R3.SR2	x				x																									
	WP6.MON.R4		x			x																						x			
		WP6.MON.R4.SR1	x			x																										
		WP6.MON.R4.SR2	x			x																										
		WP6.MON.R4.SR3	x			x																										
	WP6.MON.R5		x										x									x										
		WP6.MON.R5.SR1	x										x									x										
		WP6.MON.R5.SR2	x										x									x										

			Viz1	Viz2	Viz3	Viz4	Viz5	Viz6	Viz7	Viz8	Viz9	Viz10	Viz11	Viz12	Viz13	Viz14	Viz15	Viz16	Viz17	Viz18	Viz19	Viz20	Viz21	Viz22	Viz23	Viz24	Viz25	Viz26	Viz27	Viz28	Viz29	Viz30
ARM	WP6.ARM.R1		x			x	x																						x			
		WP6.ARM.R1.SR1	x			x	x																						x			
		WP6.ARM.R1.SR2	x			x	x																						x			
	WP6.ARM.R2		x													x	x															
		WP6.ARM.R2.SR1	x													x	x															
		WP6.ARM.R2.SR2	x													x	x															
		WP6.ARM.R2.SR3	x													x	x															
	WP6.ARM.R3																											x				

			Viz1	Viz2	Viz3	Viz4	Viz5	Viz6	Viz7	Viz8	Viz9	Viz10	Viz11	Viz12	Viz13	Viz14	Viz15	Viz16	Viz17	Viz18	Viz19	Viz20	Viz21	Viz22	Viz23	Viz24	Viz25	Viz26	Viz27	Viz28	Viz29	Viz30
HLM	WP6.HLM.R1		x	x	x	x	x																									
		WP6.HLM.R1.SR1	x	x	x	x	x																									
		WP6.HLM.R1.SR2	x	x	x	x	x																									
		WP6.HLM.R1.SR3	x	x	x	x	x																									

7 CONCLUSIONS

7.1 Significant results achieved

This deliverable analyses the visualization operational requirements and the user roles and tasks presented in [D2.2.1], refining user tasks with respect to the visual interaction with the system and grouping user roles and tasks in four groups, corresponding to four main macro activities of PANOPTESEC users.

A list of functional requirements, arranged in a hierarchical fashion, has been identified and validated for each of these groups, together with a fifth group capturing general visualization requirements, common to the whole visualization component.

The coverage of those functional requirements over the operational requirements previously identified within WP2 of the PANOPTESEC project for the visualization component has been provided, enabling the verification that all of the operational requirements are covered by the functional requirements.

These functional requirements will constitute a reference for the WP6 to design the visualization component.

7.2 Deliverable validation

The initial validation of this deliverable has been done using WP6 partners' comments and suggestions and incorporating the reviewers' feedback provided during the first period review, on 11st December, 2014. The final validation has been done through the two steps PANOPTESEC quality assurance process.

8 REFERENCES

[Bra97] S. Bradner, RFC 2119: Key words for use in RFCs to Indicate Requirement Levels, March 1997.

[Bar10] P. Barford et al.: Cyber SA: Situational awareness for cyber defence, in Cyber Situational Awareness, pages=3--13, Springer, 2010.

[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.

[D2.2.1] PANOPTESEC Consortium - "Operational Requirements Analysis" - Project deliverable D2.2.1.

[D3.1.1] PANOPTESEC Consortium - "System Hig-Level Preliminary Design" - Project deliverable D3.1.1.

[D3.1.2] PANOPTESEC Consortium - "System Hig-Level Design" - Project deliverable D3.1.2.

[D4.1.1] PANOPTESEC Consortium – "Data Collection and Correlation Component Requirements" –Project deliverable D4.1.2

[D4.1.2] PANOPTESEC Consortium – "Data Collection and Correlation Component Design" –Project deliverable D4.1.2

[D5.1.1] PANOPTESEC Consortium – "Response System for Dynamic Risk Management Requirements" – Project deliverable D5.1.1.

[D5.1.2] PANOPTESEC Consortium – "Models and High-Level Design of a Response System for Dynamic Risk Management " – Project deliverable D5.1.2