FP7-610416-PANOPTESEC

Dynamic Risk Approaches for Automated Cyber Defence

D6.3.2: Visualization Integration Prototype Report

Work-Package	WP6	Deliverable	D6.3.2
Due Date	30-06-2016	Submission Date	30-06-2016
Main Author(s)	CIS-UROME		
Contributors	All project participants		
Version	1.0	Status	Final
Dissemination level	PU	Nature	R
Keywords	Visual Analytics		

Part of the Seventh

Framework Programme

Funded by the EC - DG Connect

EXECUTIVE SUMMARY

This contribution is the D6.3.2 Report of the PANOPTESEC Project. It describes the Visualization Integration Prototype (Deliverable D6.3.1), focusing on the scientific contributions associated with the different visualizations developed for the project. In particular, it describes the visual analytics challenges that WP6 dealt with during the project evolution, the design choices, and the implemented prototypes.

HISTORY

Version	Date	Name/Partner	Comment
V0.1	25-05-2016-	Giuseppe Santucci/CIS-Urome	Initial creation of the document
V0.2	29-05-2016	Giuseppe Santucci/CIS-Urome	Section 3
V0.3	4-06-2016	Giuseppe Santucci/CIS-Urome	Section 4
V0.4	10-05-2016	Giuseppe Santucci/CIS-Urome	Restructuring of the document
v0.6	15-05-2016	Giuseppe Santucci/CIS-Urome	Restructuring of the document
v.07	22-05-2016	Nicolas Prigent/Supelec	Section 5
V.08	24-05-2016	Giuseppe Santucci/CIS-Urome	Fixing formatting issues, references and typos Document ready for Q.A.
V.09	26-05-2016	Ralph Moeller/UoL and Matteo Merialdo/Rhea	Q.A.
V1.0	30-06-2016	Giuseppe Santucci/CIS-Urome	Final version implementing Q.A. comments

TABLE OF CONTENTS

TABLE OF FIGURES

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	Managing reactive security response
CDSA	Cyber defence situation awareness
CIA	Confidentiality, Integrity, Availability
CIS-UROME	Università Degli Studi Di Roma La Sapienza
CVE	Common Vulnerability and Exposures
CVSS	Common Vulnerability Score System
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
PERCIVAL	Proactive and rEactive attack and Response assessment for Cyber Incidents using Visual AnaLytics
QA	Quality assurance
QR	Quality review
RHEA	RHEA System S.A.
RORI	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

The goal of WP6 (Visual Analytics and Display) within the PANOPTESEC Consortium is to design, develop, and validate an innovative visual analytics environment for analyzing the system model, the attack models, and the actual and historical data network. Moreover, the visual analytics component will show the automatic decisions made by the proactive and reactive systems making clear the match between the actual network state and the closest attack models.

The final goal of the Visual Analytics and Display is to support a network administrator (i) in analyzing the network configuration, (ii) in monitoring the actual status of the network, (iii) in analyzing the automatic scenario proposed by the system, and (iv) in supervising the system reaction. This report describes the different Visual Analytics solutions that compose the actual prototype that are based on state-of-the-art and beyond-state-of-the-art visual analytics approaches.

The purpose of this deliverable is to present the scientific outcomes and technical details from a general point of view.

1.1 Scope

The scope of this deliverable includes published and unpublished work. Most of the text comes from published and submitted papers to the most relevant Infovis and Visual Analytics venues.

1.2 Document structure

This D6.3.2 report 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 The Vulnerability Visualization

Section 4 The Topology Visualization

Section 5 The Attack Graph Visualization

Section 6 Coordinated and parallel views

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

2 METHODOLOGY

2.1 Information collection

The material presented in this report comes from published and under review papers submitted to relevant visualization conferences and journals: VizSec, Vinci, Journal of Visualization, Transactions on Visualization and Computer Graphics, NATO IST-133 Visual. Analytics – Cyber Security, etc. ([1][42][73][74][75]). A full description of the addressed PANOPTESEC requirements is available in Report D6.3.1R.

2.2 Information analysis

Information coming from scientific papers has been slightly adapted to the PANOPTESEC context, detailing the methodology of designing the visualizations and explaining how the selected visualization is evaluated (i.e., compared with different alternatives and assessed using user studies). Comparison with the state of the art has been simplified to make the text more readable.

2.3 Synthesis of results

A synthesis is provided showing the parallel and coordinated views prototype, in which the different visualizations are integrated and collaborate to produce a unique view.

2.4 Quality assurance

The QA in the PANOPTESEC Project relies on the assessment of a work product (i.e., deliverable) according to lists of QA checks (QA checklists) established by a QAM, validated at a consortium level and centralized in the project handbook. For the purpose of the QA of the D6.3.2 report, the deliverable was assessed according to the following checkpoints:

• PEER REVIEW (PR) QA CHECKLIST: D6.3.2 Report deliverable is a report; it then received a proper peer review according to the checks defined in this checklist.

3 THE VULNERABILITY VA SOLUTION

In order to allow security managers to assess the spread, impact, and dangerousness of the vulnerabilities that are affecting a network, the Vulnerability Visualization allows for dealing with different aspects of the network topology and vulnerabilities, relying on both general and application specific vulnerability characteristics, characteristics that are modeled using CVSS base and target environmental scores, respectively. Unique to our approach is that the CVSS target environmental score is computed automatically, using information coming from the attack graph associated with the actual detected vulnerabilities and network topology, avoiding the burden of manual input and evaluation of such data. Moreover, the visual design allows for scale to medium-large networks (see Figure 1).

3.1 Comparison with related proposals

The application of visual analytics techniques to the cyber security domain is a well known research approach (see, e.g., [3] and [7]). It encompasses many different topics, ranging from network status to intrusion detection to log and code analysis. As stated in [2] [19], a very critical aspect regards vulnerability presence in a node: in fact, exploiting a vulnerability can be the first step for attacking/penetrating the network.

Vulnerability exploitation is often the initial step of simple and complex attack paths and different contributions for dealing with them using visualizations exist in the literature, see e.g., [16] [6] [1].

Most of them focus on the visualization and analysis of cyber-events at different levels of detail, like [13] and [8]. Among them, some have sparse information on vulnerabilities, e.g., the work in [24] that allows for a basic grouping of nodes with similar vulnerabilities.

To the best of the authors' knowledge, most of the commercial tools supporting cyber-security provide limited visual information about vulnerabilities; among them we inspected CheckPoint NGSE [5], Imperva SecureSphere [11], IBM QRadar [10], RSA enVision [17]. Most of them accomplish this task in a tabular way with mostly simple visualization paradigms (e.g., bar chart, pie chart, geographical maps), and do not support more abstract visualization paradigms, best suited for coping with large networks. Following the study in [22] we choose to use an abstract visualization to represents vulnerability information, augmenting the characteristics of a treemap elements in order to provides simultaneously all the important aspects of a vulnerability.

A notable exception is the case of VisiTrend [21]: this tool proposes a visual environment representing the network topology in various way (node-link diagram, treemap) and plotting on them cyber-security parameters. One of its instantiations is directly connected to the visualization of vulnerabilities, using a treemap, among other visualizations: each rectangle represents a node, with its size mapped to data size and its color mapped to vulnerability state. Our solution improves this approach by allowing to compute and homogeneously visualize important parameters of the CVSS-like exploitability and environmental scores,

totally missing from VisiTrend. In particular, our Visual Analytics solution provides a way to automatically compute and visualize the environmental score, a crucial metric for assessing the impact that a vulnerability can have on the instantiated network on which it is exploited. Moreover, our solution proposes additional analyses, ranging from single vulnerability analysis to distribution of nodes with respect of overall score classes, that are not provided by Visitrend, and that contributes important advantages in the comprehension of the vulnerability status of a network.

The work in [9] constitutes a main contribution that coped with this problem presenting NV, a Web-based solution that utilizes treemaps and linked histograms to allow security analysts and systems administrators to discover, analyze, and manage vulnerabilities on their networks. Starting from it as an inspiration, we identified various problems in the solution itself, like the lack of scalability with respect to the chosen visual paradigm, and possible additional features that are crucial for raising the situational awareness of the security operator: our solution conveys in the same representation vulnerability information regarding cardinality, dangerousness, exploitability, spread, and impact , presenting vulnerabilities at different levels of aggregation (e.g., whole network, sub-networks, single node). Additionally, it allows the security operator to characterize and compare different vulnerabilities to identify the most dangerous, and to inspect the spread of one or several selected vulnerabilities through the network, providing a better understanding of the network status, useful to make decision and prioritize the remediation actions.

3.2 CVE and CVSS

Vulnerabilities are continuously discovered, analysed and stored in public databases like the NIST National Vulnerability Database [14]. Together with their textual description, a quantitative model has been developed to estimate their impact; such a model ensures repeatable accurate measurement, allows cyber analysts to understand the characteristics of a vulnerability and, according to NIST [15], it is well suited as a standard measurement system for industries. The actual version of the CVSS model is 3 but most of the available measures have been collected using version 2, that is the one used in the system described in this report.

CVSS version 2 organizes the metrics into three main groups:

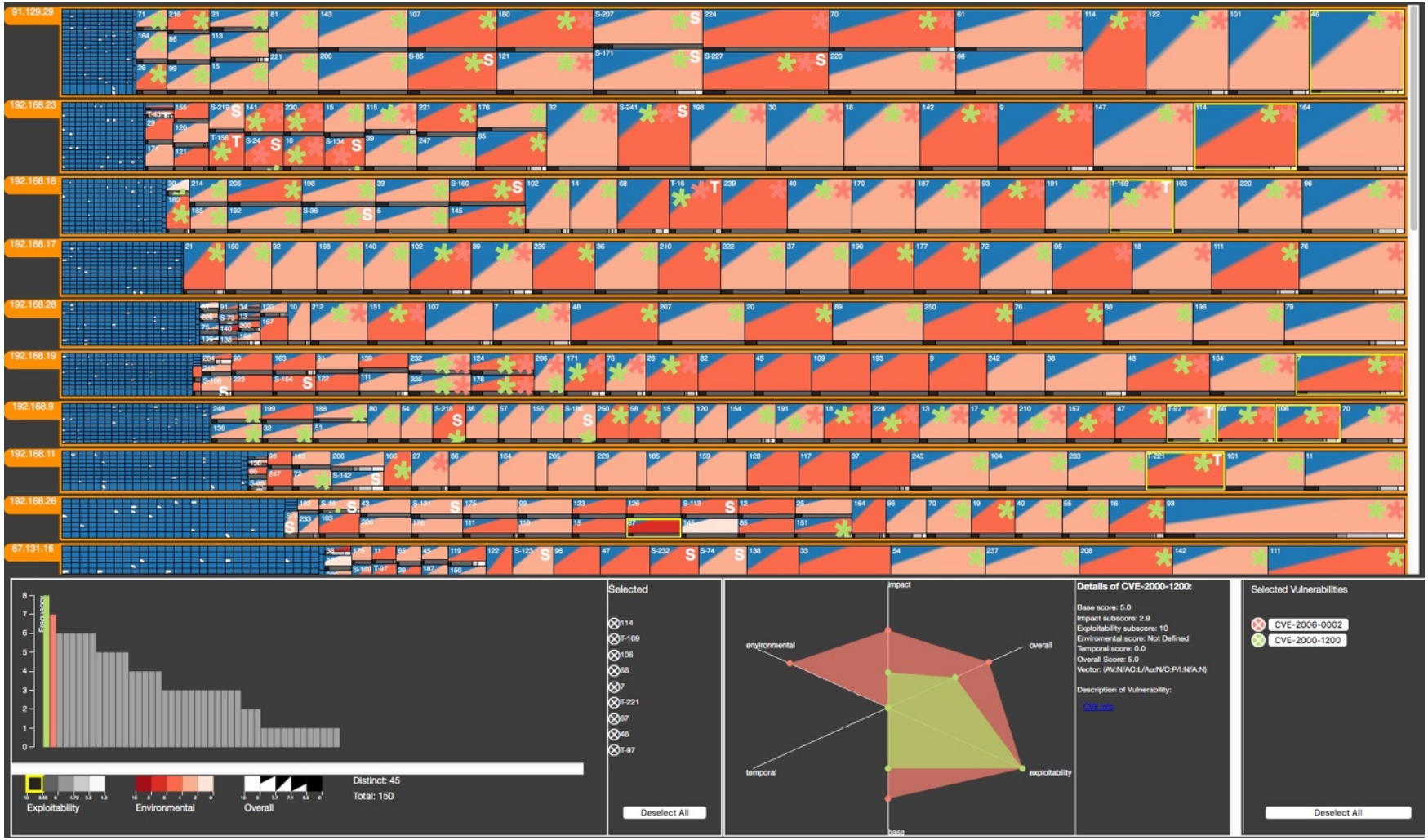


Figure 1 - The Vulnerability Visualization dealing with a synthetic network hosting 25,000 vulnerabilities spread across 5,000 nodes and 25 sub-networks. The system presents the user with intrinsic vulnerability characteristics, i.e., CVSS overall score and exploitability together with network specific environmental values, derived from the analysis of the attack graph associated with the network.

1. **Base metrics**, mandatory, representing intrinsic and immutable aspects of a vulnerability. They encompass information on how to exploit a vulnerability (local access vs remote access), on the complexity of the steps needed to exploit it, once the access to the target system has been gained, on how many times an attacker must authenticate to fully exploit a vulnerability, and on the impact of a vulnerability exploitation in terms of confidentiality, integrity, and availability, on the node on which the vulnerability exists;
2. **Temporal metrics**, optional, representing aspects that may change over time. They encompass information on whether publically available exploit code exists, on the presence and maturity of remediations (from workarounds to an official patch), and on the degree of confidence in both the existence of the vulnerability and the credibility of its technical details;
3. **Environmental metrics**, optional, that specialize the intrinsic vulnerability characteristics to the actual environment in which the vulnerability exists in terms of potential damage (that ranges from economic impact to loss of life), in terms of the spread of the vulnerability on the target system, and on the importance, i.e., requirements, of the impact on confidentiality, integrity, and availability (CIA in what follows) for the specific organization.

Metrics belonging to each group allow for computing an overall group score, ranging from 0 to 10 (the greater the worst), that summarizes the whole group; moreover, for the base group two additional sub-scores are computed: impact and exploitability. Base score, temporal score, and environmental score are used to compute the overall CVSS score, still ranging between 0 and 10, that is used to summarize the overall model metrics. In particular, if environmental and temporal scores are not available, the overall score coincides with the base score; if the temporal score is available the overall score is less than or equal to the base score while the presence of the environmental score can produce an overall score that is greater or smaller than the base score.

In the proposed solution, we use the environmental score metrics for characterizing the impact of a vulnerability exploitation in terms of potential damage and CIA on the target nodes that are traversable exploiting the analyzed vulnerability.

The atomic figures of CVSS are established using ordinal scales whose associated numerical values are used to compute sub-scores and scores. As an example, the impact sub-score of the base score uses three attributes: Confidentiality, Integrity and Availability ranging over the ordinal scale: None, Partial, Complete, whose numerical counterpart are 0, 0.275, 0.66 (the greater the worst) and are combined in a formula producing a value between 0 and 10.

The above discussion makes clear that simple figures are not descriptive enough and CVSS scores are typically accompanied by a string like (AV:N/AC:L/Au:N/C:P/I:N/A:N) that provides a concise information on the selected ordinal values (e.g., Access Vector: Network, Access Complexity: Low, Authentication: None, Confidentiality: Partial, Integrity: None, Availability: None).

The complexity of the CVSS structure pushes most of the network security analysts to inspect only the overall score, neglecting details. The visualization system presented in this report tries to overcome such a problem encoding visually the overall score (node coverage), the environmental score (colour), and the exploitability score (bargram). In this way the analyst can figure out in a quick way an overview of the nodes status and the main characteristics of the vulnerabilities; a radar diagram presents, on demand, all CVSS metrics.

3.3 The visual analytics prototype

In order to understand the implemented functionalities, we recall the two main tasks a security operator needs to fulfil during the vulnerabilities assessment of a network:

1. To get an overview of the actual vulnerability spread in the network, according to different parameters: their cardinality, their local impact and exploitability, in terms of CVSS base metrics, and their global impact on the organization's processes, in terms of potential damage, confidentiality, integrity, and availability, i.e., using the target **environmental** metrics computed using an **attack graph analysis**;
2. To select and compare specific vulnerabilities, in order to locate the most critical ones, prioritize interventions and make decisions on the the best fixing plan.

Clearly these tasks require the analysis of large amounts of data, and different analysis patterns must be available, allowing for analyzing and comparing vulnerabilities at sub-network level, node level, vulnerability level, CVE level, and CVSS level.

3.3.1 The analytical component

Data for vulnerability assessment for the PANOPTESEC project comes from vulnerabilities and network scanners (e.g., Nessus, LanGuard), able to identify the set of vulnerabilities V affecting the inspected machines and the connectivity of the nodes N of the network. Manual intervention is only required to define the set of source nodes $Sn \subseteq N$, i.e., the nodes that an intruder can use as starting point of an attack and the set of target nodes $Tn \subseteq N$, i.e., the nodes that host relevant organization processes. Moreover, each $t \in Tn$ is associated with its Impact(t) that represents the impact raising from the impairment of t in terms of potential damage and CIA, impact that is formalized using the CVSS environmental terminology and metrics.

Data about vulnerabilities is matched with the metrics and definitions contained in the CVE and CVSS repositories; connectivity, vulnerability, source nodes, and target nodes are used to compute the attack paths associated with the scanned network.

Attack paths are modelled as a sequence of pairs:

$AP = < v_0 , s >, < v_1 , n_1 >, < v_2 , n_2 >, \ldots , < v_n , t >$, where

$s \in Sn$, $t \in Tn$, $vi \in V$, and $ni \in N$ f or $i = 0 \ldots n$

representing a path from s to t, a path that is traversed exploiting the vulnerabilities v_0 , v_1 , . . . , v_n . Analyzing all the attack paths it is possible to associate to each vulnerability a set of pairs:

TargetNodesAttackPathsFrequency(v) = {< f_1 , t_1 >, . . . , < f_k , t_k >}

where k is the cardinality of Tn and each integer f_i represents the number of distinct attack paths that

a) terminate on the target node ti and

b) use v at least once in the path.

TargetNodesAttackPathsFrequency(v) provides a means to quantify the global impact of v, through the average of the impacts resulting from the impairment of the target nodes weighted through the number of attack paths leading to each target node:

TargetEnvironmental(v) = $\sum_k f_i * Impact(t_i)/(k * \sum_k f_i)$

The rationale behind the formula is the assumption that the more paths that use the vulnerability v to reach a target node t_i the higher the contribution of v to the possible impairment of t_i. Indeed, we are considering the effect of exploiting a vulnerability v not on the node on which it lives, but on the target nodes t_i reached through the attack paths that uses v. If the vulnerability v is fixed, all the fi attack paths targeting t_i are not traversable anymore. It is worth noting that v can appear on several nodes and on several attack paths to different target nodes and that a target node t_i can still be reached using other attack paths that do not use v. In summary, each vulnerability v in the Vulnerability Visualization system is associated with a local impact on the nodes on which it lives (CVSS base score) and with a global impact (CVSS environmental score) associated to the impairment of the target nodes in the end of the attack paths containing v.

3.3.2 Visualization design

The visualization solution used in the Vulnerability Visualization has been iteratively designed together with ACEA security experts and relies on the following main guidelines:

1. Space filling technique: in order to cope with large networks a space-filling layout has been selected, and a treemap solution has been the final choice, because it allows for handling the net work/sub-networks/IP node hierarchy, and it is easy to encode several variables on it. In order to facilitate the comparison of large network subset, a treemap-like solution has been selected in favour of a zoomable treemap that has the drawback of requiring complex browsing techniques (see, e.g., [4]) to guide the navigation. Our solution reduces the chance for the user to be lost in the information space. Moreover, inspecting a single hierarchy level at a time reduces the user's cognitive load.

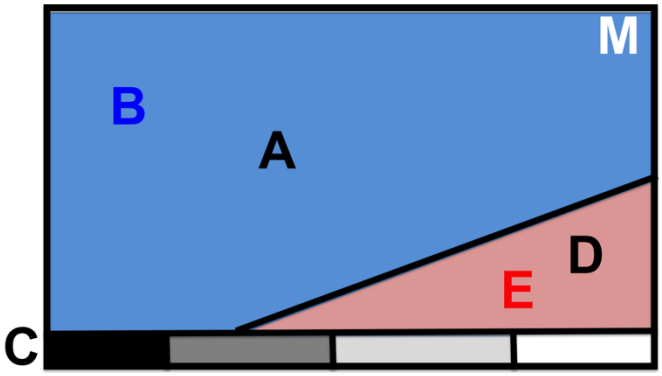


Figure 2 - Design of an element of the treemap-like visualization:

area of the main element (A), colour of the main element (B), lower bar (C), area of the over-imposed triangle (D), colour of the over-imposed triangle (E), marker (M)

2. Visual encoding: After several interactions with ACEA experts, we decided to encode on the treemap the cardinality of IPs/vulnerabilities, the overall score, the target environmental score, and the exploitability (see Figure 2).
    A. Cardinality has been mapped to the overall area of the elements, according to the standard treemap paradigm, and has a
    B. neutral colour;
    C. Exploitability is mapped to bargrams [4] that convey distribution information using a black-white scale (the chosen layout prevents simultaneous brightness contrast [23]) and the thin horizontal layout does not interfere with the treemap space-filling;
    D. Overall score has been mapped to the over-imposed triangle area conveying the impact that vulnerabilities have on the represented resource (network/sub-network/node). In this way a security operator can visually appreciate the level of coverage and identify highly impacted node from the others;
    E. Target environmental score has been mapped to a red colour scale, to pre-attentively drive the user attention on dangerous elements (the system configuration allows for using an alternative colourblind-safe scale, if needed). The target environmental score refers to the whole network, and using the same colour for highly environmental impacting nodes enables the security operator to immediately spot the most damaging ones;
    F. A marker M (S or T) allows for denoting **s**ources and **t**arget nodes.
3. Multiple coordinated and filterable views: The complexity of the application calls for the use of multiple views, and a filterable frequency distribution plot and a radar plot have been integrated with the main treemap view to facilitate the task of selecting and comparing critical vulnerabilities. The filter mechanism relies on the same colour/area size encoding used in the main view and acts as a scale legend as well.

With this visual design the security operator can quickly relate several values by looking at the visual elements, identifying problematic nodes from a multidimensional point of view and not just using a single metric encoding approach. Moreover, to increase the visual encoding effectiveness, the system dynamically collects and use quartile details on the actual network in order to maximize the usage of the scale values.

3.4 Visual component

The Vulnerability Visualization system, when launched, proposes to the security operator a visualization representing the aggregate level of vulnerabilities for the whole network. From this overview the security operator is able to traverse different hierarchies by simply selecting one of the analysis patterns.

Regarding the representation of a single element that can be a single node or a vulnerability, or a cluster of them (e.g., the whole network or a sub-network in the node case, or set of vulnerabilities with similar overall scores in the vulnerability case) the rationale is to have a different mappings to the properties of each treemap element based on the type of analysis.

The system provides various types of analysis, resulting from the combination of 3 possible clustering methods (by sub-networks, CVSS and CVE) at two possible levels of detail (root level or child level). Visualization changes accordingly to one of the 6 possible mappings, described in the following:

1. Sub-network analysis: (clustering method: sub-network, level of detail: root) This analysis allows to inspect the vulnerabilities of the network clustered by sub-networks. The area represents the cardinality of the vulnerabilities, the lower bargram represents the different levels of exploitability, the colour of the over-imposed triangle maps the average of the environmental score; its area, instead, represents the average of the overall score for the node vulnerabilities (see Figure 3 A).
2. Nodes analysis: (clustering method: sub-network, level of detail: child) This analysis expands the sub-networks in the belonging nodes, allowing to inspect the vulnerabilities of each single node in the network. The area represents the cardinality of the vulnerabilities, the lower bargram represents the different levels of exploitability, the colour of the over-imposed triangle maps the average of the environmental score; its area, instead, represents the average of the overall score for the belonging vulnerabilities (see Figure 3 B).
3. CVSS analysis: (clustering method: CVSS, level of detail: root) This analysis shows the vulnerabilities present in the network clustered by intervals of the overall score. In this way the security operator can quickly identify the most critical set of vulnerabilities and inspect them in more detail. The area maps the cardinality of the vulnerabilities belonging to a single interval of overall scores, the lower bar represents the different levels of exploitability, the colour of the over-imposed triangle indicates the average of the environmental score; its area, instead, represents the average of the overall score (see Figure 3 C).

4. Scored Nodes analysis: (clustering method: CVSS, level of detail: child) In this case, the system shows the nodes clustered by overall interval values. In this way the security operator can quickly identify the nodes affected by the most dangerous vulnerabilities and belonging to many different sub-networks. The area visualizes the cardinality of the vulnerabilities, the lower bar represents the different levels of exploitability, the colour of the over-imposed triangle maps the average of the environmental score; its area, instead, represents the average of the overall score (see Figure 3 D).
5. Vulnerabilities analysis: (clustering method: CVE, level of detail: root) In this analysis the focus is on the single vulnerabilities: each of them is represented as a single element in the treemap-like visualization. The area of the main element maps the cardinality of the nodes that are affected by that vulnerability. The lower bar represents the exploitability score of the vulnerability. Colour of the over-imposed triangle denotes the environmental score of the vulnerability; its area, instead, represents the average of the overall score that the vulnerability has on its affected nodes. In this way the security operator can visually identify the vulnerabilities that have the most impact on the system in terms of affected nodes, overall score and environmental score (see Figure 3 E)
6. Vulnerable Nodes analysis: (clustering method: CVE, level of detail: child) This analysis represents the expansion of the previous; in this case each vulnerability clusters its affected nodes. It allows the security operator to identify the most endangered nodes given a vulnerability, and propose a possible fixing plan, and to review the vulnerability contribution to the overall vulnerabilities state of the nodes. The area of the main element represents the cardinality of the vulnerabilities belonging to a single node (all of them, not just the clustering one). The lower bar represents the different levels of exploitability of the belonging vulnerabilities. Colour of the over-imposed triangle indicates the average of the environmental score for the belonging vulnerabilities; its area, instead, represents the average of the overall score for the belonging vulnerabilities (see Figure 3 F).

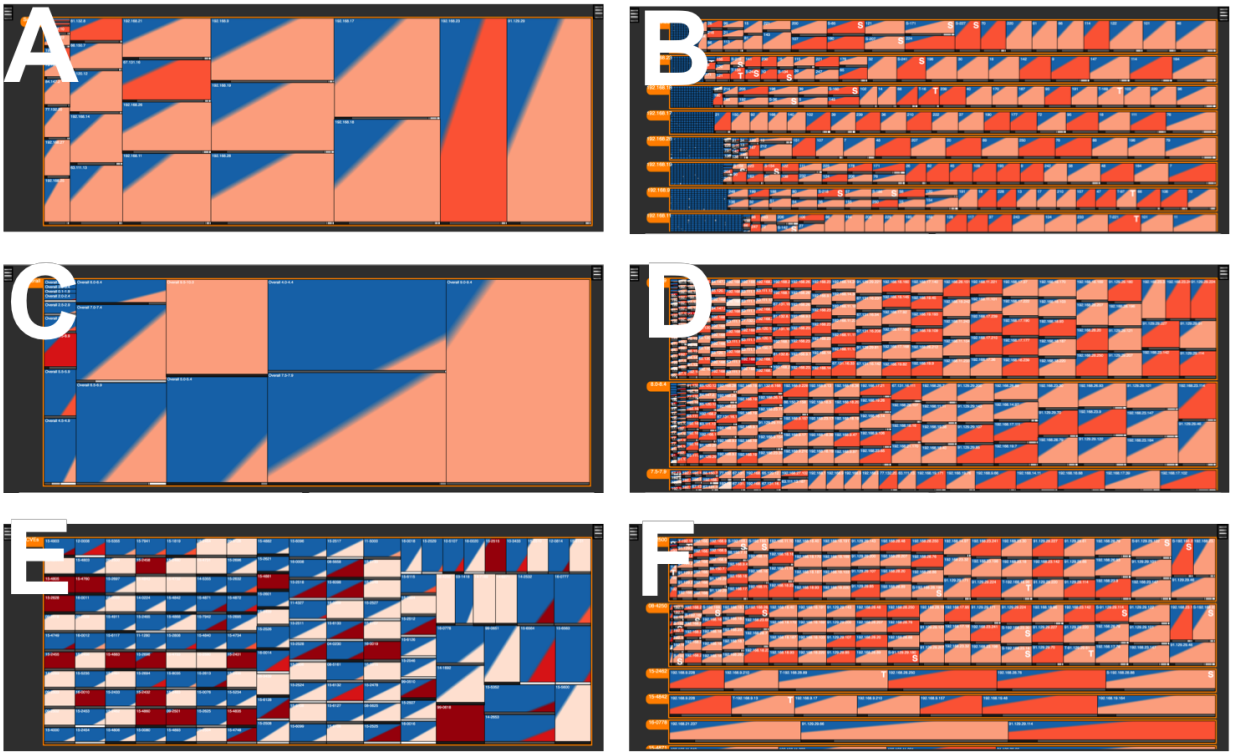


Figure 3 - The six analysis patterns of the system

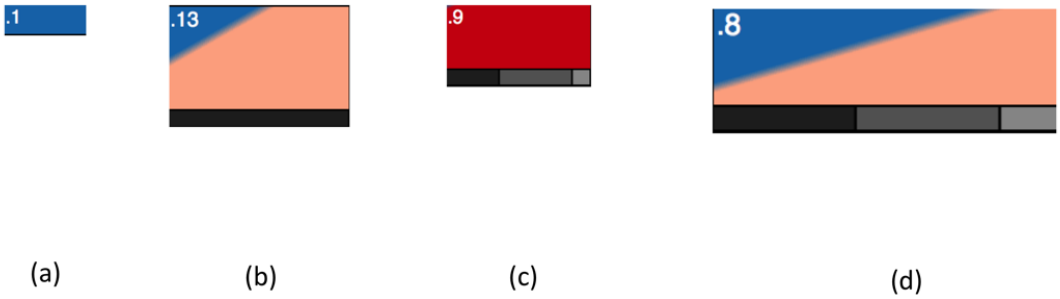


Figure 4 - Key node configurations

Figure 4 details the case of Node analysis and shows 4 key configurations:

a) represents a node with zero vulnerabilities: the spatial occupation is small, and the full blue colour helps in identifying the part of the network without problems; the choice to maintain them is justified by the need of preserving the network topology and by the dynamic nature of the assessment, where a node that is without vulnerabilities at time t_0

can become affected by several ones at time t_1 and the change has to be shown to the security operator;

b) shows a node with a small number of vulnerabilities, particularly critical for the node hosting them but with a low impact on the organization processes and with a high level of exploitability;
c) represents a node with a small number of vulnerabilities as well; however, in this case the score of vulnerabilities is highly critical and the environmental is highly critical as well; moreover, also exploitability is quite high: this node asks for immediate intervention of the security operator in order to mitigate the situation;
d) represents a node with a large number of vulnerabilities characterized by a high exploitability: however, their impact on the organization's processes is limited, even if their dangerousness (overall score) is quite high; in spite of the large cardinality this situation can be put on lower level of priority in a fixing plan.

The user can traverse the hierarchy and can select one or multiple elements. Coordinated results on the other views will be shown accordingly.

3.5 Frequency view

Here the supported goal is to identify the most frequent vulnerabilities present in the portion of the network selected by the security operator. After the selection of a subset of elements in the Network view the resulting frequency distribution is shown in the Frequency view (see Figure 5). Here the security operator can visualize the overall distribution of the vulnerabilities affecting the actual network selection increasing his situational awareness during the process. The implemented system allows for the refinement of this selection, eliminating or adding nodes starting from whichever of the three levels in order to identify interesting data from different perspectives.

In order to cope with a high number of elements in the frequency distribution, a set of 3 visual filters are provided in the bottom part, for exploitability, overall and environmental scores; the security operator can choose to refine the frequency distribution on a set of sub-intervals freely combinable among the 3 metrics. In this way she can focus only on interesting profiles of vulnerabilities (e.g., looking for vulnerabilities with high level of exploitability and environmental scores)

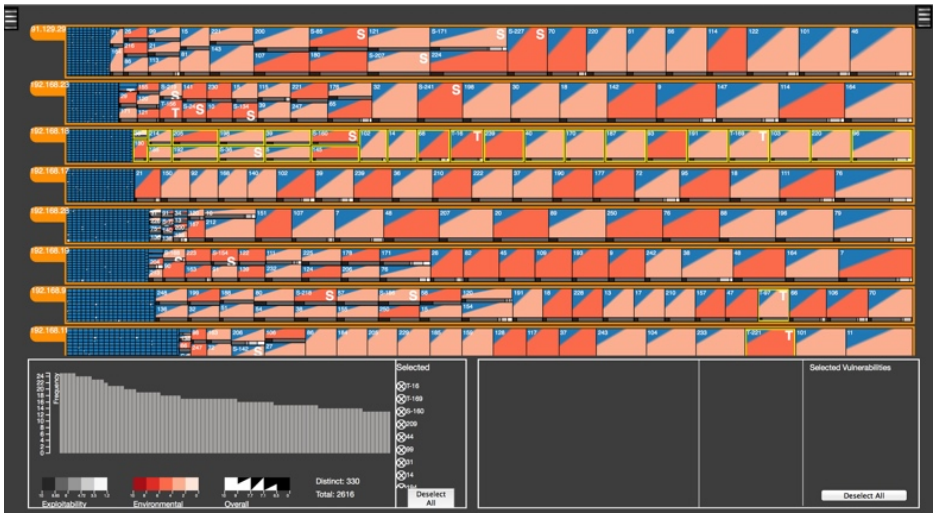


Figure 5 - Activation of the frequency distribution on a subset of elements.

Elements can be at different levels in hierarchy: the figure shows the selection of the whole top sub-network (clicking on the orange label on the left) and the nodes with highest criticality in the remaining sub-networks

The security operator can inspect the CVSS scores of each vulnerability by mouse-hovering on them. If he finds a particularly interesting vulnerability profile and wants to compare it with other profiles, she can click on it in the frequency view in order to visualize in a permanent way its profile in the radar plot: at this point, by mouse-hovering again, all the hovered vulnerabilities will become visually comparable with the previously visualized one.

3.6 Vulnerability view

This view allows for the full characterization of a subset of identified vulnerabilities. The chosen representation is a radar chart, with each axis reporting CVSS data about the vulnerability (i.e., temporal, base, environmental, impact, exploitability, and overall score). The security operator can inspect and compare vulnerabilities thanks to the peculiar characteristics of the radar chart to highlight areas of difference between the resulting relatives geometrical shapes (see Figure 1, the radar chart in the bottom area).

From the vulnerability view it is also possible to see in the right part a descriptive box containing detailed information (some data are in textual form, like the string vector of ordinal attributes); a link to the official CVE description allows for further refining the analysis. On the far right a numerical indicator represents the spread of the vulnerability in the whole network. By clicking on the corresponding button, a graphical indicator will be added to each element containing that vulnerability (see Figure 6). This process is applicable also to a subset of vulnerabilities, with an associated symbol added accordingly.

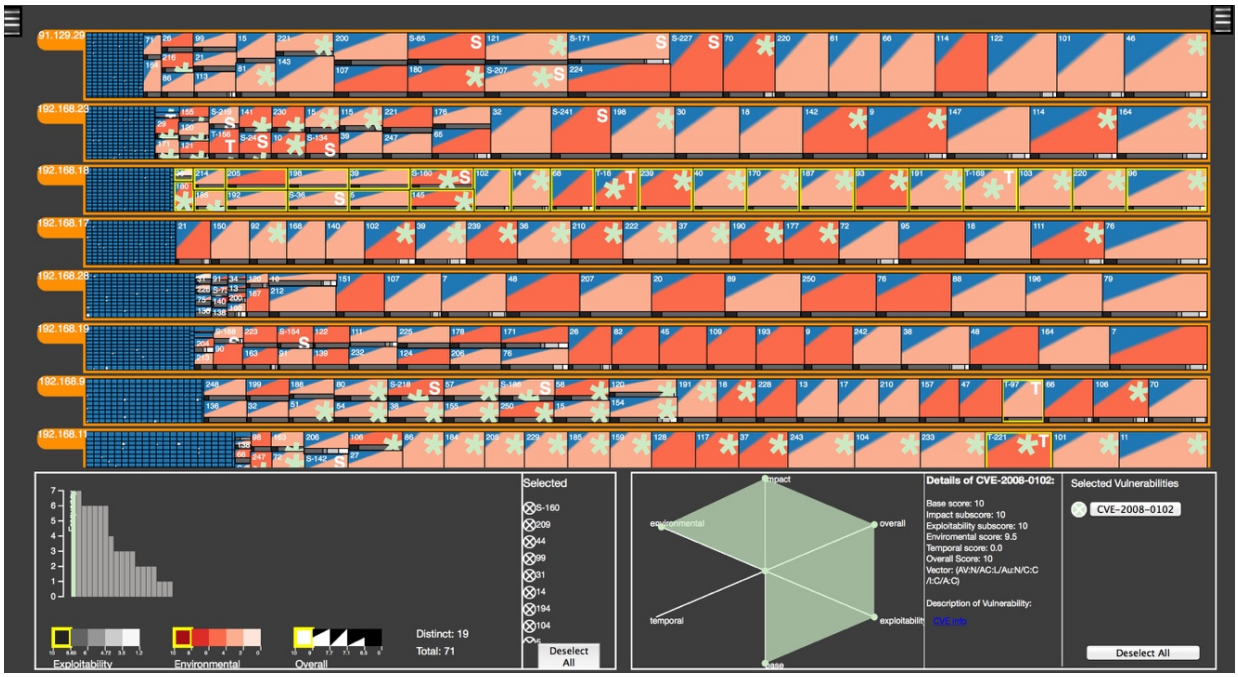


Figure 6 - The user highlights with a green marker the spread of vulnerability CVE-1999-0618 on the whole network.

3.7 Case Study: ACEA

The system is currently used in the PANOPTESEC use case, i.e., a subset of the ACEA Distribuzione network (the PANOPTESEC Project Emulation Environment) that encompassed (at the time of the extraction of these data the Emulation Environment is constantly on improvement and development) 138 IP interfaces, 14 sub-networks, 149 distinct CVE IDs that, with repetitions, result in 513 total vulnerabilities. Moreover, on such a subset, an attack graph has been computed, using 4 source nodes and 44 target nodes. That allows for computing the environmental value for all the detected vulnerabilities, distinguishing the vulnerability local impact from their global impact on target nodes. Figure 7 shows an overview of the 14 sub-networks in which it is easy to spot 4 critical sub-networks.

Three of them, 192.18.200, 10.10.0, and 192.168.1, on the right, contain a large number of vulnerabilities, with medium-low overall and environmental values, and high values of exploitability while the fourth one, 172.16.10, hosts few vulnerabilities (4) that have very high overall, environmental, and exploitability values.

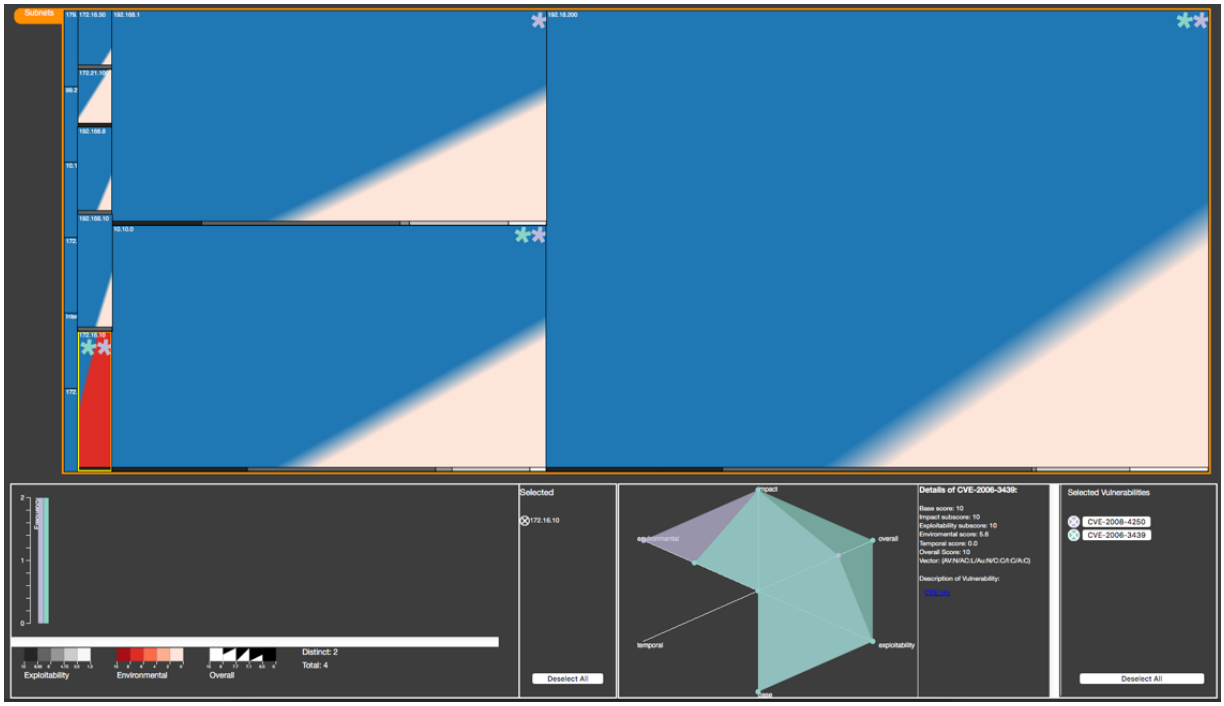


Figure 7 - Inspecting the 14 ACEA Distribuzione sub-networks:

the operator focuses on sub-network 172.16.10 (dangerous values of overall, environmental, and exploitability) and selects vulnerabilities CVE-2008-4250 and CVE-2006-3439, comparing their CVSS scores on the radar and observing their spread on the sub-networks. The radar confirms the criticality of these two vulnerabilities that show quite similar structures; moreover the officer discovers that other sub-networks are affected by these two vulnerabilities and decides to further investigate the matter.

Inspecting the frequency diagram it is possible to detect the two high risk vulnerabilities, CVE-2008-4250 and CVE-2006-3439 and, drilling down to a node level analysis, see Figure 8, it is possible to discover that both vulnerabilities affect four target nodes that exhibit extremely high values of environmental, overall, and exploitability pushing the analyst to further investigate on the services provided by the target nodes an to plan interventions that are compatible with the ACEA constraints. Moreover, the analysis at node level allows for pointing out other three vulnerabilities, as shown on Figure 9.

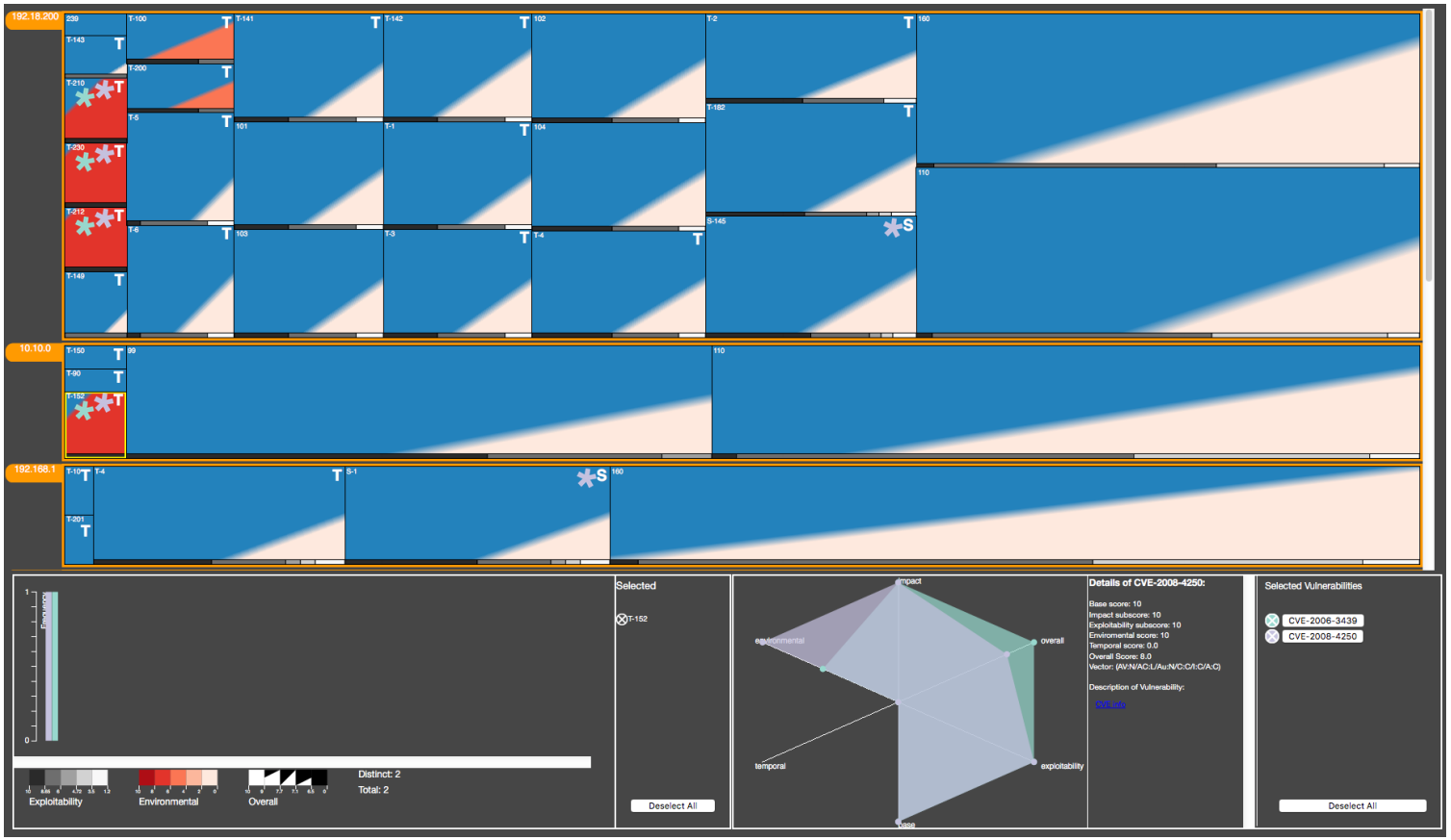


Figure 8 - Inspecting the nodes of ACEA sub-networks:

the security operator discovers that vulnerabilities CVE-2008-4250 and CVE-2006-3439 are both affecting four target nodes belonging to two different sub-networks and exhibiting critical values of overall, environmental, and exploitability. It is mandatory to fix or mitigate these two vulnerabilities. The figure makes clear the difference between overall and environmental score: target nodes 192.18.200.100 and 192.18.200.200 are affected by vulnerabilities with medium-low overall score (triangle area) and without other information it is very probable that an operator will not focus on them. However, their environmental value is high (red-orange colour) and that pushes the operator to investigate on these two nodes as well.

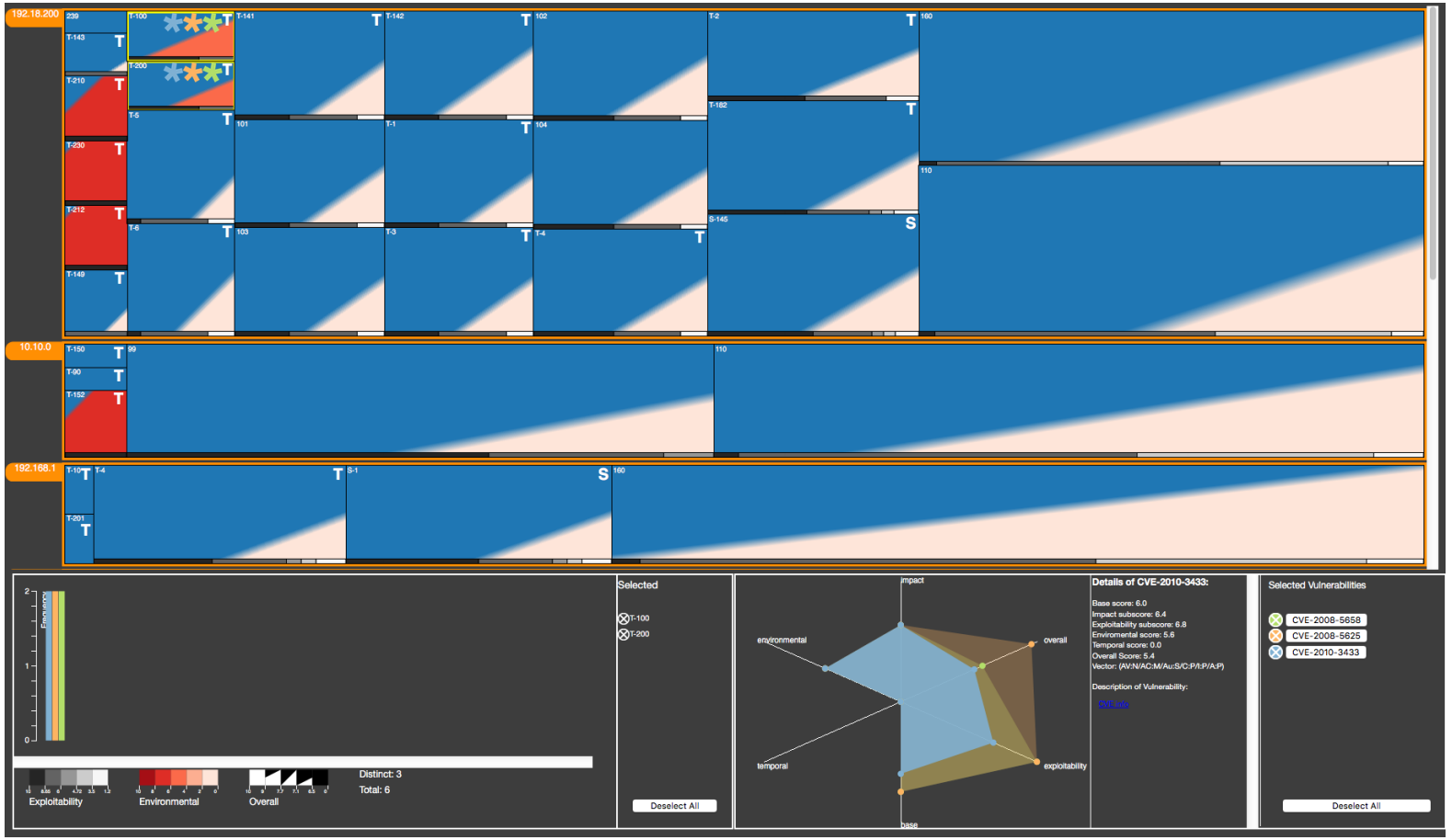


Figure 9 - Inspecting the target nodes 192.18.200.[100,200]:

the security operator discovers three new vulnerabilities, CVE-2008-5658, CVE-2008-5625, and CVE-2010-3433 that are affecting only that two nodes and have a high environmental value, meaning that resources on that nodes are quite relevant. Such vulnerabilities have high exploitability values: it makes sense to investigate on how mitigate them.

4 THE TOPOLOGY VA SOLUTION

In order to provide a security officer with information useful to understand topological and geographical aspects of a network, the topology visualization (based on ISO/OSI layer 3) relies on two different visual interfaces:

1. Abstract visualization
2. Geo referenced visualization

The abstract visualization has the goal of representing networks and sub-networks in a pure abstract way, using a standard expandable tree, produced by automatic layout algorithms. It allows for exploring single nodes, getting their details: IP, type, alerts, name, etc. This view works in tight collaboration with the geographical view, using the parallel and coordinated views mechanism. Moreover, it allows for exploring the reachability matrix, showing all the nodes that are reachable by a select node (see Figure 10).

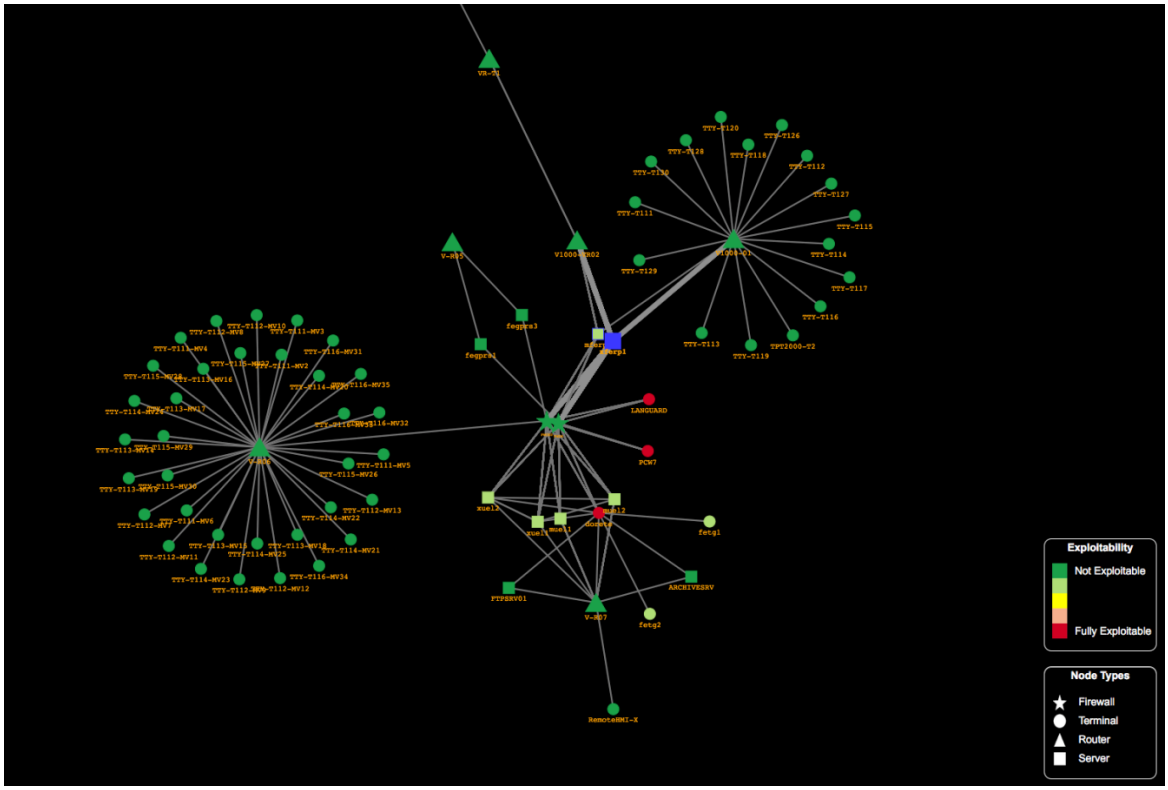


Figure 10 - A parallel view showing the logical sub-network structure, different devices, and all nodes reachable by the blue source node. Red nodes represent the critical target nodes.

The geo referenced visualization, instead, represents the topology at geographic level and its relationships with the ACEA geographical spread and business processes and has to deal with several research challenges, as described in the dedicated next subsection.

4.1 Comparison with related proposals

Situational awareness is a key concept in cyber-defence, with operators that need to intervene, mitigate risks, and determine the impact to organization's mission. As summarized in [35], cyber situational awareness and visualization are tightly connected, and the use of visual analytics environments for monitoring and reacting to cyber incidents is a common solution from both academia and industry. The application of visualizations to cyber security dates back to, at least, ten years ago (see, e.g., [27], [45]). However, e.g., [36], a common pitfall is the usage of complex visual representations that are hard to grasp. This issue can be avoided by involving the end user in the development cycle, defining clear goals that will drive the visualization design. Following this methodology, our system is based on a geographical representation, and allows for inspecting the status of multiple resources in a scalable way. In the current literature different approaches exist to address the problem of visualizing cyber security data; e.g., [33] provides a comprehensive overview of network visualizations: in particular, among others, low dimensional visualizations of networks mapped onto geographical representation.

In the particular sub-field of cyber security visualizations that make uses of geographical representations, [29] presents a system for inspecting geographical and time-dependent logs of coordinates. The authors chose to aggregate the points based on similarity, while our approach uses a mix of similarity aggregation and efficient spatial aggregation. Another work that is based on geographic visualization for large networks is [37]: the authors use a geographic representation of the resources, using the well-known GeoViz tooolkit [41], while in our approach the relevant resources are first aggregated and mapped or directly mapped onto the underlying geographical layer, according to their cardinality and space constraints. In [39] challenges about situational awareness for computer networks are presented, like awareness, confidentiality, integrity status of the command and control, intelligence, logistics, communications. Of particular interest is the integration of both geographical and logical representations for IT devices. Our solution provides an aggregate representation of these different properties for the monitoring and protection of a critical infrastructure, augmented with mission impact information. [42] presents a system that aims at integrating geographical, temporal, and logical views, while [38] presents a system that coordinates geographical visualizations with other security data: however, the mapping and aggregation are just computed in other views and then mapped statically onto the current visualization, without the tight coupling and interactivity that are present in our solution.

Concerning the visualization of security, risk, and vulnerabilities, [46] presents solutions for computing trust (availability, detection and false alarm trust values); also if the solution proposes geographical visualization, it provides only a zoom mechanism, without exploiting hierarchies or linking aggregate data to geographic areas. [43] presents a solution for merging geographical and logical topology, in which the geographical information is not tied to the network topology. Similarly to our work, this proposal allows for inspecting large networks by

clustering nodes; however, our solution preserves the geographical information of the hidden network using Voronoi diagrams.

The ”impact assessment” of a compromised resource on the organization’s mission is a key contribution of our work and one of seven major points that constitute the definition of situational awareness present in [26].

In particular, [38] assesses the importance of estimating impact of cyber threats to actual mission: the mission context can be in the military field [48] and critical infrastructures [38]. However, to the authors knowledge, less emphasis is posed to organizations and companies.

Similar high-level network status presentation is done in [10]; however, it uses a more abstract visualization paradigm that does not directly relate to the network topology.

ViSAw [47] presents a visualization environment for assessing the impact of detrimental events to the organization’s mission: however, the proposed visual solutions are more tied at an analytical evaluation (scatter-plot, tabular chart) and are less integrated in an organic view like the solution proposed in this paper. Moreover, the links between network nodes and organization’s processes are not represented.

Both [31][32] and [49] propose various 3-D representations, linking network nodes to organization’s processes: in our solution we chose to not use 3-D representations: 3-D representations are not always easy to interpret and requires manipulation from the user to overcome occlusion issues. Also the work of Carroll, in [28] copes with the same problem. However, the choice to represent the elements on a one-by-one basis poses problems of clarity and readability of the dependencies. In our solution we use 2-D layering and focus+context in order to help the user to navigate the visualization and overcome these issues. Finally, the approach used in [30] provides a visualization that emphasizes the link between the processes of an organization and physical devices; however, it does it in a block-diagram fashion, without the integration with other layers (e.g. geographical layer) that our solution envisions.

4.2 The Geo referenced visualization

Situational awareness plays a central role in cyber-defence and refers to (at least) two complementary aspects: the understanding of the network status, in terms of nodes level of endangerment, level of service, etc., and the consequences that the actual network situation has on an organization’s mission. While a common agreement exists on using visualizations for dealing with situational awareness [35], what elements need priority in visualization and which is the most effective representation still constitutes a challenging research area. Moreover, most of the proposed solutions deal only with the network structure and nodes, neglecting the relationship with the mission of the organization.

In order to improve situational awareness, it is mandatory to deal with issues arising from the cardinality of the network nodes, its large spread on the geographical level, the presence of different hierarchical layers that exists at both topological and geographical levels, the need of

combining quick awareness overviews together with local (geographical and topological) views. Summarizing, one of the main challenges is to make evident the relationship between the status of single nodes and the overall network status. Moreover, network information should be in correlation with an organization's mission using a business mission impact model, in order to assess the impact that compromised nodes have on the processes of an organization; this information is crucial to help the security officer defining and executing mitigation actions with the right priority of intervention, in order to minimize the impact of a cyber incident on the operational level of an organization's processes.

To address such challenging issues, the Visual Analytics solution that has been designed within the PANOPTESEC European project for monitoring the geographical ACEA infrastructure introduces the following key novel features:

1. seamlessly integration of the geographical and topological hierarchical layers;
2. continuous relationship between the analysis focus(es) and the context, both at geographical and topological levels;
3. representation of cyber incident risks at different scales, with an automatic cluster/Voronoi based optimization of the nodes;
4. integration of the network topology and geography with the organization mission and status;
5. novel visualization techniques able to quickly raise the user attention on the fragment(s) of the network associated with the affected organization's processes.

In the following we details de design choices for the network and mission layers that implement the above features.

4.2.1 Network layer

The visualization of the network of devices that, as a whole, constitutes the resource to protect represents a challenge: plotting too many points on the screen will produce cluttered visualizations and the user will be overwhelmed by information, having a detrimental effect on her capacity of making-sense of the data; plotting detailed information of subsets of resources will allow the user to understand what is the status of that specific area, but raises the risk of losing the associated context. The visualization must avoid pitfalls like information cluttering (that prevents correct sense-making and interaction) or the simultaneous presence of multiple information layers on the screen that can confound the user and mask important but less evident data. At the same time, the system must be able to show in real time the status of the network, allowing the user to inspect particular areas of interest and alerting her when a cyberattack or any other threat is detected.

The first aspect to consider, in relation to the nature of the network, is how to represent and relate the different hierarchies of the data under examination: we have to consider both the geographical hierarchy, based on geographical position of the resources, and the logical hierarchy, based on the semantic of any single resource. The system presents the user with a quick way to obtain the status of the overall number of resources under examination both in

an aggregated and punctual view: to do so we exploit and merge together the inner data hierarchies, in order to provide a guided exploration of the data towards areas of interest. However, given the particular characteristics of the data, a geographical hierarchy could not be always defined.

Our solution envisions to create this hierarchy, exploiting the common notion of political geography, which usually subdivides a geographical area in smaller fractions (e.g., states, provinces, cities, neighborhoods) and to use that in order to separate the resources in hierarchical levels. This hierarchy will be helpful in exploration tasks and will constitute the first hook point of the whole analysis process.

The geographical hierarchy will then be put in direct connection with the inner hierarchy of the network to visualize. Figure 11 shows an example. The data used as reference come from the power distribution network of the Italian ACEA Group that manages critical infrastructures as power and water distribution.

This hierarchy is constituted by primary cabins (70), that constitutes the primary nodes for power distribution, secondary cabins (2000) and hundreds of thousands smart meters (undisclosed numbers).

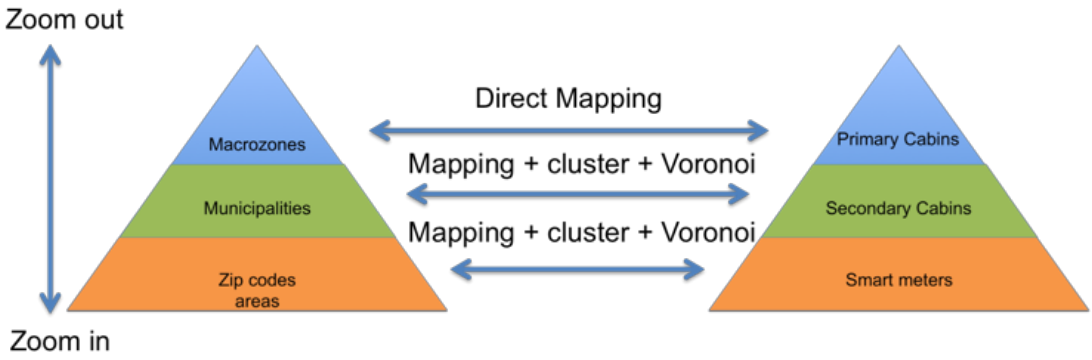


Figure 11 - Level of detail of the different hierarchies (geographical and logical) and their visual interconnections: visual behavior is added descending the hierarchies in order to better convey and correlate information

From a cyber-threats point of view each of these resources can be a potential target of cyber-attacks, and the awareness of the status of the entire network is crucial in order to quickly identify and react to possible sources of attacks spreading through the network.

When referring to the primary cabins, it is pretty clear that their number does not constitute a problem and the system can be able to plot all of them at the same time on the map. Nonetheless the first layer of the visualization will not present just the primary cabins, but also aggregated indicators computed for each area of the geographical hierarchy. The rationale is to allow the user to quickly have an idea of where the possible problems can be located and further investigate just these zones.

In order to avoid clutter phenomena or plotting of the whole secondary cabins set, our solution envisions a progressive refinement of the resources visualized on the following axes:

- Geographical axis: it allows the user to switch among representation based on sequentially more refined version of the area. Particular to the used dataset, these areas are constituted by the macro zones of Rome (ranging from North to South-West), the Municipality (21 entries), and the Zip codes;
- Topological axis: representing the logical connection (link) existing among the different nodes of the network.

Exploiting these two coordinates, the system is able to present to the user all the resources constituting the network under protection in a scalable way.

To mitigate the clutter raising from plotting thousands network nodes, the following techniques have been used: for the areas with enough space available with respect to the number of contained resources, nodes are grouped into clusters (using a K-means algorithm with an adaptive k with respect to the number of primary cabins present in the area). Additionally, in order to immediately convey the geographic space interested by the selected nodes, a Voronoi diagram is computed to create sub-areas containing a constant number of nodes. In this way, the user will have information also on the extension of the interested areas and on the number of involved nodes, tightly coupling security information with geographical one.

This technique avoids situation in which a sub-area or a cluster results too cluttered and allows for a better separation of the secondary cabins with respect to the available space. Moreover, also from an interaction point of view, the system will make visible only the resources or areas that correspond to the actual user's interest, reducing the clutter produced by all the other points. Multiple selections are possible: the user can expand or collapse any of the inspected cluster/area, allowing the highlight of the interesting subset of the network resources. Colour coding and frequency of update are also two additional visual cues used in order to convey information: areas affected differently by attacks or vulnerabilities will be presented with red or yellow shade, more severe when the connected metrics have high values. The colour-code is maintained during the exploration of the hierarchy, and serves as a hint for quickly highlight the areas that needs to be inspected. Nodes under attack or malfunctioning will blink, distinguishing them from the secure ones: in this way the user is pre-attentively alerted if some resource is under attack and can quickly select it to inspect additional parameters, using coordinated visualizations.

4.2.2 Integrating local and geographical layer 3 topologies

This section introduces the novel layer 3 topology added to the system, dealing with the issue that in a pure geographic visualization each single point has a specific meaning, and representing more elements in the same point (e.g., local networks within a building) integrating them with the overall geographical view is not a trivial task. To solve the problem, it is needed to distinguish at geographical level single nodes and sub-networks, allowing for

semantic zooming in local topologies, according to the specific nature of multi-scale networks (see, e.g., [43]) preserving the integration with the geographical layer. The selected encoding has been a glyph [44], in order to capture different aspects of the inner sub-network. In particular, a composite node is represented either with a glyph portraying connection information, or with a glyph summarizing some relevant sub-network characteristics, e.g., the node risk level distribution, see Figure 12.

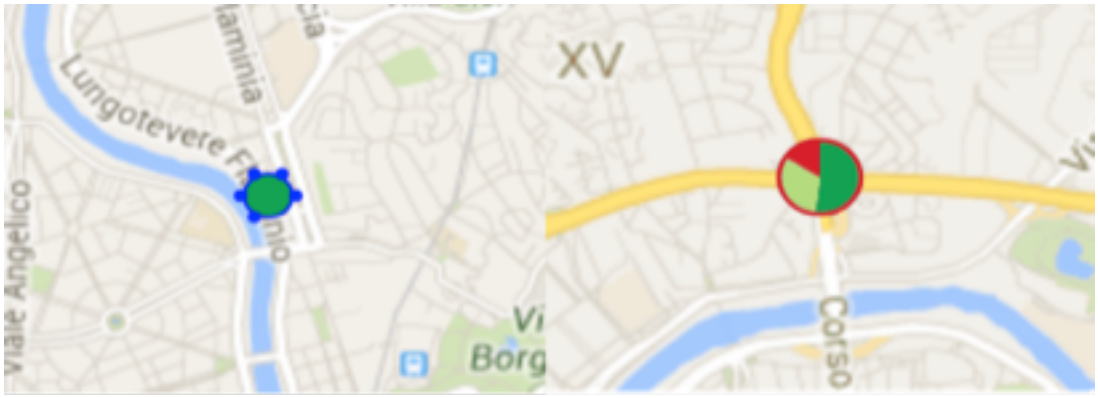


Figure 12 - Two examples of glyphs

used for a) distinguishing single node by complex nodes with inner topology and b) conveying aggregate information of local complex topologies. The one on the left allows for making explicit the IP interfaces of the whole sub network, while the one on the left is representing the distribution of risk of the sub-network nodes

In order to get details on the inner sub-network, a semantic zoom interaction has been designed. Clicking on a composite node will expand the node's internal structure using an adjacency matrix, composed of a grid, located in the middle, and of four bars, each one located on a side of the grid, see Figure 13. Each bar represents all the nodes of the sub-network, and black dots in the matrix indicate that the two corresponding nodes are connected at layer 3. The redundancy of information allows for a better representation of layer 3 links when a composite node is required to be connected to the rest of the network: the geographical area is split to avoid visual occlusion, and logical links are drawn selecting the best connection side, minimizing crossings and occlusion, see Figure 14. This technique is a novel one and correspond to the actual state of the art [45].

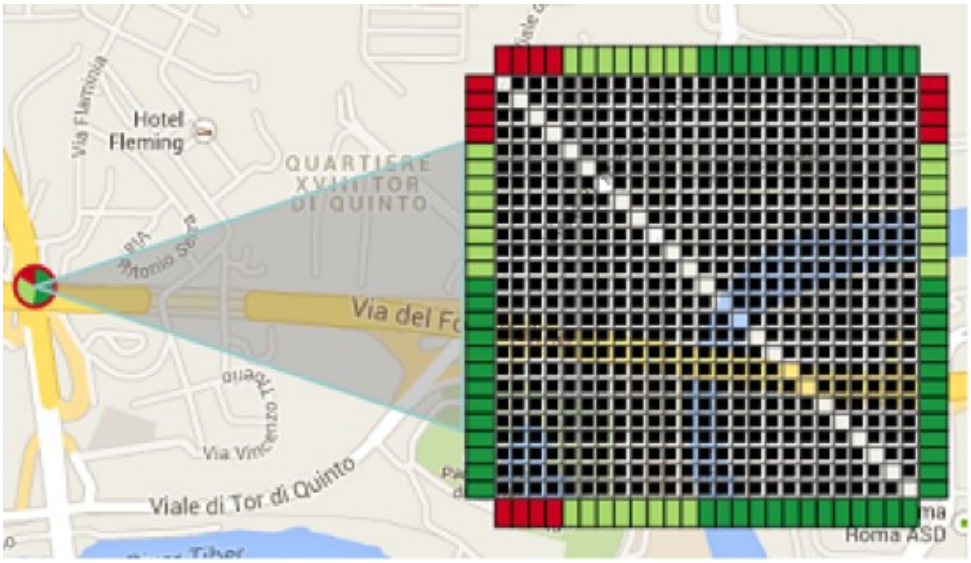
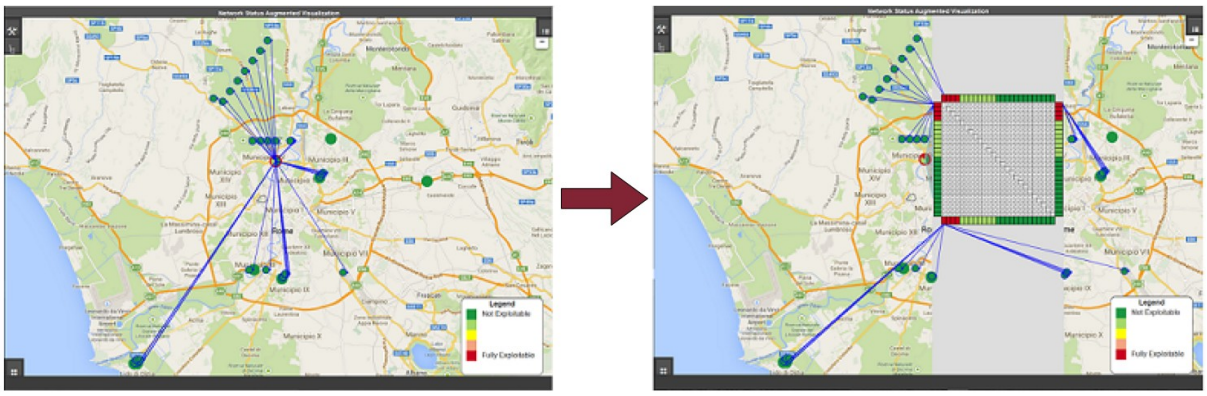


Figure 13 - Semantic zoom on a composite node.

The adjacency matrix allows for representing in a compact way the layer 3 topology of the sub-network: a black dot in position i, j indicates that node i and node j are connected at level 3. Colour coding represents node risk levels



View without expanded nodes

View with expanded nodes

Figure 14 -Semantic zooming on a composite node

showing details of the internal layer 3 topology connections, using a redundant adjacency matrix, and preserving the overall geographical view. Redundancy allows for optimizing the drawing of the connections of the composite node with the rest of the graph. Colour coding on matrix row and columns provide the same information of the nodes risk distribution shown in Figure 12 and facilitate the understanding of the redundant representation

To further investigate the topology of a composite node, it is possible to activate a coordinated view that shows details on the subnet, like detailed division in sub-networks and node types (e.g., firewall, router, etc.), and the roles they have with respect to attack paths: source node, intermediate node, and target node. Hovering on a composite node for more than 2 seconds triggers the pop-up view shown on Figure 5; further interacting with such new view allows for

making explicit the list of nodes reachable by a specific source node, showing all reachable nodes and highlighting the reachable target nodes, activity that is particularly useful when inspecting attack paths, see Figure 10.

4.2.3 Mission impact layer

The Mission impact layer will provide the user with crucial information about the impact that the compromised nodes have on the organization's mission. In order to reach this goal, the system uses a Mission Impact Model, providing a connection between the business processes of the organization and the network nodes (devices) that support them. While different contributions exist on model definitions (see, e.g., [20]) the proposed solution is general with respect to underlying chosen model.

The model used in the paper follows the Business Process model and Notation 2.0 (http://www.bpmn.org/). The organization is modelled as a company: it features, among other description fields, the list of all business processes and the definition of possible missions.

Each business process is associated with:

1. a priority, based on the selected mission, that represents the importance of the process to that particular mission;
2. a list of feared events; a feared event is an event that can lead to a situation in which a business process might not be accomplished anymore or will lower its operational level. For each feared event, a list of con-human understanding, will help linking the loss of operational level of a process to actual impact on connected services.

Each process has an internal structure, composed by sub processes, each with a weight in the accomplishment of the main process. For each sub-process a list of supporting devices is defined. A device is part of the overall network (routers, firewalls, etc.) defined in the network layer. For each device an operational impact score is defined, with respect to each feared event. The impact scores will quantify the detrimental effect on the sub-process if the node is compromised, under the relative feared event.

Organization of processes into sub-processes proves to be particularly suited when designing the association between overall process and supporting devices. Our solution envisions to represent each sub-process with an area encompassing the geo-localized devices supporting it; its contour is defined by the most external devices, using a convex hull algorithm. The same colour will be used for filling the shapes representing sub-processes that belongs to the same process. The devices will be still represented as circles, with colour coding the level of endangerment; this time the radius will not be the same for all the devices, but will represent the importance that a device has for the supported sub-process. An example is visible in Figure 15.

To deal with the case in which a monolithic process has its supporting devices scattered through the map, an adaptive clustering algorithm based on K-means has been used; adaptation depends on the number of devices and the distance among them. In this way a

process can be split in artificial sub-processes; this solution proves useful to avoid situations where the area encompasses the whole visualization also in cases of a very low number of sparse devices.

To visually convey the impact of a compromised device on its supported process, the visualization uses the concept of **area corruption**. Each compromised device will produce a hole in the area representing the supported sub-process, hole that is proportional to the value of its operational impact score. If the sub-process is perfectly operative, the area will be totally filled. Conversely, if the sub-process is supported by compromised devices, particular parts of the area will disappear like they were corrupted. The extension of corrupted areas will be an immediate clue for the user about which device is most responsible for the loss of operational level. To highlight changes in the status of a process and alert the user, animation plays a key role. The corrupted areas will be represented as blinking areas, in order to give to the user information about evolution of the operational level of the process. The described behaviour is shown in Figure 16.

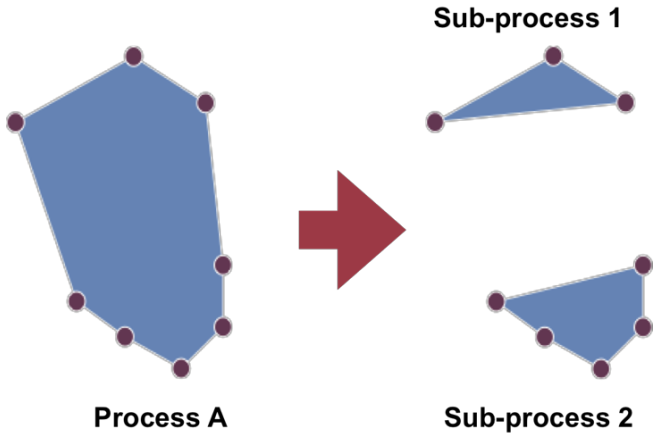


Figure 15 - The Process A is spawn over a too wide area;

it is then split in its constituting sub-processes. The two newly obtained areas cover much less space and allow for better inspection. Colour coding ties the sub-processes to the parent process

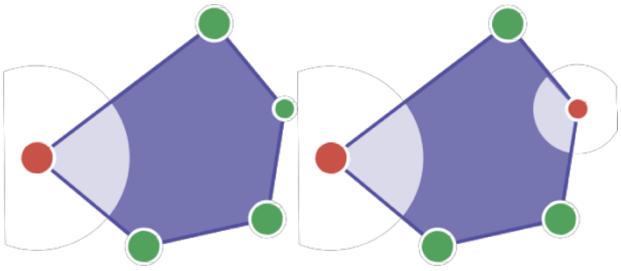


Figure 16 - Left: initial situation in which just the node on the left is compromised:

its weight (radius) is big, and also its operational impact (area of corruption). Right: a second node on the right become compromised; however, its weight and operational impact are limited

4.2.4 The prototype

This section describes the visual environment prototype that implements the design principles introduced in the previous section.

The prototype uses the MVC (Model-View-Controller) pattern, in order to achieve better encapsulation and to allow further modules to be developed and integrated in the current environment. Used technologies for the prototype include D3.js to plot organization's processes, network nodes and their relationships and the Leaflet framework to handle the map representation. When the prototype is started, the map with macro-zones and the primary cabins is shown to the user together with a sidebar (on the left) to control the activation of the different layers of analysis. The system presents the user with a quick overview of the status of the overall network at geographical level, allowing to drill down the analysis without losing the context; primary cabins are directly plotted on the map and, together with the aggregated risk visualization, represent the first analysis level provided by the system.

In order to maintain under control, the clutter resulting from the visualization of a high number of elements, when plotting the secondary cabins, the prototype implements a progressive drill-down/roll-up of the visualized resources. The user can drill-down/roll-up the geographical hierarchy and inspect the network nodes grouped by geographical entities (i.e., municipalities); conversely, the user can drilldown/roll-up the network nodes hierarchy and obtain a further refinement of analysis into the same geographical entity.

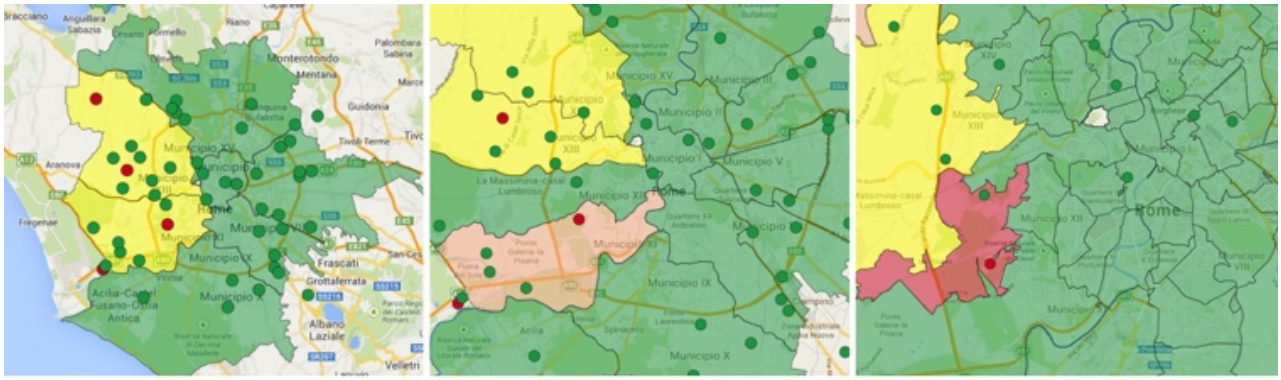


Figure 17 - The three geographic layers: 7 Rome Macrozones, 15 Municipalities, and 73 Zip codes

These two mechanisms are fully integrated and the user can refine the inspection by seamlessly using one or the other.

The geographic layer is a hierarchical layer (Figure 17) going from a macro-zones view (less specific) through a municipalities view to a zip codes view (more specific). Hovering mouse on a specific area makes visible its status, showing risk indicators. The mouse left-click on an area changes the geographic layer to a view that is more specific (where possible): for instance, left-clicking on a macro-zone transforms the geographic layer to the one with municipalities.

Conversely, the mouse right-click on an area changes the geographic layer to a less specific view.

In the same way, exploring the network nodes hierarchy allows an accurate analysis of the situation about the status of the network, moving from primary cabins to clusters of secondary cabins and from clusters to secondary cabins details (Figure 18).

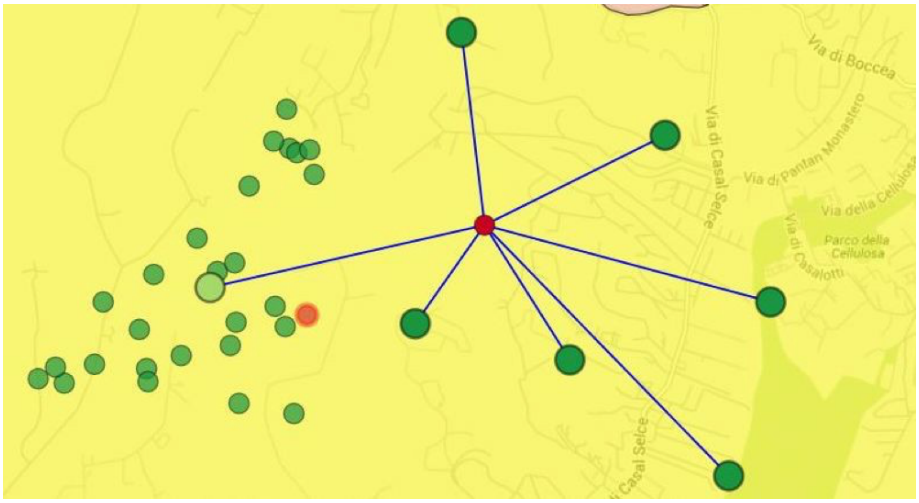


Figure 18 - The expanded view of a primary cabin into secondary cabin clusters (represented by their centroids) with the further expansion of a compromised cluster in the associated secondary cabins (left) in which the secondary cabin that is the source of failure pops up in red.

By right-clicking on one of primary cabins the user can expand it in the composing clusters of secondary cabins, organized in a Voronoi diagram; each Voronoi area will be computed on the centroid of a cluster of secondary cabins, and will have a colour representing the aggregated level of endangerment of the encompassed network nodes. Multiple selections are possible: the user can expand or collapse any of the inspected cluster/area, allowing the highlight of the interesting subset of resources. Colour coding and frequency of update are also two additional visual cues used in order to convey information: areas affected differently by attacks or vulnerabilities will be presented with red or yellow shade, depending on the severity of the threat. The colourcode is maintained during the exploration of the hierarchies, and serves as a hint for quickly highlight the areas that needs

The prototype encompasses several overlapping layers that can be included or excluded according to the user preferences. The layers in question are the map layer (cached Google Maps tiles), the geographic layer (which defines the bounds of the areas), the primary cabins layer (showing the status of each primary cabin, drawn by red or green circle marker), the clusters layer (useful in order to aggregate the secondary cabins linked to a primary one) and the secondary cabins layer (showing the status of each secondary cabin). Some interactions with the map add also other layers as the primary cabins logical links layer (showing the logical

network topology) and the already mentioned Voronoi diagram layer. The layering limits the number of details the user has to control at the same time, reducing the complexity of the visualization and increasing the efficiency of the user's response when a fast reaction is required. Such a combination of different hierarchy levels allows to monitor a network with thousands of nodes, insuring scalability and preserving the focus+context control (see the example in Figure 19).

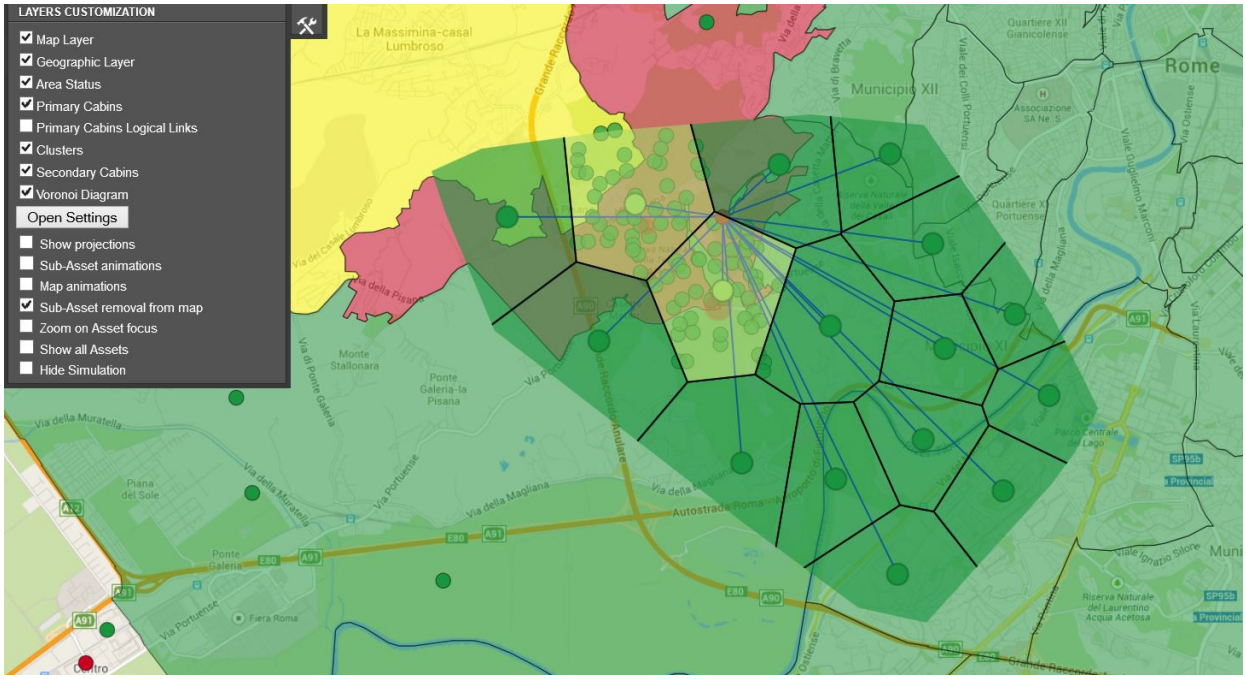


Figure 19 - A significant example in which all the layers (cabins, area status, Voronoi and logical links) are visible to the user, who can monitor the whole situation.

A 5-colour scale shows the level of endangerment of a specific node or of a geographic area. For aggregated elements (e.g., clusters, Voronoi, and geographic areas), a percentage function computes the colour according to the proportion of compromised nodes. Colours are assigned to each element of the layers by using the inner hierarchy: starting from the secondary cabins, which can either be red (compromised) or green (secure), the percentage function assigns colours to the Voronoi areas and clusters; the same function is used to assign the colour of the geographic areas: each area assumes a colour

4.2.5 Mission impact visualization

An additional layer of analysis is constituted by assessing the impact of a cyber-threat on the actual mission of an organization. In order to put in relation organization's processes information with network nodes status, the prototype provides additional visualizations organized in three main areas:

1. Mission selector and processes list area: this area contains summarized information on the overall level of the selected mission and associated processes;

2. Overview area: this area contains all the information described before for what concerns network status; its functionality is augmented with a visual association between business mission impact and network topology;
3. Context area: this area contains detailed information about organization's processes and their supporting network devices.

The mission selector and processes list area (see Figure 20) includes a panel containing the ordered list of business processes, each of them featuring its specific information: name, number of devices supporting the process, priority over the current mission, plus its endangerment and operational level, both expressed in percentage. On top area the mission selector is available; it allows the user to choose among different missions. As soon as the target mission changes, all business processes are reordered based on their priority level for the new selected mission.

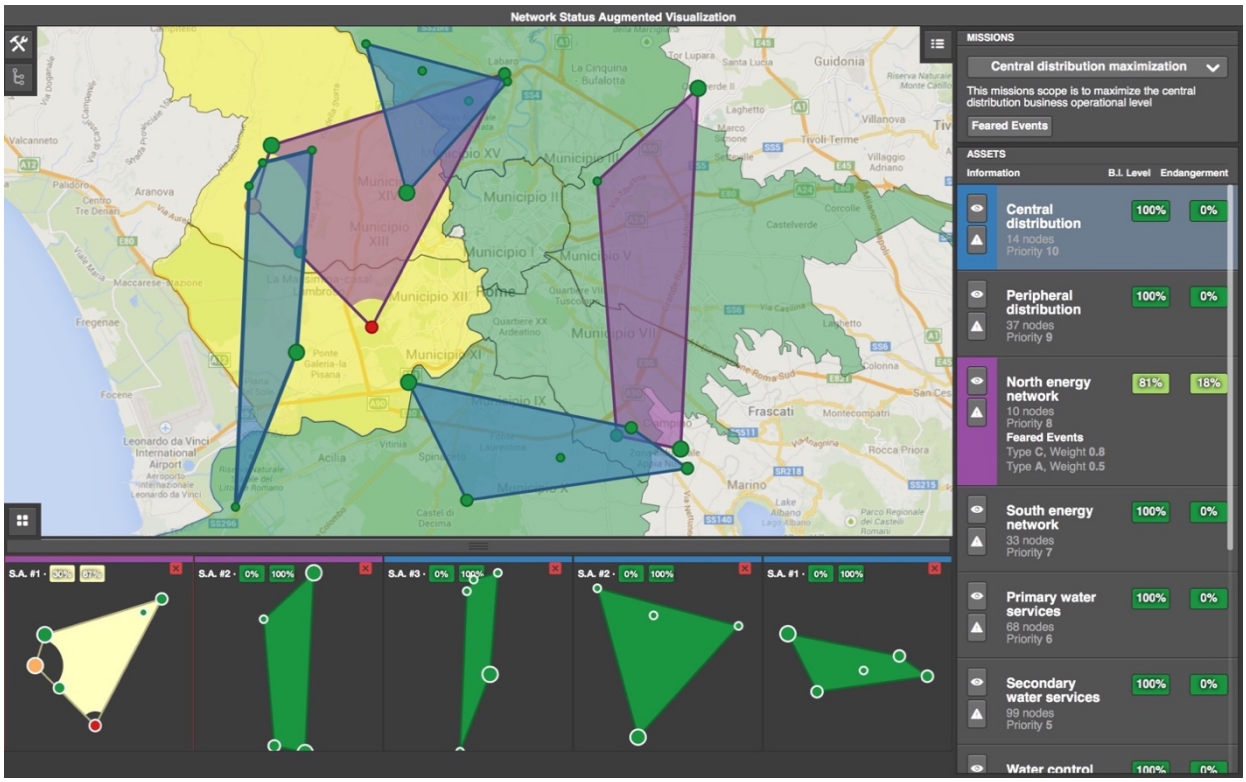


Figure 20 - Mission selector and ordered list of processes (right), overview area (center) and context area (bottom). The overview area contains three network fragments (in blue) associated with the Central Distribution process (100% functional) and two fragments (in violet) associated with the North Energy Distribution process (partially compromised), showing a sub-process impacted by compromised devices (red nodes).

In the Overview area, processes and their supporting sub-processes are displayed over the geographical layer, together with their supporting devices. Selecting a process from the list immediately highlights it over the geographical representation.

The Context area, triggered by clicking on a process, is visible in the lower part of the visualization and contains a detailed view of all the sub-processes of the selected processes, as shown in Figure 11. This contextual visualization rearranges the clusters based on both their spatial position and their parent process. In this visualization the colour of the area encodes the operational level of the sub-process, derived from the devices supporting it. The colour scale used is the RdYlGn, where a green fill shows a well operating resource, whilst a red fill identifies a critical situation. The colour of the bar present on the top represents the association with the parent process. To avoid to present the user with not relevant information, the prototype allows for showing just the processes with a lowered operational level, in contrast with presenting all of them. The user can always request to see the whole list of processes.

Figure 21 shows the importance of the relationship of compromised network nodes with supported business processes. On the top-left the expansion of the Voronoi area encompassing compromised nodes on the Rome south-west area is shown; it encompasses a fully compromised node, that we will label node A. On the bottom-left the supported business process layer is displayed; as visible in the enlarged Context Area in the bottom-right, even if node A is fully compromised (red colour), its contribution to the operational level of the supported process is marginal (as visible by the small corrupted area it creates in the shape representing the supported process). Conversely, the lightly compromised node B (on the left, represented with orange colour) results in a strong detrimental effect on operational level of the process: it needs to be fixed with a higher priority with respect to node A in order to restore the operational level of the supported process. Simply visualizing the network nodes level of endangerment cannot capture this insight. Basing the analysis on just level of endangerment, the security officer would have concentrated efforts on first fixing node A and much later node B. Instead, with mission impact information, the right priority in mitigating the attack can be pursued in order to fast recover the requested operational level of the involved processes.

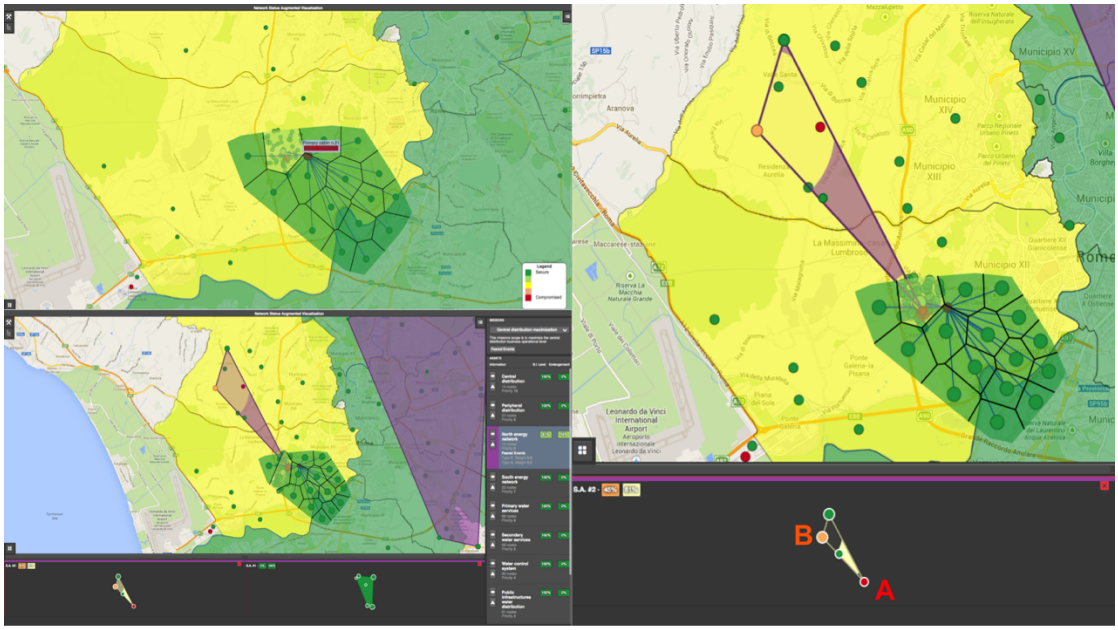


Figure 21 - Example of raising security officer's situational awareness by using mission impact visual representation

5 PERCIVAL: THE ATTACK GRAPH VA SOLUTION

The objectives of *situational awareness* are to fulfil at least three goals: *understanding the system* (what are its components, how do they communicate, what are their configurations, what are their known vulnerabilities, etc.), *understanding the security events that are happening on the system* (a web server has been compromised) and *what are their consequences* (what other devices are reachable when the attacker uses the compromised web server). The attack graph visualization, named PERCIVAL in the following, is a situational awareness tool that relies on attack graphs representation and offers in a unified way the understanding of the system configuration (proactive approach) as well as the evaluation of security events and their consequences (reactive approach). Based on the information provided by the orchestrated components of the PANOPTESEC system (architecture of the monitored system, details of its components configuration as well as collection, aggregation and correlation of the security events), PERCIVAL evaluates the risk level and proposes counter measures.

To our knowledge, PERCIVAL is the first visualization tool that provides in a unified way *proactive analysis* (attack path analysis considering path topology, likelihood and risk, inspection of automatically generated mitigation actions and forensics analysis of previous attack) and *reactive analysis* (analysis of the attack progress along the proactively computed attack paths, response plan analysis in terms of completion and efficacy of triggered mitigation actions, and predictive analysis, providing insights on the possible evolutions of attacks).

5.1 Comparison with related proposals

Attack graphs have been extensively studied (see reviews [62, 68] for instance) and are commonly recognized as being a very efficient tool to describe and evaluate the various attack scenarios against a system. However, as systems become more complex, attack graphs are increasingly difficult to understand and therefore to take benefit from. Visualization has been proposed to improve how humans understand them.

Some proposals addressed the representation of attack graphs in the proactive context, i.e., attack graphs that are built based on topology, configuration and known vulnerabilities of the system. NetSPA [61] is a complete tool to build attack graphs. It comprises a graphing subsystem component based on graphviz [59] that generates a visual representation of the computed attack graph. NetSPA graphing subsystem makes the attack graph simpler by pruning it: When a node is identified as a goal, every node that is reachable from that node is deleted; Similarly, paths that do not lead to a goal are deleted. While this approach efficiently simplifies the attack tree, it is based on the hypothesis that all of the attacker's goals have been properly identified, which might be a strong assumption in some cases. GARNET [73] extends this work by proposing another graph subsystem based on a treemap that reflects physical or logical topology and allows reachability display and evaluation through interactions. NAVIGATOR [57] has been proposed as an improvement to GARNET. It allows better zooming

(up to the node level), shows network infrastructure devices and includes client side, credential and trust-based threats.

Noel and Jajodia [65] address attack graphs usability through aggregation and interactions. Aggregation is performed following various rules such as “multiple exploits deal with the same attacker/victim couple”, “machines belong to the same subnetwork”, “a given device exhibits various vulnerabilities”, etc. User can also perform unaggregation to obtain details on parts of the attack graph. Noel et al. later extended this work with supplementary representations [64] such as adjacency matrices that offer other opportunities to drill-down into attack graphs and to evaluate the impact of changes in network configuration. [67] presented another extension of this work that allows to evaluate the consequences of hardening on the attack graph, the evaluation method being presented [66]. [60] proposed another simplification of attack graphs based on trimming ”useless”, i.e., redundant attack paths.

By contrast with PERCIVAL, these proposals only address the management of the static risk level: They do not help in evaluating the dynamic risk level, i.e., in monitoring the attacks that are happening on the system and the way they spread on it. This difference is especially relevant in recent contexts where attacks can start on almost any device with rapid expansion to the whole system, as it is the case with worms and botnets for instance.

Some other proposals addressed the reactive context. Mathew et al. [63] proposed a visualization tool that displays attack tracks based on security events detected by IDSes or collected in log files. As such, this tool helps security operators in understanding ongoing attacks and evaluating the dynamic risk level.

Vandenberghe presented NTE (Network Traffic Exploration) in [71], a tool which objective is to allow users to explore network traffic to search for attacks. Among numerous other representations, NTE proposes a representation that maps network events to networks diagrams. This mapping therefore displays the attack sequences. Users can obtain more information about proposed responses to attacks, secondary effects as well as operational and IT impacts.

Summarizing, the main differences of PERCIVAL compared to these previous contributions lies in the following points: First, PERCIVAL addresses both proactive and reactive contexts. Second, it relies both on visualization and on pre-computation to improve user’s understanding of the attack graph/situation. Third, it allows for countermeasures visual assessment.

5.2 Objectives and Context

PERCIVAL helps security operators *understand the current risk level of the system* and eases *incident response* by evaluating the effectiveness of counter-measures. Two types of risk levels are considered. First, the *static risk level* corresponds to the evaluation of known threats that exist against a system in the absence of attacks. It is computed based on the system architecture and configuration: what are the devices that compose the system, how are the

devices interconnected and connected to the other networks (often, the Internet), what are the deployed services, how are the devices and services configured, are there any known vulnerabilities against these devices, services and configurations, etc. Second, the *dynamic risk level* takes into consideration attacks that are currently happening. Computing the dynamic risk level therefore uses information about detected malicious activities and define what parts of the system are currently compromised. Compared to the *static risk level*, the dynamic risk level enables analysis of the consequences of successful attacks.

PERCIVAL follows a cyclic approach during which:

- Attack graphs are displayed to allow evaluation of the static and dynamic risk level,
- counter-measures are proposed, selected and deployed,
- new attack graphs and risk levels resulting from the deployed counter measures are computed and displayed.

PERCIVAL therefore helps security operators understand the static risk level of their system, what parts of the system are the most at risk, the consequences of this situation based on attack graphs and the location and the effectiveness of the deployed counter-measures. Furthermore, it displays dynamic events that elevate the risk level (e.g., attacks that are currently happening or changes in the topology) and help understand the potential consequences of these successful attacks thanks to attack graphs.

5.3 Attack Graphs

Attack graphs are a tool of choice to model and better understand the various possible successions of steps an attacker could perform to reach her objectives. In an attack graph, each step of an attack is represented by a node for which various granularities (sub-networks, devices, user privileges in devices, etc.) can be used.

In common attack graphs proposals, some specific nodes have been considered potential ultimate objectives by defenders and are flagged as being *goals* for the attacker. Other nodes are sometimes flagged as *entry points*, i.e., the first steps an attacker could reach to perform a complex attack.

Links between nodes represent the possible transitions for an attacker to go from one step of the attack to the next. This transition can be due to an action that would have been legitimate if performed by a legitimate user (for instance, connecting to a database from a web server) or to a successful attack.

In practice, nodes are flagged by the defender as being *goals* or *entry points* based on *a priori* estimations. However, it may be possible that an attacker has a specific goal that was not considered by the defender. Due to the large importance taken by client-based attacks such as phishing and local exploits for instance, it might also be very difficult to provide a relevant set of entry points. Similarly, links among nodes in the attack graph are created based on the knowledge the defender has of the system architecture, configuration, and known vulnerabilities. An attack graph could therefore be incomplete at a given time, for instance if

the attacker benefits from a zero-day exploit. Therefore, we advocate that a visualization system that ensures situational awareness should present information both about both the *static risk level* and the *dynamic risk level.*

5.4 Design Sketches

The PERCIVAL system represents attack graphs that are the set of attack paths computed by the system based on various characteristics of the network (e.g., vulnerabilities, connections, configurations, firewall rules, etc.). Nodes of the network are represented as circles labelled with their IPs, while black lines represent logical links (level 3) connecting them (see mock-up on Fig.22). In particular, a computed attack path is represented as an ordered sequence of connected nodes. The thickness of the edges encodes the static risk level tied to the path. The precomputed attack path that best matches the set of compromised nodes is represented as nodes connected by shaded red links. The detected attack sequence is represented by red links.

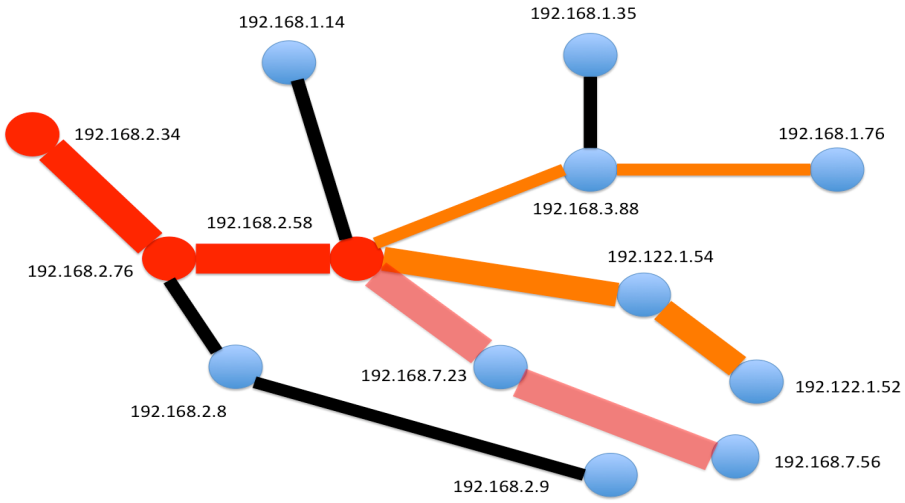


Figure 22 - Mock-up of the attack graph and attack sequence representation.

Black denotes edges for which no information about exploitability is present. Orange denotes computed attack paths (their union forms the attack graph), shaded red denotes the instantiated attack path and red denotes the last detected attack sequence.

In the reactive scenario of an ongoing attack, the focus of the system immediately shifts on the *last compromised node* (i.e., 192.168.2.58 on Figure 22). The set of outgoing links, both high risk edges (in orange) and the black unknown risk edges (in black) are highlighted. Highlighting the edges belonging to an attack path helps the security operator in understanding the mitigation actions that can be triggered by the system to stop the spreading of the attack. The highlight of the other links simply gives the operator information regarding nodes can be reached without belonging to any attack paths but could in fact be important.

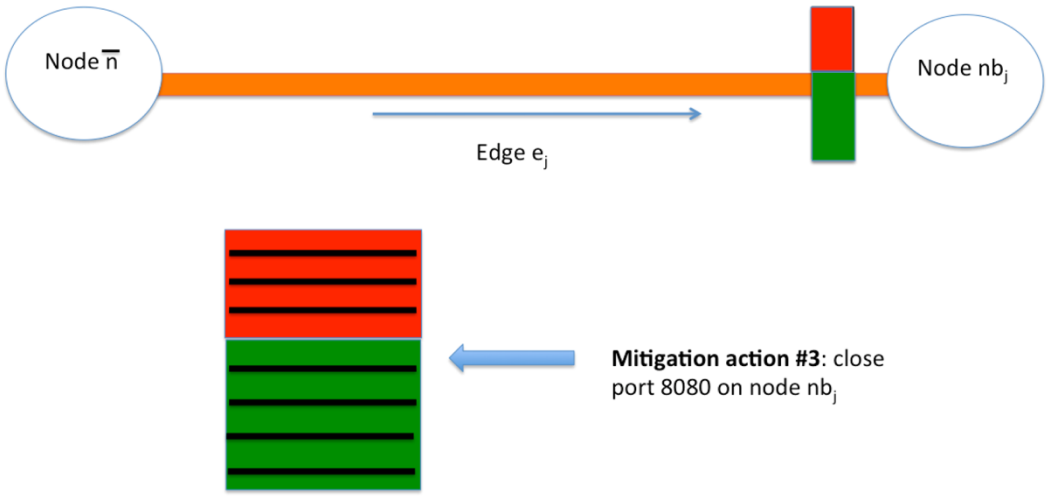


Figure 23 - A barrier of mitigation actions

with colour coding tied to their final state (green being successful, red unsuccessful) drawn on the corresponding edge and target node (top); mouse hovering on it (bottom) shows a detailed list of the mitigation actions.

The part of the *response plan* that is currently associated with the actual *attack sequence* is visualized by drawing a set of « barrier of mitigation actions », i.e., a rectangle whose dimension is proportional to the number of triggered mitigation actions (see Figure [2]) on high risk edges.

The initial colour of a barrier of mitigation actions is white, representing the state in which none of the mitigation actions has been deployed. As soon as an attack leads to a compromises, the system automatically starts deploying mitigation actions. As a result, the rectangle representing a barrier starts being filled with the proportion of mitigation actions correctly executed and mitigation actions that failed (due to external factors or factors tied to the particular attack).

5.5 Implementation

Figure 24 presents the overall PERCIVAL visual analytics environment.

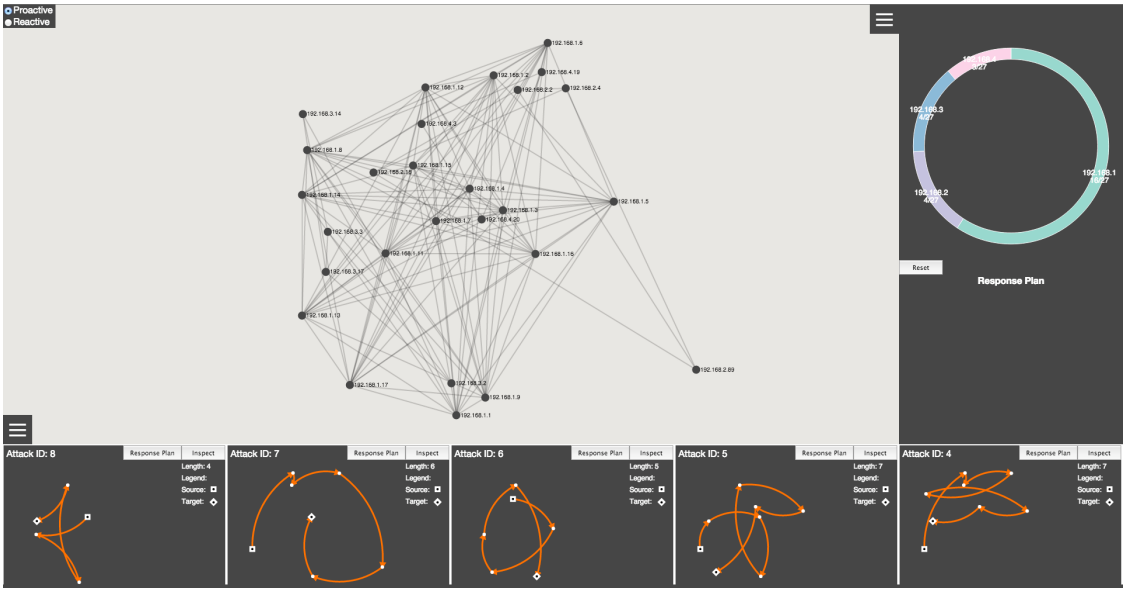


Figure 24 - The PERCIVAL main view.

It encompasses the following components:

- **Network Topology View**: This view presents the network topology. Each dot represents a device of the network (servers, routers, gateways, etc.) with logical links represented as black shaded arcs.
- **Attack path summary**: This view allows the security operator to review the various attack paths computed by the system.
- **Attack path details view**: This view allows the security operator to inspect in details the selected attack path.

All the visualizations are interactive and coordinated and follow the overview first-zoom & filter-details on demand paradigm, allowing the security operator to start the analysis on any of them and propagate the results on the others.

Following an ideal workflow of analysis, we describe the prototype functionalities first for the proactive mode, then for the reactive mode.

5.5.1 Proactive mode

In the proactive mode, the system is not currently under attack. The main goal of the security operator is therefore to review the attack paths computed by the system and their associated response plans.

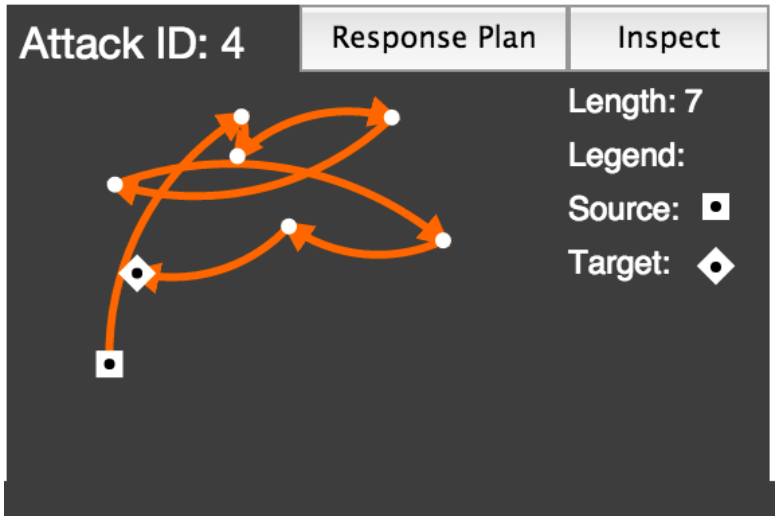


Figure 25 - Detailed view of an attack path;

the figure shows the sequence of nodes, the path length, source and target nodes. It also allows for animating the attack steps (“Inspect" button) or to review the linked response plan (“Response Plan" button).

Every time a new attack path is computed, it is inserted in the *attack path summary* list at the bottom of the main view. Figure 25 shows an example of an attack path representation. The attack path is represented as nodes connected by orange edges. Different symbols are used for the source and the target nodes. On the right, the length of the path is reported. The “inspect" button allows for animating the path to better convey the steps sequence to the user. When the security operator selects one or more attack paths, these attack paths are drawn in the Network Topology view and the Attack path details view, as shown on Figure 26. The thickness of the edges encodes the static risk level associated with the attack path, improving the security operator awareness about the attack paths that are more likely to be exploited.

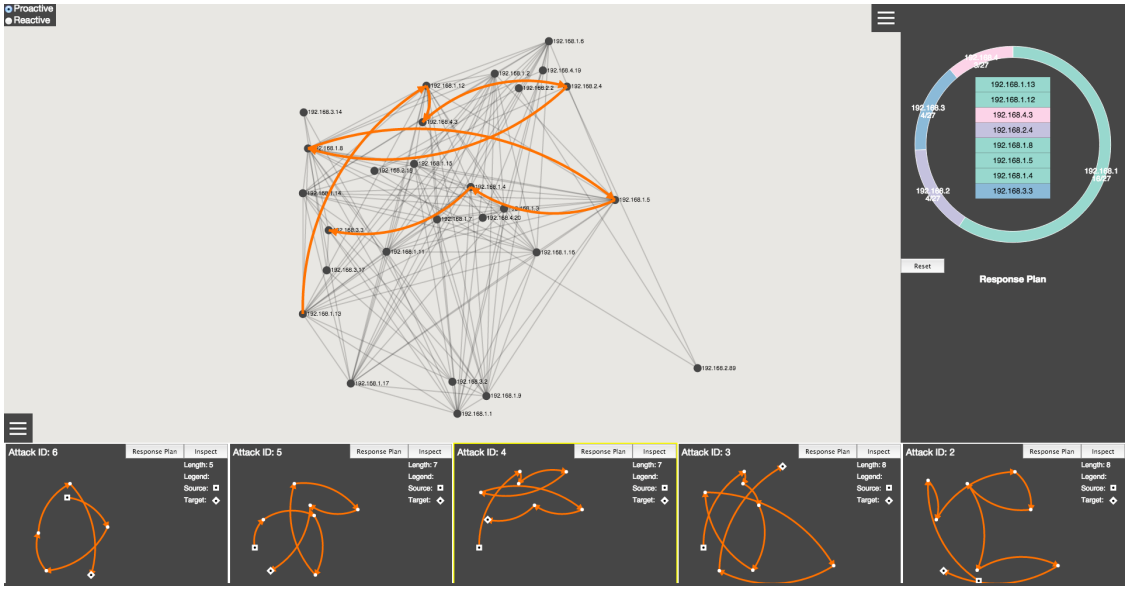


Figure 26 - Visualizing a selected attack path in the network topology view. The thickness of the arcs encodes the static risk level.

In order to better explore and inspect each attack path, the security operator is able to interact with the attack path detailed view. This view is made of two main elements, the Network Inspector and the Attack Table. The Network Inspector is represented as a Donut Chart that represents the composition of the network topology by its sub-networks. Hovering on each of them triggers the visualization of the corresponding sub-network in the Topology Network View. Moreover, it highlights the subset of nodes of the attack path that belongs to the selected sub-network. Finally, an additional tiny arc is drawn near the selected one, representing the proportion of nodes of the sub-network that belong to the attack path.

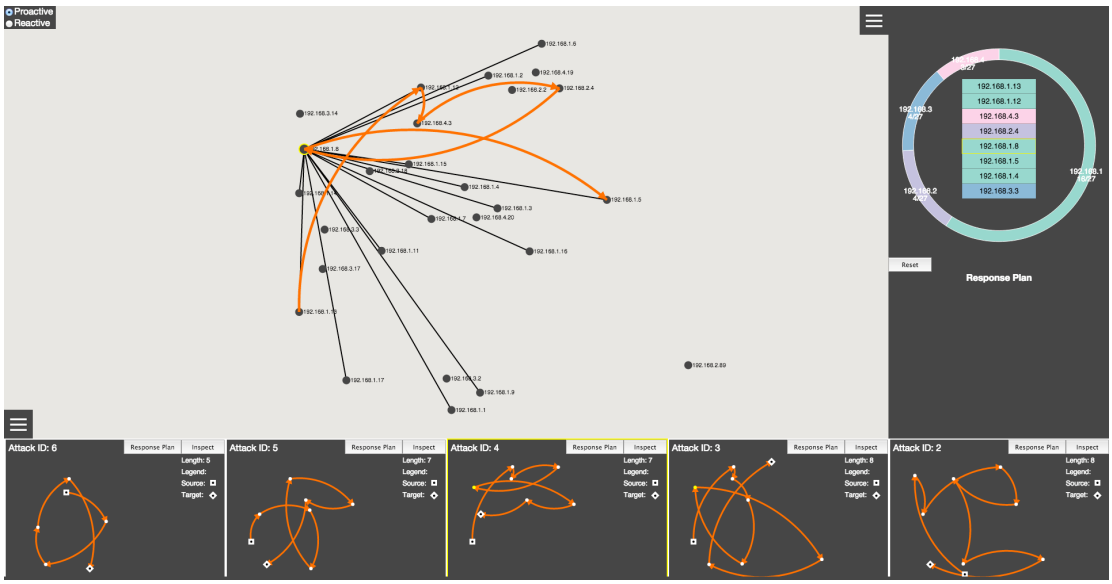


Figure 27 - Inspection of an attack path at nodes level.

Clicking on a node will trigger view the visualization of the attack path up to the selected node on the network topology, with all the possible outgoing edges, as shown in Figure 27. The security operator can therefore inspect both the possible evolution of the attack (avoiding cluttered visualization) and the connectivity of each node on the attack path. Finally, by clicking on the “Response Plan" button, the security operator can inspect the computed response plan, as shown in Figure 28, getting details as types of mitigation actions and interested nodes. Attack paths in the Attack Path summary are ordered according to their static risk (giving importance to the most dangerous).

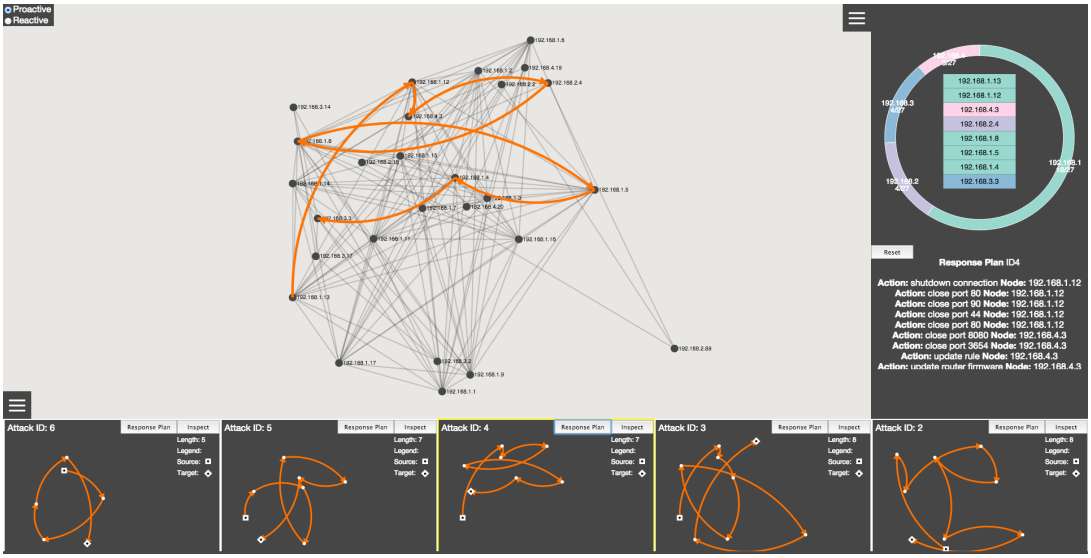


Figure 28 - By clicking on the “Response Plan" button of an attack path, the user can inspect in details the composition of the plan.

5.5.2 Reactive mode

The reactive mode is automatically selected when an attack is detected. The visual environment remains the same, while the system focuses the attention of the security operator towards the most relevant nodes and edges. The sequences of alerts are matched with the precomputed attack paths by the PANOPTESEC correlation system that produces a list of attack paths, ordered by probability. PERCIVAL represents the actual attack sequence in in full red and the most probable attack path in shaded red so as to both parts: on one hand the security operator has a prediction of the possible evolution of the attack; on the other, he can check the attacked nodes and explore additional details (see Figure 29).

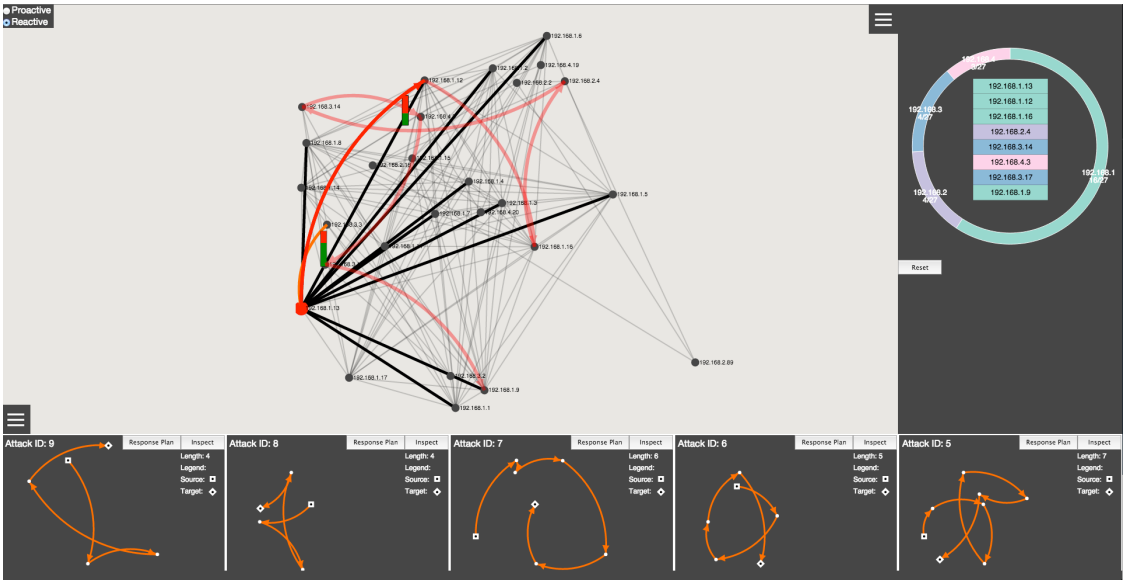


Figure 29 - PERCIVAL allows predicting possible evolutions.

For each compromised node the list of outgoing edges will be visualized using this colour coding rationale: in red, edges belonging to the attack sequence, in shaded red, those belonging to the most probable precomputed attack path, in orange, edges that belong to any other precomputed attack paths, and in black, those that do not belong to any attack path but for which a network path exists. For attacks paths, a *barrier of mitigation actions* is displayed near the target node connected to the compromised node by one of the aforementioned edges. This barrier represents the portion of mitigation actions that affects directly the target node, and that will be immediately deployed; colour coding is associated with the two possible states: green to successful, meaning that the deployment of the mitigation action completed, and red to failed, meaning the mitigation action failed to complete. The barrier is animated and reports the proportion of mitigation actions that successfully completed and the ones that did not, giving immediate feedback to the security operator on the outcome of the corrective measures against the spreading of the attack.

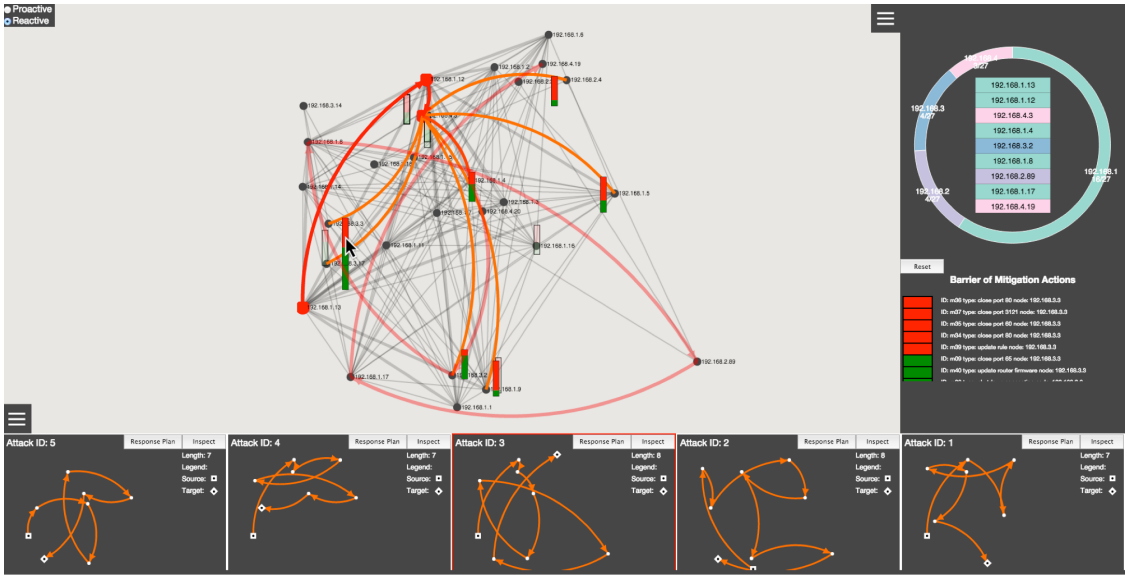


Figure 30 - By clicking on one of the barrier of mitigation actions in the network topology view, the security operator can inspect its details on the right, like ID, category and target node.

By clicking on a barrier, the user can inspect the single mitigation actions, (see an example on Figure 30). Black edges do not belong to any attack path and do not have any precomputed set of mitigation actions. However, the possibility for the security operator to cut them is offered. This will help the security operator when the ongoing attack diverges from any precomputed situation, like in the case of a zero-day attack.

Outcomes of this scenario can be classified in three main cases:

- *Barriers totally green and attack stopped.* This scenario represents the success of the response plan against the attack. All barriers are green and the attack neutralization is also visible and contained in the area delimited by barriers.
- *Barriers totally green and attack keeps going on.* In this case the information provided is the ineffectiveness of (some of) the precomputed response plan. Security operator, after the neutralization of the attack, should review again the plan, trying to understand why mitigation actions did not stop the attack.
- *Barriers with red parts and attack still going on.* Not all the mitigation actions have been successfully executed, and the attack keeps spreading. Attention will focus on the next compromised node, while plan should be reviewed to discover possible reasons of failure.

To increase the scalability of the solution, two techniques are available in the PERCIVAL system:

- among the promoted attack paths, only the edges that are directly connected to the instantiated attack path will be drawn on the network graph;

- an adaptive threshold is used to reduce the number of attack paths promoted to be visualized.

Moreover, the instantiated attack path is always visualized in its full length, giving the security operator a strong advice on the most probable attack spread.

5.6 Evaluation

We evaluated PERCIVAL with interviews assessing Feature set utility and innovations, Usability and learnability and User experience and preference.

In particular, we conducted a user study to evaluate PERCIVAL, involving network security experts from the ACEA Italian organization. ACEA provides power and water purification services to cities in central Italy (millions of end users) and is the PANOPTESEC user stakeholder. It is worth noting that such experts are exactly the users the system is intended for: the tool's goal is to contribute to situational awareness for critical infrastructure, like the ACEA one. In particular, 7 experts (1 female and 6 males) were involved in the study. The study was conducted using a synthetic dataset that represents well the characteristics of the ACEA infrastructure. The goal of the study was to assess a) the PERCIVAL innovation and b) the comprehensibility and efficacy of the proposed visualization.

5.6.1 Methodology

Before starting the study, the experts were instructed through an oral presentation about PERCIVAL background and a practical use of the system was demonstrated. After that, participants were allowed to use PERCIVAL for 20 minutes, freely playing with the system functionalities and reporting their opinions on a questionnaire.

The questions had a Likert scale interval ranging from 1 to 5, in which each numerical score was labelled with a description: **1:not at all, 2:a little, 3:enough, 4:a lot, 5:quite a lot**. The following questions were asked:

- Is the addressed problem relevant for the involved stakeholders?
- Are the proposed visualizations adequate for dealing with the addressed problem?
- Do the tools and techniques currently used in ACEA for dealing with the addressed problem offer interactive and advanced visualizations?
- Is the proposed visual tool clear and understandable?
- Is the proposed visual tool effective for dealing with the addressed problem?
- To what extent will the proposed visual tool enhance the productivity of the involved stakeholders (SOC/SCADA operators, security operators)?

An open field allowed participants to report comments and suggestions.

The first three questions had the goal of collecting opinions about the relevance of the addressed problem (Q1), the PERCIVAL adequateness (Q2) and the degree of interactiveness (Q3) of the visual tools used within ACEA for the same purpose. The last three questions were aimed at assessing the PERCIVAL understandability (Q4), effectiveness (Q5), and efficiency (Q6).

5.6.2 Results

The questionnaire results are depicted in Figure 10, which presents the distribution of the answers.

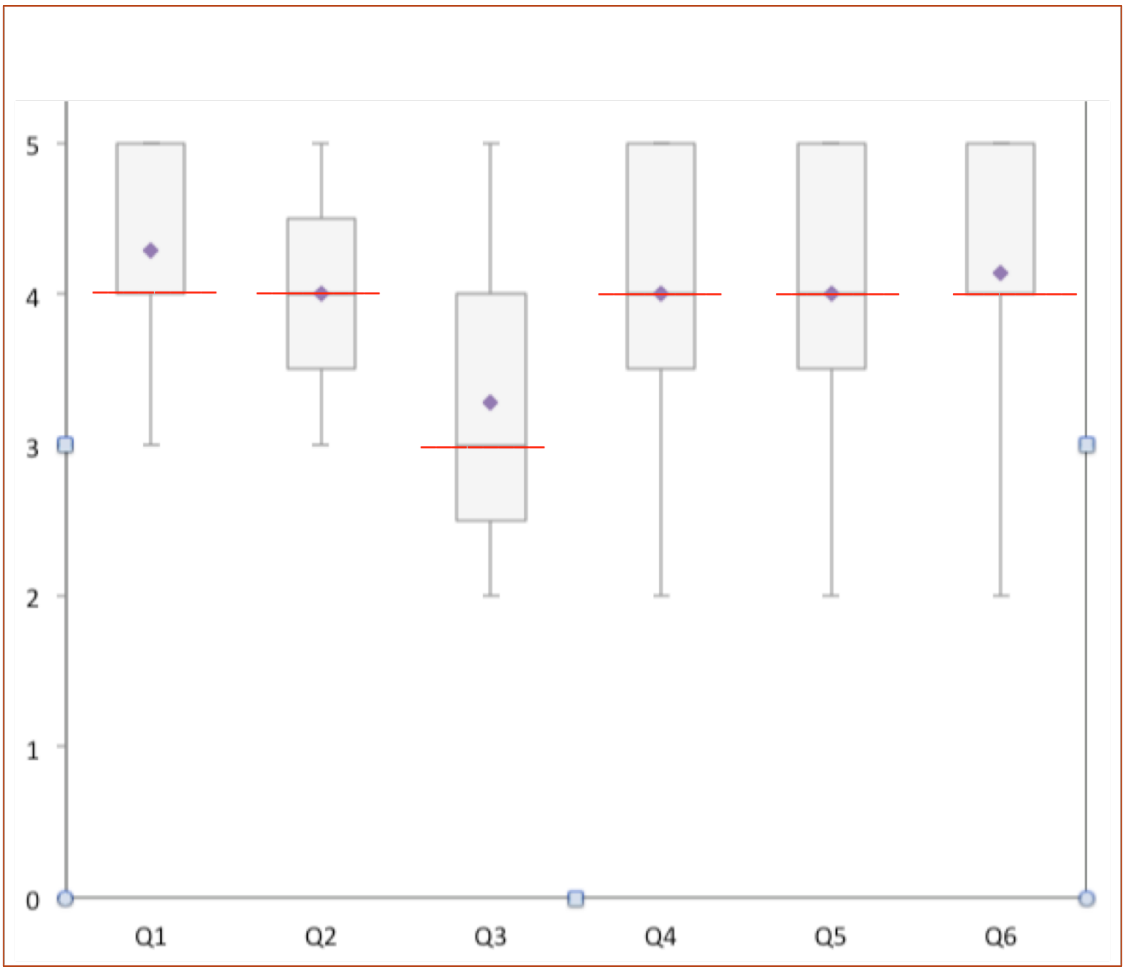


Figure 31 - Box plots reporting the PERCIVAL validation results; diamond markers represent averages and red lines show the medians.

Figure 31 allows to conclude that the addressed problem has been judged relevant by the involved stakeholders (85% of the 7 answers to Q1 are in the range [4, 5] with mean=4.29 and STD=0.76) and that the visualizations used within PERCIVAL are adequate (71% of the 7 answers to Q3 are in the range [4,5] with mean=4.00 and STD=1.11) and that used tools within ACEA are offering an average interactivity (85% of the 7 answers to Q3 are in the range [2, 4] with mean=3.29 and STD=0.76). According to the experts' opinion, PERCIVAL is therefore proposing something quite new in the field. We can also conclude that the tool is

understandable (71% of the 7 answers to Q4 are in the range [4, 5], mean=4.00 and STD=1.15), effective (71% of the 7 answers to Q5 are in the range [4, 5], mean=4.00 and STD=1.15), and can increase the operators' productivity (85% of the 7 answers to Q6 are in the range [4, 5], mean=4.14 and STD=1.07).

The study results give clear indications on the usefulness and the innovation of the PERCIVAL system. However, while one person out 7 was acknowledging the problem relevance (Q1=4) and was quite confident about the visualization adequateness (Q2=3) has been quite disoriented by the visualization (Q4=Q5=Q6=2). An informal discussion confirmed some usability issues (e.g., the continuous animation on the bottom was rising change blindness issues) and some misunderstanding about the "likelihood" term. This feedback provided furthers insights to improve the PERCIVAL systems.

5.6.3 Conclusion

PERCIVAL is a visual analytics tool relying on attack graphs that allows security operators to understand both the static risk level and the dynamic risk level of the system they monitor. It provides better understanding and reduction of the risks faced by the system both in the absence of attacks and when under attacks. allows to reduce them while it also allows security operators to monitor security events that happen on the system, to understand their possible consequences and to evaluate potential mitigation. The results of the user evaluation showed that PERCIVAL addresses a relevant problem, is innovative, understandable and efficient.

6 COORDINATED AND PARALLEL VIEWS

The research results described in the previous sections have been engineered and tailored to fulfil the PANOPTESEC requirements (See D6.1.1 and D6.3.1). The actual implementation of the Visualization Component has been deployed within the Liferay portlet container that provides not only basic architectural components (e.g., security layer, authentication layer, communication layer among users, role management, etc.) but also high integration flexibility, allowing for easily arranging different visualization in the same page and exchanging information among them, fostering the implementation of the parallel and coordinated view paradigm. This constitute a powerful added value, allowing the composition of different visualization in order to show different aspects of the same complex situation. As an example, Figure 32 shows an interaction with the system in which the System Manager is inspecting the sub-network 192.168.1. In the vulnerability view, bottom left, it is possible to analyze the vulnerability affecting the nodes of the sub-network, getting an overview of their frequency an inspecting/comparing their CVSS scores. Using the multiple coordinated view approach, the same sub-network is selected on the other three views:

1. The geographic view, upper left, shows the location of such composite node, making clear the layer 3 links with other isolated node on the map;
2. The topological view, bottom right, highlight with the blue color the nodes of the sub-network, allowing for inspecting details about nodes, interfaces, links, and reachability submatrixes (all the nodes reachable by a single node);
3. The attack graph view allows for inspecting the attack graph (proactive in the example) associated with the vulnerabilities shown in the vulnerability view.

The Liferay environment allows for dynamically arranging two or more views on the same page, automatically enabling the synchronization among them. This provides the means for setting different views combinations according to user preferences in order to address different and complex analysis scenarios.

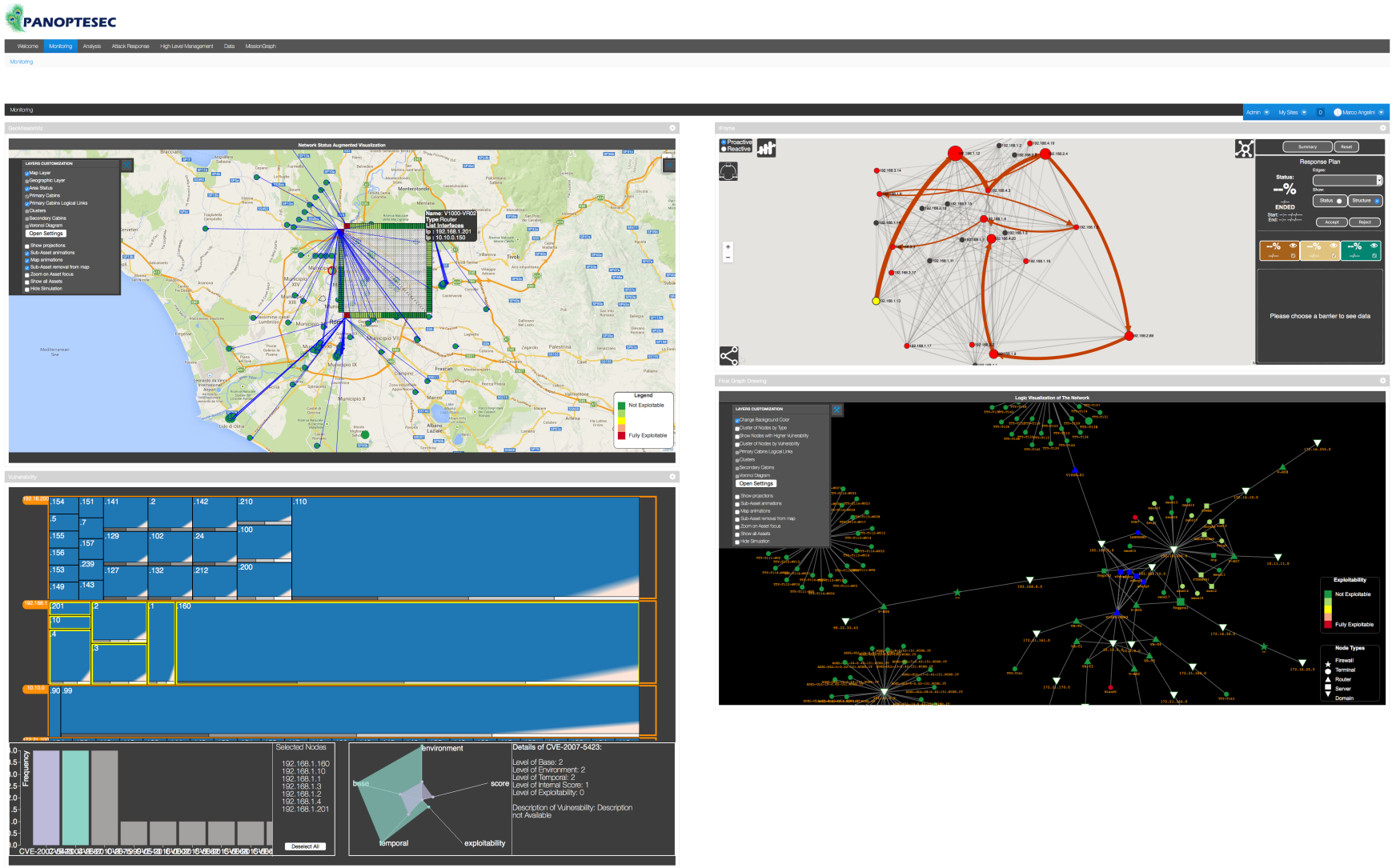


Figure 32 - Screenshot coming from the ACEA premises, (4k' monitor) showing four views cooperating to solve a complex analysis

7 CONCLUSION

This report presented the main visualization scientific results and implemented VA systems produced during the PANOPTESEC project lifecycle. Such results have been engineered and tailored within the visual component prototype that constitutes the user interface of the PANOPTESEC system. The next project steps foresee a strong validation of the full system with ACEA technicians, with the main goal of validating the synergy of the integrated and coordinate visualizations.

8 BIBLIOGRAPHY

PANOPTESEC reports and deliverables

[D2.1.1] PANOPTESEC Consortium, *"Deficiency Evaluation", Project deliverable D2.1.1*, Version 1.0, 28.04.2014

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

[D3.1.2] PANOPTESEC Consortium, *"System High Level Design", Project deliverable D3.1.2*, Version 2.0, 27.03.2015

[D4.1.1] PANOPTESEC Consortium, *"Data Collection and Correlation Requirements", Project deliverable D4.1.1*, Version 2.0, 27.03.2015

[D4.2.2] PANOPTESEC Consortium, *"Data Collection and Correlation Components Prototypes II", Project deliverable D4.2.2,* Version 1, 31.10.2015

[D4.2.2R] PANOPTESEC Consortium, *"Data Collection and Correlation Components Prototypes II, Verification Report", Project deliverable D4.2.2,* Version 1, 06.04.2016

[D4.3.1] PANOPTESEC Consortium, *"Data Collection and Correlation Integration Prototype", Project deliverable D4.3.1,* Version 1, 30.06.2016

[D4.3.1R] PANOPTESEC Consortium, *"Data Collection and Correlation Integration Prototype Verification Report", Project deliverable D4.3.1,* Version 1, 30.06.2016

[D5.1.1] PANOPTESEC Consortium, *"Response System for Dynamic Risk Management Requirements", Project deliverable D5.1.1*, Version 2.1, 27.03.2015

[D5.1.2] PANOPTESEC Consortium, *"Response System for Dynamic Risk Management Models and High-Level Design", Project deliverable D5.1.2*, Version 1.0, 31.10.2014

[D5.2-3.3] PANOPTESEC Consortium, *"Proactive/Reactive Response System Components Prototypes II", Project deliverable D5.3.3, D5.2.3,* Version 1, 31.10.2015

[D5.2-3.3R] PANOPTESEC Consortium, *"Proactive/Reactive Response System Components Prototypes II, Verification Report", Project deliverable D5.3.3, D5.2.3,* Version 1, 06.04.2016

[D6.1.1] PANOPTESEC Consortium, *"Visualization Requirements", Project deliverable D6.1.1*, Version 2.0, 27.03.2015

[D6.2.2] PANOPTESEC Consortium, *"Visualization System Components Prototypes II", Project deliverable D6.2.2,* Version 1, 31.10.2015

[D6.2.2R] PANOPTESEC Consortium, *"Visualization System Components Prototypes II, Verification Report", Project deliverable D6.2.2,* Version 1, 06.04.2016

[D6.3.1R] PANOPTESEC Consortium, *"Visualization Integration Prototype Verification Report", Project deliverable D6.3.1,* Version 1, 30.06.2016

[D7.2.2] PANOPTESEC Consortium, *"Integration Framework Prototype II", Project deliverable D7.2.2,* Version 1, 31.10.2015

[D7.2.2R] PANOPTESEC Consortium, *"Integration Framework Prototype II Verification Report", Project deliverable D7.2.2,* Version 1, 06.04.2016

[D7.3.1] PANOPTESEC Consortium, *"Integration Framework Prototype II", Project deliverable D7.3.1,* Version 1, 30.06.2016

[D7.3.1R] PANOPTESEC Consortium, *"Integration Framework Prototype II Verification Report", Project deliverable D7.3.1,* Version 1, 30.06.2016

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

Papers

[1] M. Angelini, N. Prigent, and G. Santucci. Percival: proactive and reactive attack and response assessment for cyber incidents using visual analytics. In Visualization for Cyber Security (VizSec), 2015 IEEE Symposium on, pages 1–8. IEEE, 2015.

[2] P. Barford, M. Dacier, T. G. Dietterich, M. Fredrikson, J. Giffin, S. Jajodia, S. Jha, J. Li, P. Liu, P. Ning, et al. Cyber sa: Situational awareness for cyber defense. In Cyber Situational Awareness, pages 3–13. Springer, 2010.

[3] R. Bearavolu, K. Lakkaraju, W. Yurcik, and H. Raje. A visualization tool for situational awareness of tactical and strategic security events on large and complex computer networks. In Military Communications Conference, 2003. MILCOM '03. 2003 IEEE, volume 2, pages 850–855 Vol.2, Oct 2003.

[4] R. Blanch and E. Lecolinet. Browsing zoomable treemaps: Structureaware multi-scale navigation techniques, Nov 2007.

[5] Checkpoint Software solutions ltd. Ckeckpoint Next Generation SmartEvents. https://www.checkpoint.com/products/ smartevent/.

[6] M. Chu, K. Ingols, R. Lippmann, S. Webster, and S. Boyer. Visualizing attack graphs, reachability, and trust relationships with navigator. In Proceedings of the Seventh International Symposium on Visualization for Cyber Security, pages 22–33. ACM, 2010.

[7] G. Conti. Security data visualization: graphical techniques for network analysis. No Starch Press, 2007.

[8] F. Fischer, J. Davey, J. Fuchs, O. Thonnard, J. Kohlhammer, and D. A. Keim. A visual analytics field experiment to evaluate alternative visualizations for cyber security applications. In Proc. of the EuroVA International Workshop on Visual Analytics, 2014.

[9] L. Harrison, R. Spahn, M. Iannacone, E. Downing, and J. R. Goodall. Nv: Nessus vulnerability visualization for the web. In Proceedings of the Ninth International Symposium on Visualization for Cyber Security, pages 25–32. ACM, 2012.

[10] IBM. IBM Qradar. http://www-03.ibm.com/software/products/en/qradar.

[11] Imperva. Imperva SecureSphere. http://www.imperva.com/Products/WebApplicationFirewall.

[12] R. P. Lippmann and K. W. Ingols. An annotated review of past papers on attack graphs. Prepared for the Department of the Air Force under Contract F19628-00-C-0002, Mar. 2005.

[13] F. Mansmann, F. Fischer, D. A. Keim, and S. C. North. Visual support for analyzing network traffic and intrusion detection events using treemap and graph representations. In Proceedings of the Symposium on Computer Human Interaction for the Management of Information Technology, page 3. ACM, 2009.

[14] MITRE. Common vulnerabilities and exposures (cve) list, 2015.

[15] NIST. https://nvd.nist.gov/cvss.cfm, 2015.

[16] S. Noel and S. Jajodia. Managing attack graph complexity through visual hierarchical aggregation. In Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security, VizSEC/DMSEC '04, pages 109–118, New York, NY, USA, 2004. ACM.

[17] RSA enVision. RSA enVision. http://www.emc.com/support/rsa/eops/siem.htm.

[18] V. Shandilya, C. B. Simmons, and S. Shiva. Use of attack graphs in security systems. Journal of Computer Networks and Communications,2014, Oct. 2014.

[19] H. Shiravi, A. Shiravi, A. Ghorbani, et al. A survey of visualization systems for network security. Visualization and Computer Graphics, IEEE Transactions on, 18(8):1313–1329, 2012.

[20] The PANOPTESEC Consortium. The Official Website of the PANOPTESEC Project, http://www.PANOPTESEC.eu/, 2014.

[21] VisiTrend. VisiTrend. http://visitrend.tumblr.com/.

[22] M. Wagner, F. Fischer, R. Luh, A. Haberson, A. Rind, D. A. Keim, and W. Aigner. A survey of visualization systems for malware analysis. In EG Conference on Visualization (EuroVis)-STARs, pages 105–125, 2015.

[23] C. Ware. Information Visualization: Perception for Design. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2004.

[24] L. Williams, R. Lippmann, and K. Ingols. An interactive attack graph cascade and reachability display. In VizSEC 2007, pages 221–236. Springer, 2008.

[25] The Official Website of the PANOPTESEC Project, http://www.PANOPTESEC.eu/, 2014.

[26] P. Barford, M. Dacier, T. G. Dietterich, M. Fredrikson, J. Giffin, S. Jajodia, S. Jha, J. Li, P. Liu, P. Ning, et al. Cyber SA: Situational awareness for cyber defense. Springer, 2010.

[27] R. Bearavolu, K. Lakkaraju, W. Yurcik, and H. Raje. A visualization tool for situational awareness of tactical and strategic security events on large and complex computer networks. In Military Communications Conference, 2003. MILCOM'03. 2003 IEEE, volume 2, pages 850–855. IEEE, 2003.

[28] S. C. Carroll. Mission impact analysis visualization for enhanced situational awareness. Technical report, DTIC Document, 2008.

[29] V. Y. Chen, S. Ko, D. S. Ebert, C. Z. Qian, and A. M. Razip. Semanticprism: A multi-aspect view of large high-dimensional data: Vast 2012 mini challenge 1 award: Outstanding integrated analysis and visualization. In Proceedings of the 2012 IEEE Conference on Visual Analytics Science and Technology (VAST), VAST '12, pages 259–260, Washington, DC, USA, 2012. IEEE Computer Society.

[30] S. Creese, M. Goldsmith, N. Moffat, J. Happa, and I. Agrafiotis. Cybervis: visualizing the potential impact of cyber attacks on the wider enterprise. In Technologies for Homeland Security (HST), 2013 IEEE International Conference on, pages 73–79. IEEE, 2013.

[31] A. D'Amico and M. Larkin. Methods of visualizing temporal patterns in and mission impact of computer security breaches. In DARPA Information Survivability Conference & Exposition II, 2001. DISCEX'01. Proceedings, volume 1, pages 343–351. IEEE, 2001.

[32] A. D'Amico and S. Salas. Visualization as an aid for assessing the mission impact of information security breaches'. In DARPA Information Survivability Conference and Exposition, 2003. Proceedings, volume 2, pages 190–195. IEEE, 2003.

[33] M. Dodge. Building an atlas of cyberspace. Cartographic Perspectives, (34):47–52, 1999.

[34] R. F. Erbacher. Visualization design for immediate high-level situational assessment. In Proceedings of the Ninth International Symposium on Visualization for Cyber Security, pages 17–24. ACM, 2012.

[35] U. Franke and J. Brynielsson. Cyber situational awareness–a systematic review of the literature. Computers & Security, 46:18–31, 2014.

[36] C. Gates and S. Engle. Reflecting on visualization for cyber security. In ISI, pages 275–277, 2013.

[37] N. Giacobe and S. Xu. Geovisual analytics for cyber security: Adopting the geoviz toolkit. In Visual Analytics Science and Technology (VAST), 2011 IEEE Conference on, pages 315–316, Oct 2011.

[38] J. R. Goodall and M. Sowul. Viassist: Visual analytics for cyber defense. In Technologies for Homeland Security, 2009. HST'09. IEEE Conference on, pages 143–150. IEEE, 2009.

[39] M. Gr´egoire and L. Beaudoin. Visualisation for network situational awareness in computer network defence. Visualisation and the Common Operational Picture, pages 20–1, 2005.

[40] M. R. Grimaila, R. F. Mills, and L. W. Fortson. Improving the cyber incident mission impact assessment (cimia) process. In Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead, CSIIRW ’08, pages 32:1–32:2, New York, NY, USA, 2008. ACM.

[41] F. Hardisty and A. C. Robinson. The geoviz toolkit: using component-oriented coordination methods for geographic visualization and analysis. International Journal of Geographical Information Science, 25(2):191–210, 2011.

[42] M. Angelini and G. Santucci. Visual cyber situational awareness for critical infrastructures. In Proceedings of ACM VINCI '15, August 24-26, 2015, Tokyo, Japan.

[43] D. Auber, Y. Chiricota, F. Jourdan, and G. Melan_con. Multiscale visualization of small world networks. In Proceedings of the Ninth Annual IEEE Conference on Information Visualization, INFOVIS'03, pages 75-81, Washington, DC, USA, 2003. IEEE Computer Society.

[44] R. Borgo, J. Kehrer, D. H. Chung, E. Maguire, R. S. Laramee, H. Hauser, M. Ward, and M. Chen. Glyph-based visualization: Foundations, design guidelines, techniques and applications. Eurographics State of the Art Reports, pages 39-63, May 2013. http://diglib.eg.org/EG/DL/conf/EG2013/stars/039-063.pdf.

[45] J. Buchmller, D. Jckle, F. Sto_el, and D. A. Keim. SpaceCuts: Making Room for Visualizations on Maps. In E. Bertini, N. Elmqvist, and T. Wischgoll, editors, EuroVis 2016 - Short Papers. The Eurographics Association, 2016.

[46] V. Y. Chen, S. Ko, D. S. Ebert, C. Z. Qian, and A. M. Razip. Semanticprism: A multi-aspect view of large high-dimensional data: Vast 2012 mini challenge 1 award: Outstanding integrated analysis and visualization. In Proceedings of the 2012 IEEE Conference on Visual Analytics Science and Technology (VAST), VAST '12, pages 259-260, Washington, DC, USA, 2012. IEEE Computer Society.

[47] S. Creese, M. Goldsmith, N. Mo_at, J. Happa, and I. Agra_otis. Cybervis: visualizing the potential impact of cyber attacks on the wider enterprise. In Technologies for Homeland Security (HST), 2013 IEEE International Conference on, pages 73-79. IEEE, 2013.

[48] A. D'Amico and M. Larkin. Methods of visualizing temporal patterns in and mission impact of computer security breaches. In DARPA Information Survivability Conference & Exposition II, 2001. DISCEX'01. Proceedings, volume 1, pages 343-351. IEEE, 2001.

[49] A. D'Amico and S. Salas. Visualization as an aid for assessing the mission impact of information security breaches'. In DARPA Information Survivability Conference and Exposition, 2003. Proceedings, volume 2, pages 190-195. IEEE, 2003.

[50] N. Giacobe and S. Xu. Geovisual analytics for cyber security: Adopting the geoviz toolkit. In Visual Analytics Science and Technology (VAST), 2011 IEEE Conference on, pages 315-316, Oct 2011.

[51] J. R. Goodall and M. Sowul. Viassist: Visual analytics for cyber defense. In Technologies for Homeland Security, 2009. HST'09. IEEE Conference on. IEEE, 2009.

[52] M. Gr_egoire and L. Beaudoin. Visualisation for network situational awareness in computer network defence. Visualisation and the Common Operational Picture, 2005.

[53] F. Hardisty and A. C. Robinson. The geoviz toolkit: using component-oriented coordination methods for geographic visualization and analysis. International Journal of Geographical Information Science, 25(2):191-210, 2011.

[54] Y. Hideshima and H. Koike. Starmine: A visualization system for cyber attacks. In Proceedings of the 2006 Asia-Paci_c Symposium on Information Visualisation - Volume 60, APVis '06, pages 131-138, Darlinghurst, Australia, Australia, 2006. Australian Computer Society, Inc.

[55] E. Karapistoli, P. Sarigiannidis, and A. A. Economides. Srnet: a real-time, cross-based anomaly detection and visualization system for wireless sensor networks. In Proceedings of the Tenth Workshop on Visualization for Cyber Security, pages 49-56. ACM, 2013.

[56] M. Nusinov, S. J. Yang, J. Holsopple, and M. Sudit. Visaw: Visualizing threat and impact assessment for enhanced situation awareness. In Military Communications Conference, 2009. MILCOM 2009. IEEE, pages 1-7. IEEE, 2009.

[57] M. Chu, K. Ingols, R. Lippmann, S. Webster, and S. Boyer. Visualizing attack graphs, reachability, and trust relationships with navigator. In VizSec 2010, 2010.

[58] U. Franke and J. Brynielsson. Cyber situational awareness–a systematic review of the literature. Computers & Security, 46:18–31, 2014.

[59] E. R. Gansner and S. C. North. An open graph visualization system and its applications to software engineering. SOFTWARE - PRACTICE AND EXPERIENCE, 30(11):1203–1233, 2000.

[60] J. Homer, A. Varikuti, X. Ou, and M. A. McQueen. Improving attack graph visualization through data reduction and attack grouping. In VizSec 2008, 2008.

[61] R. P. Lippmann. NetSPA : a network security planning architecture. Master Thesis, 2002.

[62] R. P. Lippmann and K. W. Ingols. An annotated review of past papers on attack graphs. Prepared for the Department of the Air Force under Contract F19628-00-C-0002, Mar. 2005.

[63] S. Mathew, R. Giomundo, S. Upadhyaya, M. Sudit, and A. Stotz. Understanding multistage attacks by attack-track based visualization of heterogeneous event streams. In VizSec 2006, 2006.

[64] S. Noel, M. Jacobs, P. Kalapa, and S. Jajodia. Multiple coordinated views for network attack graphs. In VizSec 2005, 2005.

[65] S. Noel and S. Jajodia. Managing attack graph complexity through visual hierarchical aggregation. In VizSec 2004, 2004.

[66] S. Noel, S. Jajodia, B. O'Berry, and M. Jacobs. Efficient minimum-cost network hardening via exploit dependency graphs. In Computer Security Applications Conference, 2003. Proceedings. 19th Annual, pages 86–95, Dec 2003.

[67] S. O'Hare, S. Noel, and K. Prole. A graph-theoretic visualization approach to network risk analysis. In VizSec 2008, 2008.

[68] V. Shandilya, C. B. Simmons, and S. Shiva. Use of attack graphs in security systems. Journal of Computer Networks and Communications, 2014, Oct. 2014.

[69] D. Staheli, T. Yu, R. J. Crouser, S. Damodaran, K. Nam, D. O'Gwynn, S. McKenna, and L. Harrison. Visualization evaluation for cyber security: Trends and future directions. In VizSec 2014, 2014.

[70] The PANOPTESEC Consortium. The Official Website of the PANOPTESEC Project, http://www.panoptesec.eu/, 2014.

[71] G. Vandenberghe. Network traffic exploration application: A tool to assess, visualize, and analyze network security events. In VizSec 2008,2008.

[72] L. Williams, R. Lippmann, and K. Ingols. An interactive attack graph cascade and reachability display. In VizSec 2007, 2007.

[73] M. Angelini and G. Santucci. Cyber Situational Awareness: from geographical alerts to high-level management. Journal of Visualization 2016. To appear.

[74] M. Angelini, G. Santucci and D. Wiemer. Geographical visualization for security risk and mission impact assessment. Specialists Meeting on "Visual Analytics (Cyber Security) " (IST-133) from Monday, October 12, 2015 to Wednesday, October 14, 2015 in Copenhagen, DENMARK

[75] M. Angelini and G. Santucci. A Reference Architecture for Visual Analytics in Cyber-Security domain. 5th International Conference on Software Engineering for Security & Defense Applications SEDA 2016. 2016.