FP7-610416-PANOPTESEC

Dynamic Risk Approaches for Automated Cyber Defence

D8.1.3 – Dissemination Report

Work-Package	WP8	Deliverable	D8.1.3
Due Date	M36	Submission Date	11/11/2016
Main Author(s)	RHEA, ACEA		
Contributors	All project participants		
Version	V1.1	Status	FINAL
Dissemination Level	PU	Nature	R
Keywords	Dissemination, publicity, website, social media, events, publications, external communications		

Part of the Seventh

Framework Programme

Funded by the EC - DG Connect

EXECUTIVE SUMMARY

This is the deliverable D8.1.3 - Dissemination Report of the FP7 project Dynamic Risk Approaches for Automated Cyber Defence (PANOPTESEC). This work was carried out as part of the WP8 Dissemination and Demonstration and specifically Task 8.1 Information Dissemination.

An important goal of the PANOPTESEC project is to ensure the sustainability of the project's outcomes through the Dissemination & Exploitation activities to be developed during the project and will continue after its completion. This deliverable documents the communication and dissemination activities of various nature that have taken place during the execution of the project, including scientific publications, participations to events and conferences, and organization of workshops.

This document is linked to Deliverable D8.2.3, Operational Workshop, which is the final and most comprehensive communication action of the project.

HISTORY

Version	Date	Name/Partner	Comment
V0.0	03-03-2016	Hervé Debar/IMT	Initial creation of the document and writing assignments
V0.1	26-10-2016	Francesco Bosco/ACEA	Added stats on linkedin, and twitter Added conferences, papers and press review for all the partner
V0.2	29/10/2016	Francesco Bosco/ACEA	Added section on operational workshop Minor adjustments
0.3	08/11/2016	Douglas Wiemer/RHEA	Added content and updates following QA review and partner contribution updates.
V1.0	11/11/2016	Douglas Wiemer/RHEA	Final updates following QA review by all partners.
V1.1	11/11/2016	Douglas Wiemer/RHEA	Inserting UROME Master's Thesis publications

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

ACRONYMS AND DEFINITIONS

Table 1: Acronym List

Acronym	Meaning
ACEA	ACEA S.p.A.
ALBLF	Alcatel-Lucent Bell Labs France
CIS-UROME	Università Degli Studi Di Roma La Sapienza
DoW	Description of Work
EPIST	Epistematica SRL
ICT	Information and Communication Technology
IMT	Institut Mines-Telecom
RHEA	RHEA System S.A.
SUPELEC	Ecole Supérieure D'Électricité
UoL	Universität zu Lübeck
SCADA	Supervisory Control And Data Acquisition
IRT	Institut de Recherche Technologique
IPR	Intellectual Property Rights

1 INTRODUCTION

1.1 Purpose

The purpose of this document is to provide information concerning the dissemination methods, results and opportunities of the EU-funded study into Dynamic Risk Approaches for Automated Cyber Defence (PANOPTESEC). It provides details concerning the dissemination and exploitation activities that have been undertaken during the project as well as an outlook on possible activities after its completion. Dissemination activities are listed in detail and are incorporated into an outline schedule. All activities related to Exploitation achievements and plans are described in a companion document D8.1.4 Exploitation Report.

1.2 Scope of the PANOPTESEC Dissemination Report

The main purpose of the PANOPTESEC Dissemination report is to provide an overview of the dissemination activities through the project supporting measurement of the dissemination results.

The PANOPTESEC dissemination and exploitation activities have been coordinated by RHEA, the consortium partner that is responsible for the Task 8.1 Information Dissemination. All participating members of the consortium provide support and participate in the dissemination and exploitation activities as required by the DoW. RHEA has been responsible for supporting the PANOPTESEC Steering Committee regarding the dissemination activities of the project and worked closely with the project partners ensuring timely and effective communication and interaction with targeted audiences, so that the project results can be optimally exploited.

The disseminations overall mission includes the following activities:

- To support high level dissemination of project results and achieved milestones;
- To keep the public updated via the project website, social media, events and publications; and
- To support the intellectual property rights activities of the partners and to ensure each partner claims are properly dealt with.

1.3 Document Structure

Following this introductory section, this document is divided into five sections covering aspects of the dissemination and exploitation activities and related schedule. The first section covers the dissemination plans including the main tools and channels used to communicate the major project results. This section is followed by the methodology that was followed to develop the dissemination and exploitation plans. The next section outlines the activities in a timeline grid according to the project development year. The document concludes with a summary of the results and recommendations.

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

Section 2 Methodology: describes the approach for the development of the dissemination and exploitation plan.

Section 3 General Strategy for Dissemination: describes the general approach followed in the development of dissemination activities.

Section 4 General Dissemination Activities Report: describes the general dissemination activities accomplishments.

Section 5 Scientific Dissemination and Project Presentation Activities Report: describes the scientific dissemination activities accomplishments in tabular form.

Section 6 Conclusion: summarises the findings and results.

2 METHODOLOGY

2.1 Development of Dissemination Strategy and Plan

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

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

The dissemination and exploitation strategy and plan has been based on the analysis of the stakeholders identified above and assessment of the needs of the cyber security community. The overall strategy and plan is presented in the PANOPTESEC deliverable D8.1.2.

The PANOPTESEC project set out to achieve the following general dissemination objectives:

1. PANOPTESEC public website: The website will provide all necessary and relevant information about the project and the consortium. As progress is made on each of the component modules, significant findings can be announced via the website for broad distribution;
2. EU project clustering activities: Coordinated by the SECCORD (SECurity and trust COoRDination and enhanced collaboration) project, PANOPTESEC will conduct coordination activities with SECCORD and participate in SECCORD clustering events;
3. Scientific publications and conferences: Scientific publications and conferences provide a recognized means to disseminate results. Each PANOPTESEC partner planned to contribute papers and participate in one industry-relevant conference per year;
4. Project workshops: The project set out to organise two workshops. The first workshop being near or at the end of the component experiments and refinement phase when individual component modules will be in a position to highlight the results of their project contributions in specific areas. The second workshop being at the conclusion of the project when the results of the integrated system could be demonstrated at ACEA.

2.2 Quality assurance

The quality assurance (QA) activities of the PANOPTESEC project rely on the assessment of a work product (i.e. deliverable) according to applicable QA checklists, validated at the consortium level and centralised in the Project Handbook and Quality Review Procedures.

The D8.1.3 deliverable has been assessed according the following checklists:

- PEER REVIEW (PR) QA CHECKLIST: the D8.1.3 deliverable is a report, it therefore required a proper peer review according to the checks defined in this checklist;

Detailed results of the review are captured in a report (called QRSR2.1.1). Checklists are available on the PANOPTESEC SVN.

3 GENERAL STRATEGY FOR DISSEMINATION

3.1 Dissemination objectives

The Dissemination and Exploitation Plan described in D8.1.2 identified the necessary and potential means for dissemination and exploitation of the project and set the objectives intended to be achieved by the project. The dissemination and exploitation plans were created in order to pursue the following objectives:

- The scientific and technical community as well as other potentially interested audiences would become aware of the PANOPTESEC project, its content, goal and results;
- PANOPTESEC would establish a leading role within the information security fora, workshops etc. and will build relationships with other FP7 related projects;
- PANOPTESEC concepts and approaches would be promoted to target markets relevant to future exploitation activities;
- The PANOPTESEC state-of-the-art technologies would be exploited after the completion of the project.

3.2 Target audiences

The target groups of PANOPTESEC dissemination activities included the following categories:

- Scientific and technical community;
- EU stakeholders;
- Target market stakeholders; and
- General audiences.

3.3 PANOPTESEC Identity

The PANOPTESEC project identity has been established through the use of a distinct logo and document templates.

3.3.1 PANOPTESEC logo

'Panoptes' is an ancient Greek term meaning "all eyes" or "all seeing", and has been incorporated into the project name, PANOPTESEC, to reflect the overall goals of the project.

In Greek mythology, Argos Panoptes was a hundred-eyed giant, who was requested by Hera, the wife of Zeus, to watch over the consort of her husband. After he was slain while performing his duty, Hera posthumously rewarded Panoptes by placing his hundred eyes on the tail of her sacred peacock.

The eyes on the peacock feather have been used in the PANOPTESEC logo, linking Greek mythology with the project concept.

The last three letters at the project name, SEC, link the name of the mythological figure Panoptes with the security domain of the project.

Figure 1: PANOPTESEC Logo

3.3.2 Templates for documentation and presentation

Templates for documentation and presentation have been designed and are available since Month 3 of the project. They have been revised, incorporated in the project handbook and verified through quality assurance after the 1st review.

3.4 Communication Tool and Channels

3.4.1 Project Website

The PANOPTESEC project website (http://panoptesec.eu/) was already been created during the first 3 months of the project timeline by using the latest technological requirements and following the best practice guidelines made available by the EU funding agency for FP7 projects. The project website complemented the activities of the PANOPTESEC project activities and has been used to promote the dissemination of the results and achievements to interested user communities as well as the general public.

There is also a special mobile-friendly version of the website to provide access to its contents using mobile devices (http://panoptesec.eu/mobile).

3.4.1.1 Website Images

The website has adopted a neutral background of a partly clouded blue sky. All website images (company and academia logos, EU and FP7 logos, technical diagrams, tables, etc.) are in standard image formats (jpg, gif, png), with transparent backgrounds where appropriate.

3.4.1.2 Web Domain

The web domain selected for the project website is www.panoptesec.eu, following best practice guidelines defined for EU project websites. The domain name has been registered for five years, covering the full three years of the project duration, plus an extra two years.

3.4.1.3 Technical Principles

The PANOPTESEC website adopts standard web technologies for the construction of the website. These include HTML, SHTML, Cascading Style Sheets (CSS) and JavaScript applets.

3.4.1.4 Design Principles

The project website is designed for easy maintenance, separating different content sections into different directories, and employing Server Side Include (SSI) files for repeatedly used content areas, such as headers and footers. A horizontal pull down menu is employed to facilitate navigation.

3.4.2 Social Media

3.4.2.1 LinkedIn Group

The PANOPTESEC LinkedIn Group (https://www.linkedin.com/groups/PANOPTESEC-Cyber-Security-Project-7461693/about) was created during the first months of the project. This group has been used to promote the PANOPTESEC news and also create an area for open discussion about related cyber security topics, further establishing the project's presence in this domain.

Figure 2: PANOPTESEC LinkedIn Group Banner

The PANOPTESEC LinkedIn Group The group is open to visitors who wish to read its content but it requires moderator acceptance for membership. Publication of posts and, in general any information, is supervised by the group moderators to ensure that there is no spam or stale information. Currently, there are 134 members in the group. This number has increased incrementally after various project events. Also, these events have also resulted in traffic coming back to the website.

The LinkedIn Group has been an effective tool to promote project dissemination activities.

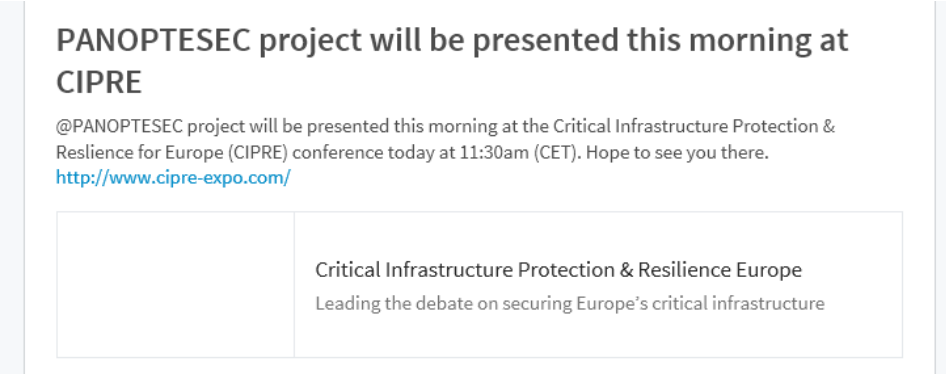

Figure 3: PANOPTESEC LinkedIn account use to promote project activities

Statistics of the LinkedIn Group activity for the duration of the project are provided in Figure 4 (updated at 26/10/2016):

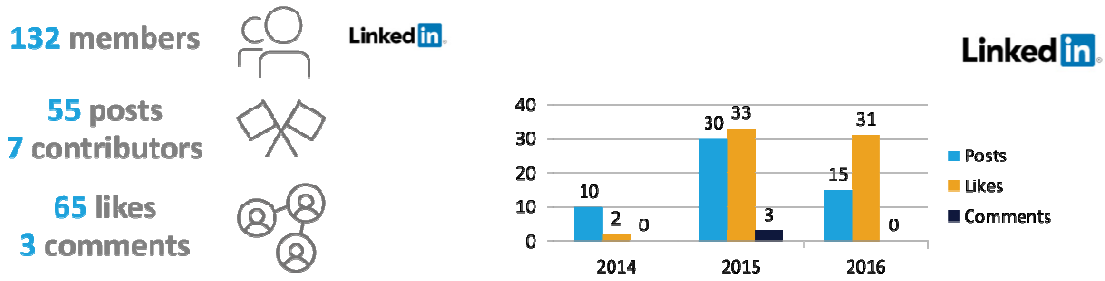

Figure 4: PANOPTESEC LinkedIn Group statistics

3.4.2.2 Twitter Account

In addition to the PANOPTESEC LinkedIn group, PANOPTESEC has established a dedicated Twitter account. This account is used to promote ongoing activities of the project and comment on news and events related to cyber security.

Figure 5: PANOPTESEC Twitter account

The Twitter account has been effective to further promote dissemination activities. For example participation in the Critical Infrastructure Protection for Europe (CIPRE) conference was promoted through the twitter account. In particular the Twitter account was effectively used during the Operational Workshops to promote and advertise the event.

Figure 6: Twitter account used to promote project operational workshops

Use of the Twitter account also takes advantage of extended social media links as followers of the group can 're-tweet' the PANOPTESEC announcements. This is supported by project partners who publish news in their social media accounts. As can be seen in the example below, the PANOPTESEC presentations dissemination events are re-tweeted by various partners and third-parties as illustrated in Figure 7.

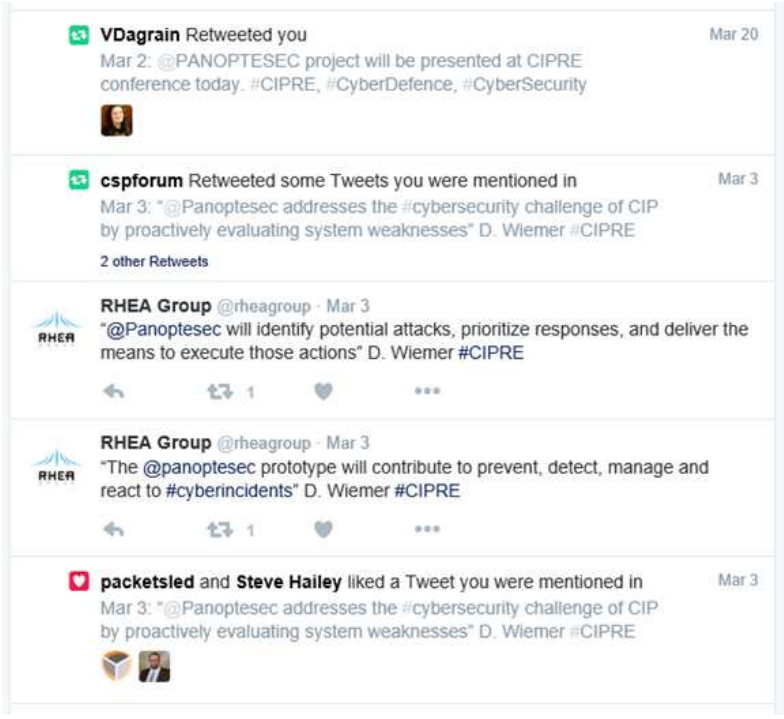

Figure 7: Twitter account activity is promoted by partners and other parties

Statistics of the Twitter Account activity and related re-Tweets on other accounts for the duration of the project are provided in Figure 8.

Figure 8: PANOPTESEC Twitter statistics

3.4.3 Conferences and presentations

Each PANOPTESEC partner planned to contribute papers and participate in at least one relevant conference per year. These contributions were coordinated between partners such that the collaborative nature of the PANOPTESEC consortium could be promoted to the industry and the cyber defence research community. In addition, the PANOPTESEC project sought to benefit from the visibility that publications focusing on cyber security and related technical developments could offer. In addition to the press releases published in the project's channels (website and LinkedIn group), the dissemination of the project's results have been realised via technical and general publications, newsletters, conference proceedings and associated websites. The results of these activities are listed in Section 5.

3.4.4 Press reviews

All the planned tools for the dissemination of the PANOPTESEC gave to the Project a good external visibility and a number of Press Releases regarding PANOPTESEC Project have been released:

- June 13 2016 : Acea Distribuzione Deploys Check Point SCADA Security Solution to Protect Critical Infrastructure against Cyber Threats, reporting PANOPTESEC experience (Market Wired Press Releases http://www.marketwired.com/press-release/acea-distribuzione-deploys-check-point-scada-security-solution-protect-critical-infrastructure-nasdaq-chkp-2133554.htm);
- June 13 2016 : Acea Distribuzione Deploys Check Point SCADA Security Solution to Protect Critical Infrastructure against Cyber Threats, reporting PANOPTESEC experience (Il corriere della sicurezza Press Releases http://www.ilcorrieredellasicurezza.it/articolo.asp?idarticolo=acea-distribuzione-al-sicuro-grazie-alle-soluzioni-scada-di-check-point_15689);

- June 13 2016 : Acea Distribuzione Deploys Check Point SCADA Security Solution to Protect Critical Infrastructure against Cyber Threats, reporting PANOPTESEC experience (Check Point Press Releases https://www.checkpoint.com/press/2016/acea-distribuzione-deploys-check-point-scada-security-solution-protect-critical-infrastructure-cyber-threats/http:/finance.yahoo.com/news/acea-distribuzione-deploys-check-point-120000630.html/);
- July 27 2016 : Cooperation on Cyber Defence to Enhance Cyber Situational Awareness, RHEA System newsletter (http://www.rheagroup.com/cooperation-cyber-defence-enhance-cyber-situational-awareness/);
- October 06 2016Infrastrutture e sicurezza: l'esempio ACEA di Alessia Valentini - Giovedì 6 Ottobre 2016 (http://blog.pmi.it/06/10/2016/infrastrutture-critiche-informatizzate-e-sicurezza-lesempio-di-acea/);
- October 26 2016 PANOPTESEC, protezione per infrastrutture critiche di Alessia Valentini - Mercoledì 26 Ottobre 2016(http://blog.pmi.it/26/10/2016/panoptesec-protezione-per-infrastrutture-critiche/);
- October 27 2016 Cyber defense, come funziona PANOPTESEC (http://www.askanews.it/altre-sezioni/technofun/cyber-defense-come-funziona-panoptesec_711928028.htm).

4 GENERAL DISSEMINATION ACTIVITIES REPORT

4.1 Project workshops

The project has participated to or organized the following workshops.

4.1.1 Mid-project operational workshop

An Operational Workshop was organized and conducted on September 8-9, 2015. The goal was to obtain additional end user feedback on the PANOPTESEC requirements, concepts and prototypes.

The workshop was conducted in collaboration with the H2020 PaaSword project. The project sent 205 targeted invitations as well as making use of the CSP Forum and The Hague Security Delta to further distributed the invitation via email and social media. The event was also promoted on LinkedIn, Twitter, Google+ and the participant newsletters before, during and after the event. Despite lower than anticipated attendance, the event provided a good opportunity to get necessary feedback from potential end-users outside the energy distribution sector. A formal survey was conducted and outcomes indicate generally good alignment with participant requirements.

Sept 8th (day 1) targeted cloud service providers and SMEs interested in cloud services, to evaluate the degree to which the PANOPTESEC solution could improve cloud service operations, particularly in support of diverse SME client needs. 10 people registered for Sept 8th. 5 guests attended Sept 8th. 2 surveys were received.

Sept 9th day 2) addressed a broad range of agency, large enterprise, banking/finance, transportation and other critical infrastructure providers (e.g., European Defence Agency or similar, large enterprise, banking and finance, etc). 13 people registered for Sept 9th. 5 guests attended Sept 9th. 3 surveys were received.

The three most important received technical comments were as follows:

1. The mission impact analysis, dynamic response management and visualization were identified as the most relevant advances in the state-of-the-art.
2. Several comments related to refinements of the visualization that were valuable to consider (e.g., placing configurable limits on some indicators to prevent operators being overwhelmed by information).
3. Additional threat awareness related information was noted as a feature that would be valuable to add in the future.

4.1.2 Mid-project workshop #1

The project hosted a 2-day project workshop on 8-9 September, 2015. The workshop was conducted in Brussels and hosted at the Diamant Business and Conference Centre. The workshop was conducted in collaboration with the H2020 PaaSWord project. The focus of the workshop was split each day, with Day 1 having focus on Cloud service providers and SMEs, while Day 2 was focused on agency level and large enterprise organizations. Each

project had the opportunity to present their overall project concepts and approach. The PANOPTESEC project then provided detailed demonstrations of project status.

4.1.3 Mid-project workshop #2

The project conducted a half-day security workshop as part of the InfoSecurity Europe Conference held in London, 7-9 June, 2016. This workshop also provided the opportunity for the project to host a project booth over the three days in the Innovation Zone, allowing increased opportunity for project members to interact with conference participants.

The half-day workshop was attended by 24 participants, nearly filling the room capacity of 25. The 24 participants represented a range of market sectors including Banking and Finance; Government; Information Technology; Retail; Telecommunications; Manufacturing; and Catering, Hotels and Leisure Entertainment. From among these communities, the survey feedback indicated that the PANOPTESEC project is both significantly relevant and innovative across many capability categories.

4.1.4 Final operational workshop

The operational workshop was held in ACEA premises from 17th to 28th October, 2016.The operational workshop was organized in 16 sessions in order to facilitate interaction with a range of external stakeholders.

The operational workshops have been considered a high point of the project, resulting in a total of 92 external and 13 internal stakeholders taking part in the Operational Workshops. The participants represented several industries including Public Utilities; Information Technology; Banking and Finance; Defence; Telecommunications, Television and Transportation and involving both from small to medium enterprise (SME) and large enterprise.

The full description and the results of feedback of the operational workshop are described in Deliverable D8.2.3.

4.1.5 External advisory board

The members of the External Advisory Board have been active participants in the review of project activities and outcomes. Their feedback has been influential in the shaping and direction of project outcomes. Most significant in terms of project dissemination has been their participation in validation of the project achievements as part of the MS7 Qualification Review in Month 35. Members of the External Advisory Board participated in a face-to-face meeting with the project to receive a working demonstration of the project outcomes. This meeting provided valuable feedback in preparation of the Operational Workshops planned for 17-28 October 2016.

4.2 Collaboration with Organisations and Synergies with other Projects

The project has maintained interactions with the following organizations and projects:

- EU FP7 project SecCord (http://www.seccord.eu) prepares for the EC an annual yearbook providing an overview of the major research and innovation achievements

of the FP7 Trust and Security Programme. PANOPTESEC has been included in the EU Yearbook 2014 - FP7 project SecCord. PANOTPESEC has also been included in the SecCord publication highlighting "Contributions of the FP7 Trust & Security projects towards the EU Cybersecurity Strategy" in 2015.

http://www.cspforum.eu/Annex_4_Contributions_to_EU_Cyberstrategy_copy.pdf

- The PaaSword project participated in the first mid-project operational workshop organized by PANOPTESEC in Brussels in September 2015.
- Following participation in the Critical Infrastructure Protection & Resilience for Europe (CIPRE) conference, June 2016, the project took steps to establish collaboration with the PRE-EMPTIVE project. The PRE-EMPTIVE Project places emphasis on sensor data collection in critical infrastructure environments. Due to the early stage status of the PRE-EMPTIVE project, collaborative opportunities have been limited, but will be pursued as part of project follow-up activities;
- ACEA promoted the PANOPTESEC project within the FP7 Security Project ECOSSIAN "European COntrol System Security Incident Analysis Network" (www.ecossian.eu) through the Consortium partner Poste Italiane SpA;
- ACEA promoted the PANOPTESEC project within the H2020 Project SUCCESS "securing critical energy infrastructures (www.success-energy.eu/) through the Consortium partner ASM Terni SpA;
- ACEA promoted the PANOPTESEC project within the FP7 C2-SENSE "Interoperability Profiles for Command/Control System and Sensor Systems in Emergency Management" (www.c2-sense.eu) through the Consortium partner Lutech SpA.

4.3 Official EU Dissemination Channels

The PANOPTESEC project is participating to clustering and community building activities supported by the European Union in the area of cybersecurity and/or trustworthy ICT.

The following dissemination activities are particularly noteworthy:

- May 20, 2014: Participation by D. Wiemer (RHEA) at CSP forum - Athens, Greece
- June 18-19, 2014: Participation by A. Guarino (ACEA) in "Security Summit 2014", organised by AIIC-Clusit
- July 3, 2014: Participation by A. Guarino (ACEA) in "First National Conference on Cyber Security for the Energy Sector-2014", organised by EnergyMedia – World Energy Council (WEC)
- October 15, 2014: Participation by A. Guarino (ACEA) in "CyberSec 2014 event", organized by Intel Security
- November 5, 2014: Conference participation by M. Merialdo, G. Mihalachi and K. Zidoune (RHEA) at the SECONOMICS Summit (Security Economics for Critical Infrastructure) – Brussels, Belgium

- March 2-3, 2016: The PANOPTESEC project was presented at the Critical Infrastructure Protection & Resilience for Europe (CIPRE) conference – The Hague, The Netherlands.

Public deliverables are made available to the Commission for publication on the Project web site and other communication channels.

5 SCIENTIFIC DISSEMINATION AND PROJECT PRESENTATIONS ACTIVITIES REPORT

5.1 Project publications

Table 2: List of scientific (peer reviewed) publications

No	Title	Main author(s)	Title of the periodical or series	Number, date or frequency	Place of publication	Year of publication	Relevant pages
1	Formalizing Agents' Beliefs for Cyber-Security Defense Strategy Planning	Karsten Martiny, Alexander Motzek, and Ralf Möller	CISIS 2015 : 8th International Conference on Computational Intelligence in Security for Information Systems		Burgos, Spain	2015	
2	Indirect Causes in Dynamic Bayesian Networks Revisited	Alexander Motzek, Ralf Möller	Proceedings of the 24th International Joint Conference on Artificial Intelligence		Buenos Aires, Argentina	2015	
3	Exploiting Innocuousness in Bayesian Networks	Alexander Motzek, Ralf Möller	Proceedings of the 28th Australasian Joint Conference on Artificial Intelligence, AI 2015		Canberra, Australia	2015	
4	Event Prioritization and Correlation based on Pattern Mining Techniques	Mona Lange, Ralf Möller, Gregor Lang, Felix Kuhr	Proceedings of the 14th International Conference on Machine Learning and Applications (ICMLA), ICMLA 2015		Miami, USA	2015	
5	Probabilistic Mission Impact Assessment based on Widespread Local Events	Alexander Motzek, Ralf Möller, Mona Lange, Samuel Dubus	NATO IST-128 Workshop on Cyber Attack Detection, Forensics and Attribution for Assessment of Mission Impact		Istanbul, Turkey	2015	
6	Mission Impact Assessment in Power Grids	Mona Lange and Marina Krotofil	NATO IST-128 Workshop on Cyber Attack Detection, Forensics and Attribution for Assessment of Mission Impact		Istanbul, Turkey	2015	
7	Considering technical and financial impact in the selection of security countermeasures against Advanced Persistent Threats (APTs)	Gonzalez-Granadillo, Gustavo and Garcia-Alfaro, Joaquin and Debar, Herve and Ponchel, Christophe and Martin, Laura Rodriguez	2015 7th International Conference on New Technologies, Mobility and Security (NTMS)		Paris, France	2015	
8	Selecting optimal countermeasures for attacks against critical systems using the attack volume model and the RORI index	Gonzalez-Granadillo, G and Garcia-Alfaro, J and Alvarez, E and El-Barbori, M and Debar, H	Computers and Electrical Engineering	47	Pergamon	2015	13-34
9	Using a 3D geometrical model to improve accuracy in the evaluation and selection of countermeasures against complex cyber attacks	Gonzalez-Granadillo, Gustavo and Garcia-Alfaro, Joaquin and Debar, Herve	11th EAI International Conference on Security and Privacy in Communication Networks (SecureComm),		Dallas, Texas, USA	2015	

No	Title	Main author(s)	Title of the periodical or series	Number, date or frequency	Place of publication	Year of publication	Relevant pages
10	Elementary Risks: Bridging Operational and Strategic Security Realms	Waël Kanoun, Serge Papillon, Samuel Dubus	Proceedings of the 11th International Conference on Signal Image Technology & Internet Based Systems (SITIS 2015),		Bangkok, Thailand	2015	
11	Visual Cyber Situational Awareness for Critical Infrastructures	Angelini M., Santucci G.	Proceedings of the 8th International Symposium on Visual Information Communication and Interaction		Tokyo, Japan	2015	
12	PERCIVAL: proactive and reactive attack and response assessment for cyber incidents using visual analytics	Angelini M., Prigent N. and Santucci G	Proceedings of the 12th IEEE Symposium on Visualization for Cyber Security		Chicago, Illinois, USA	2015	
13	Towards an Automated and Dynamic Risk Management Response System	Gustavo Gonzalez Granadillo, Ender Alvarez, Alexander Motzek, Matteo Merialdo, Joaquin Garcia-Alfaro, Hervé Debar	NordSec 2016: 21st Nordic Conference on Secure IT Systems		Oulu, Finland	2016	
14	An n-sided polygonal model to calculate the impact of cyber security events	G. Gonzalez Granadillo, J. Garcia Alfaro, and H. Debar	11th International Conference on Risks and Security of Internet and Systems		France	2016	
15	Selection of Mitigation Actions Based on Financial and Operational Impact Assessments	G. Gonzalez-Granadillo, A. Motzek, J. Garcia-Alfaro, H. Debar	International Conference on Availability, Reliability and Security		Austria	2016	
16	Considering internal vulnerabilities and the attacker's knowledge to model the impact of cyber events as geometrical prisms	G. Gonzalez-Granadillo, J. Rubio Hernan, J. Garcia Alfaro, and H. Debar	The 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications		China	2016	
17	Using a Deep Understanding of Network Activities for Security Event Management	Mona Lange, Felix Kuhr, Ralf Moeller	International Journal of Network Security & Its Applications			2016	
18	Probabilistic Mission Defense and Assurance	Alexander Motzek, Ralf Möller	NATO IST-148 Symposium on Cyber Defence Situation Awareness		Sofia, Bulgaria	2016	
19	Selection of Mitigation Actions Based on Financial and Operational Impact Assessments	Gustavo Gonzalez Granadillo, Alexander Motzek, Joaquin Garcia-Alfaro, Hervé Debar	ARES 2016: 11th International Conference on Availability, Reliability and Security		Salzburg, Austria	2016	
20	Semantic Normalization and Merging of Business Dependency Models	Alexander Motzek, Christina Geick, Ralf Möller	CBI 2016: 18th IEEE Conference on Business Informatics		Paris, France	2016	
21	Time Series Data Mining for Network Service Dependency Analysis	Lange, M. & Moeller, R.	9th International Conference on Computational Intelligence in Security for Information Systems		San Sebastien, Spain	2016	

No	Title	Main author(s)	Title of the periodical or series	Number, date or frequency	Place of publication	Year of publication	Relevant pages
22	Using a Deep Understanding of Network Activities for Workflow Mining	Lange, M. & Kuhr F. & Moeller, R.	39th Annual German Conference on Artificial Intelligence (ISBN: 978-3-319-46072-7)		Berlin Heidelberg, Klagenfurth, Austria	2016	177-184
23	Using a Deep Understanding of Network Activities for Network Vulnerability Assessment	Mona Lange, Felix Kuhr, Ralf Möller	Proceedings of the 1st International Workshop on AI for Privacy and Security, PrAISe@ECAI 2016		The Hague, Netherlands	2016	
24	An On-line Multi-step Attack Detector for Complex Distributed Systems (under review)	Marco Angelini, Silvia Bonomi, Emanuele Borzi, Antonella Del Pozzo, Simone Lenti, Giuseppe Santucci	First Itallian Conference on Cyber Security		Italy	2017	
25	A Dynamic Risk Management Response System to handle threats in critical infrastructures (under review)	G. Gonzalez Granadillo, S. Dubus, A. Motzek, E. Alvarez, M. Merialdo, S. Papillon, J. Garcia-Alfaro, and H. Debar	Journal of Future Generation Computer Systems, Special Issue on Measurements and Security of Complex Networks and Systems				
26	A polytope-based approach to measure the impact of events against critical infrastructures	G. Gonzalez Granadillo, J. Garcia Alfaro, and H. Debar	Journal of Computer and System Sciences, Special Issue on “Cyber Security in the Critical Infrastructure: Advances and Future Directions, DOI:10.1016/j.jcss.2016.02.004			2016	
27	Assessing Mission Impact of Cyber Attacks: Towards a Model-Driven Paradigm	Alexander Kott, Mona Lange, Jackson Ludwig	IEEE Security Privacy, 2016			2016	
28	On-line Multi-step Attack Detection in the PANOPTESEC System: Metric definition and evaluation	Andrea Battistelli	Master’s Thesis		University of Rome “La Sapienza”, Italy	2016	
29	Managing Attack Graph Evolution in the PANOPTESEC System	Riccardo Ghera	Master’s Thesis		University of Rome “La Sapienza”, Italy	2016	
30	Potential Attack Path Identification in the PANOPTESEC System	Ivano Giancaterina	Master’s Thesis		University of Rome “La Sapienza”, Italy	2016	

5.2 Project presentations and dissemination activities

Table 3: List of presentations and other dissemination activities

No	Type of activities	Main leader	Title	Date/Period	Place	Type of audience	Size of audience	Countries addressed
1	Presentation	G. Santucci (University of Rome)	Incremental and Interactive Visualizations	2014/01/07	University of Rostock	Community		DE
2	Presentation	A. Guarino (ACEA)	The fault of defaults - don't let anyone else make your security choices	2014/01/24	IFIP WG 10.4 - 65th Meeting - Sorrento, Italy	Community, industry		
3	Presentation	J. Garcia-Alfaro (IMT)	Current EU Trends in Cyber Attack Protection	2014/01/24	CIISE Distinguished Seminar, Concordia Institute for Information Systems Engineering, CA	Community		CA
4	Presentation	G. Santucci (University of Rome)	PANOPTESEC	2014/02/19	University of La Havana	Community		
5	Press release	P. Reizi (RHEA)	First milestones for the new Cyber Security Project – PANOPTESEC	2014/04/25		Media		
6	Article	P. Reizi (RHEA)	The first milestones of PANOPTESEC	2014/04	The CSP newsletter	Media		
7	Presentation	G. Santucci (University of Rome)	Number Vizualization	2014/055/15	University of Padua	Community		
8	Presentation	J. Garcia-Alfaro (IMT)	SCADA Cyber-Physical Threats Research" via Software Co-Simulation	2014/06/04-05	Advanced Intrusion Detection and Prevention Workshop (AIDP'14), Co-located with IFIP SEC 2014	Community		EU
9	Presentation	W. Kanoun, S. Papillon, S. Dubus (ALBLF)	Analysis Support to Decision Making in Cyber Defence and Security	2014/06/10	SAS-106 Symposium, Tallinn, Estonia	Community		EU
10	Press release	P. Reizi (RHEA)	Early progress for PANOPTESEC after the Plenary Design Meeting	2014/07/17		Media		EU
11	Article	P. Reizi (RHEA)	SecCord Research and Innovation EU Yearbook 2014	2014/07/31		Media		EU
12	Article	P. Reizi (RHEA)	Early progress of PANOPTESEC	2014/08	The CSP newsletter	Media		

No	Type of activities	Main leader	Title	Date/Period	Place	Type of audience	Size of audience	Countries addressed
13	Presentation	EPIST	PANOPTESEC concept	2014/10	Road-mapping Cybersecurity Research and Innovation Seminar and the ICT EU Day	Community		EU
14	Presentation and	H.Debar (IMT)	PANOPTESEC	2014/11/11	Dagstuhl Seminar 14292 "Network Attack Detection and Defense: Securing Industrial Control Systems for Critical Infrastructures"	Community		EU
15	Presentation	EPIST	PANOPTESEC concept		Security Focus Group, Faculty of Science, University of Reading (UK)	Community		EU
16	Presentation	EPIST	PANOPTESEC concept		the Fund Raising Team at Brunel Business School (London, UK)	Community		EU
17	Presentation	J. Garcia-Alfaro (IMT)	On the Adaptation of Physical-layer Failure Detection Mechanisms to Handle Attacks against SCADA Systems	2014/12	Symposium on Digital Trust	Community		FR
18	Presentation (invited)	M. Lange (UoL) and M. Krotofil	Mission Impact Modelling for Industrial Control Systems	2014	1st SCADA Security Conference LATAM, Sao Paulo, Brazil	Community		
19	Press release	P. Reizi (RHEA)	First year project results presented to the External Advisory Board	2015/02/20		Media		EU
20	Article	P. Reizi (RHEA)	First year project results of PANOPTESEC	2015/03	The CSP newsletter	Media		
21	Poster presentation	D. Wiemer and M. Merialdo (RHEA)	PANOPTESEC	2015/04/28-29	Cyber Security & Privacy Innovation Forum, Brussels	Community		EU
22	Demonstration	D. Wiemer (RHEA)	PANOPTESEC concepts and prototype demonstration	2015/05/16	Representatives of the City of Montreal 'Smart Cities' initiative	Policy makers		CA
23	Lecture	UROME/RHEA	seminary on Software Architecture at UROME,	2015/05/20-21	course "Progetto di Applicazioni Software (UROME)	Community		IT

No	Type of activities	Main leader	Title	Date/Period	Place	Type of audience	Size of audience	Countries addressed
24	Lecture	A. Del Pozzo (University of Rome) and M. Merialdo (RHEA)	PANOPTESEC architecture	2015/05/22	Distributed System Seminars Course of the University of Rome	Community		IT
25	Demonstration	D. Wiemer (RHEA)	PANOPTESEC concepts and prototype demonstration	2015/06/01	5th meeting of the NATO IST-108 Cyber Defence Situational Awareness Research Task Group (RTG)	Community, Policy makers		EU
26	Demonstration	D. Wiemer (RHEA)	PANOPTESEC concepts and prototype demonstration	2015/06/26	European Defence Agency (EDA) Cyber Project Team	Community, Policy makers		
27	Workshop	PANOPTESEC	PANOPTESEC	2015/09/8-9	Brussels, Diamant Centre	Community		EU
28	Invited talk	P.Colamarino (RHEA)	"Threat Analysis", the pitfalls that affect many Risk Analysis - A practical experience	2015/09/22	2nd International Workshop on Reliability and Security Aspects for Critical Infrastructure Protection (Delft)	Community		EU
29	Article and Demonstration	D. Wiemer (RHEA), G. Santucci (CIS-UROME), M. Angellini (CIS-UROME)	Geographical visualization for security risk and mission impact assessment	2015/10/12	NATO IST-133 "Visual Analytics – Cyber Security" Specialists Meeting, Copenhagen, Denmark	Community, Policy makers	~35	All NATO nations.
30	Presentation	A.Guarino (ACEA)	PANOPTESEC	2016/02	Cyber Security Energia 2015, Rome	Community	~50	IT
31	Presentation	F.Bosco (ACEA)	Potential Impact of cyber security on water sector	2016/02/11	EUREAU EU3 meeting, Berlin	Community	~15	EU
32	Presentation	D. Wiemer (RHEA)	PANOPTESEC	2016/03/03	CIPRE 2016, The Hague, The Netherlands	Community	~200	Europe
33	Presentation	R. Moeller (UzL)	PANOPTESEC System technical demonstration	2016/04/11	CYPP	Community		DE
34	Presentation	R. Moeller (UzL)	PANOPTESEC System technical demonstration	2016/04/11	DFN-CERT	Community		DE
35	Presentation and press conference	A.Guarino (ACEA)	PANOPTESEC Presentation	2016/04/19-20	Check Point Experience 2016, Nice	Community & press		EU

No	Type of activities	Main leader	Title	Date/Period	Place	Type of audience	Size of audience	Countries addressed
36	Demonstration	M.Merialdo(RHEA)	Demonstration of the PANOPTESEC System to General Electric – GE Industrial Communication representatives	2016/05/26	Acea, PANOPTESEC Room	Community	2	IT/SP/EU
37	Presentation	A.Guarino (ACEA)	"Improvement security incident response with the PANOPTESEC System	2016/05/27	European Mobility & Endpoint Security User Group Meeting,	Community		
38	Workshop	RHEA	PANOPTESEC	2016/06/7-9	Infosec Europe conference	Community	25	EU
39	Booth	RHEA	PANOPTESEC	2016/06/7-9	Infosec Europe conference	Community	~200	EU
40	Presentation	A.Guarino (ACEA)	PANOPTESEC project presentation	2016/07/	Outthink threats IBM, Roma	Community		IT
41	Presentation	D. Wiemer (RHEA)	PANOPTESEC	2016/07/20-21	Slovak EU Presidency Conference, Cooperation on Cyber Defence, Bratislava	Community, Policy makers		EU
42	Booth and demonstrations	M.Merialdo (RHEA) M. Angelini (CIS-UROME)	PANOPTESEC	2016/09/29	CyberTech Europe, Rome	Community		IT
43	Invited talk	J. Garcia-Alfaro (IMT)	Security of Cyber-Physical Systems - From Theory to Testbeds and Validation	2016/09/26-30	2nd Workshop on the Security of Industrial Control Systems & Cyber-Physical Systems CyberICPS 2016, Greece	Community		GR,EU

5.3 Dissemination Activities after the Project End

The project's work and results will continue to be part of the dissemination activities by all partners whenever the context allows it. It is possible that publications will continue to include results related to the PANOPTESEC project. Also, the project website will remain online for at least two additional years and the project partners can individually update further project results. Last, the project's social media channel will also stay online and open for posting further relevant discussions on Cyber Security and PANOPTESEC.

6 CONCLUSIONS

The PANOPTESEC project partners have taken significant steps towards dissemination of project results. In comparison to project objectives, the project has exceeded expectations:

1. Use of online public dissemination channels: In addition to the planned PANOPTESEC public website, the project leveraged additional public dissemination channels such as social media (including Twitter, LinkedIn) and the Press;
2. Participation in clustering activities: The project participated in publications of the SECCORD as well as participating in CSP Forum events. The project collaborated with the H2020 PaaSWord project and has initiated discussions with the PRE-EMPTIVE project. The project was also represented at the SECONOMICS Summit and CIPRE conference, among others.
3. Scientific publications and conferences: The project has contributed 30 publications to the scientific community and made presentation or otherwise participated in 43 other dissemination events and conferences;
4. Project workshops: The project hosted three workshops including a preliminary 2-day workshop in period 2, followed by a half-day workshop at a significant industrial event (INFOSEC EU) and finally hosting a series of half-day workshops including operational system demonstrations, spanning a 2-week period. The final workshop was attended by 92 external and 13 internal stakeholders. The workshops provided an opportunity to present the project results to multiple industries and sectors including Telecommunications, Information Technology, Banking and Finance, Government, Transportation, Space, Small-Medium Enterprise and large industry.

Throughout the project, feedback from all dissemination channels has been extremely positive, identifying the project as highly relevant and innovative. The project has been praised for its significant achievements by the cyber security community.