MITIGATE

EUROPEAN COMMISSION

MITIGATE

Multidimensional, IntegraTed, rIsk assessment framework and dynamic, collaborative risk manaGement tools for critical information infrAstrucTrurEs

www.mitigateproject.eu

Grant Agreement No.653212
Topic: H2020-DS-2014-01
Risk Management and Assurance Models
Innovation Action

Deliverable D6.2

External Pilot Operations

Contractual Date of Delivery:	M29 / January 2018
Editor:	Thanos Karantjias, Spryos Papastergiou (UPRC)
Work-package:	6
Distribution / Type:	PU (Public)
Version:	1.0
File:	Storage location / File-direction

Project co-funded by the European Union within the Horizon 2020 Programme

Abstract

The main MITIGATE scope is to provide an innovative Maritime Security System, which integrates an effective, collaborative, standards-based (i.e. ISO27001, ISO28000) Risk Management services' platform for Maritime Organizations and Critical Infrastructures (i.e. ports). Specifically, it enables Maritime Organizations to manage their security in a holistic, integrated and cost-effective manner, while at the same time producing and sharing knowledge associated with the identification, assessment and quantification of cascading effects from their Supply Chain (SC). Since, the first stable version of the MITIGATE system is already up and running, it has been presented to all involved Business Partners and the training material of all types (online help, videos, etc.) is already prepared, the consortium prepared all pilot sites to first involve their internal users.

The main objective of deliverable D6.2 is to present the results of the MITIGATE pilot's operations with external pilot users, and their organization, considering the pilot scenarios specified in WP2 and WP5 and the training processes performed in WP5.

Executive Summary

The main objective of deliverable D6.2 is to present the results of the MITIGATE pilot's operations with external pilot users, and their organization, considering the pilot scenarios specified in WP2 and WP5 and the training processes performed in WP5.

In order to achieve the goals of D6.2, the deliverable is structured as follows:

- Section 2 presents the overall operation plan of the MITIGATE project
- Sections 3 - 6 introduces the pilots' organization in each specific pilot, providing also the evaluation results that came out from each site by covering two different perspectives:
    - on one side, Supply Chain Services Business Partners' specific features and actions, and
    - on the other hand, the problems and barriers that each partner had to dealed with in order to successfully perform the organized pilot events and the overall plan.
- Finally, section 7 provides the overall conclusions of the Internal pilot activities within the MITIGATE project

Version History

Version	Date	Comments, Changes, Status	Authors, contributors, reviewers
0.1	5/06/2017	First Draft ToC	Thanos Karantjias, Spyros Papastergiou
0.2	20/12/2017	Revised ToC	Thanos Karantjias, Spyros Papastergiou
0.3	17/1/2018	Contibution from UPRC & PPA	Thanos Karantjias, Spyros Papastergiou, Stamatios Glykos, Vassilis Vasilakopoulos, Christos Douligeris, Menia Chatzikou, Ioannis Stavrakis, Petros Salichos, Yiannis Papagiannopoulos
0.4	3/2/2018	Contribution from VPort	Pablo Giménez Salazar, Rafa Company Peris
0.5	13/2/2018	Contribution from Fraunhofer	Claudia Bosse
0.6	24/2/2018	Contribution from Ravenna	Andrea Minardi, Alberto Squarzina, Armend Duzha
0.7	26/2/2018	Final input and Revised version from UPRC	Thanos Karantjias, Spyros Papastergiou
1.0	28/2/2018	Final version of the Deliverable	Thanos Karantjias, Spyros Papastergiou

Contributors

First Name	Last Name	Partner	Email
Thanos	Karantjias	UPRC	thanos.karantjias@gmail.com
Spyros	Papastergiou	UPRC	spyrospapastergiou@gmail.com
Andrea	Minardi	PRA	andrea.minardi@port.ravenna.it
Alberto	Squarzina	PRA	alberto.squarzina@port.ravenna.it
Armend	Duzha	MAGG	armend.duzha@maggioli.it
Pablo Giménez	Salazar	VPort	pgimenez@fundacion.valenciaport.com
Rafael	Company	VPort	rcompany@fundacion.valenciaport.com
Claudia	Bosse	Fraunhofer	claudia.bosse@cml.fraunhofer.de
Gunther	Klein	Fraunhofer	gunter.klein@dbh.de
Ralf	Fiedler	Fraunhofer	ralf.fiedler@cml.fraunhofer.de
Yannis	Papagianopoulos	PPA	ypapagiannopoulos@olp.gr
Stamatios	Glykos	UPRC	stamatisglykos@gmail.com
Vassilis	Vasilakopoulos	UPRC	filabros@hotmail.com
Christos	Douligeris	UPRC	cdoulig@unipi.gr
Menia	Chatzikou	UPRC	mhatzikou@gmail.com
Ioannis	Stavrakakis	UPRC	ioannis@di.uoa.gr
Petros	Salichos	UPRC	petros.salichos.0@gmail.com

Glossary

Acronym	Explanation
CII	Critical Information Infrastructure
RA	Risk Assessment
RM	Risk Management
SC	Supply Chain

Table of Contents

List of Figures

List of Tables

1 Introduction

This section introduces the headlines of the MITIGATE project pilot operation plans with external pilot users, considering the pilot scenarios specified in WP2 and WP5 and the training processes performed in WP5.

The main MITIGATE scope is to provide an innovative Maritime Security System, which integrates an effective, collaborative, standards-based (i.e. ISO27001, ISO28000) Risk Management services' platform for Maritime Organizations and Critical Infrastructures (i.e. ports). Specifically, it enables Maritime Organizations to manage their security in a holistic, integrated and cost-effective manner, while at the same time producing and sharing knowledge associated with the identification, assessment and quantification of cascading effects from their Supply Chain (SC).

Targeting towards this direction, Maritime Organizations are able to predict potential security risks, but also to mitigate and minimize the consequences of divergent security threats and their cascading effects in the most cost-effective way i.e. based on information associated with simulation scenarios and data acquired from online sources and repositories (i.e. NIST Repositories, CVE Details, etc.).

This innovative system empowers:

(i) A range of reasoning, data mining, crowd-sourcing and Big-Data analytics techniques that incorporate and leverage a variety of data sources and data types, enabling efficient handling of data that are incomplete, uncertain, and probabilistic;

(ii) Pioneering mathematical techniques for predicting and analyzing threats patterns; and innovative visualization and simulation techniques, which optimize the automatic analysis of diverse data.

Since, the first stable version of the MITIGATE system is already up and running, it has been presented to all involved Business Partners and the training material of all types (online help, videos, etc.) is already prepared, the consortium prepared all pilot sites to first involve their internal users. Based on the feedback from these internal pilot users, the consortium prepared and executed the pilots sites for external users.

The main objective of deliverable D6.2 is to present the results of the MITIGATE pilot's operations with external pilot users. In order to achieve the goals of D6.2, the deliverable is structured as follows:

- Section 2 presents the overall operation plan of the MITIGATE project
- Sections 3 - 6 introduces the pilots' organization in each specific pilot, providing also the evaluation results that came out from each site by covering two different perspectives:
  - on one side, Supply Chain Services Business Partners' specific features and results, and
  - on the other hand, the problems and barriers that each partner had to dealed with in order to successfully perform the organized pilot events and the overall plan.
- Finally, section 7 draws conclusions

Therefore, in the following sections, partners report the main finding about:

- External Pilot operation (brief description, context, etc.)
- Main pilot operations' results (number of events, number of users participated, number of completed evaluation reports collected – port operators)
- The selected pilot scenarios and how these were realized in the MITIGATE system

- During the pilot operations several problems were faced, but every partner had carried out actions and remedies to overcome problems
- Information and knowledge sharing
- Visibility and dissemination actions taken from each project partner in order to attract as many as possible potential users of the MITIGATE system

2 Pilot Operations Plan

2.1 Overall Plan

Following the methodology adopted for the internal pilot operations, this section introduces the full plan for all participated Pilot Sites with external users.

In particular, MITIGATE pilot operations officially cover the period from the (01/09/2017 - 28/2/2018).

The table below summarizes the main tasks of the internal pilots and their scheduling:

Task	Description	Start date	End date
Pilots stabilization	The first stable version of the MTITIGATE System, the required training material and corresponding documentation, as well as the initial configuration of the services were released and the Pilot sites for both internal and external users have been already established.	01/09/2016	28/02/2018
Training of Partners and External Users	Presentations were prepared to train the partners and external users in using properly the MITIGATE System and its services based on their role.	01/09/2016	(ongoing)
Pilot Operation with External Users	During this period, all pilots with internal users were organized and performed successfully, enabling Project Partners to become familiar with the MITIGATE platform and optimize the presentation and training process required for performing the corresponding pilots with external users	01/07/2017	(ongoing)
Evaluation & Validation	During this period, all invited users (external and internal) evaluated the MITIGATE System and the accompanying from a technical, technological, usability and business perspective. The evaluation process was made based on pre-defined online questionnaires.	01/02/2017	(ongoing)
Evaluation results	This period covered the analysis of the evaluation responses to produce a qualitative conclusions report for the usability, business	01/02/2017	(ongoing)

	impact and technical aspects of the MITIGATE System.		
Fine Tuning	The MITIGATE system has undergone a thorough upgrade during this period aiming at solving any problems came out during the external users pilots, and at enhancing the system with additional functionality.	01/02/2017	(ongoing)

Table 1: Overall Pilot Operation Planning

The following Sections provide more detailed information on the each pilot operation for external users.

3 Greek Pilot Operations

3.1 Introduction

As in the case of the Pilots for internal users, pilot operations for external users in Greece were organized and coordinated mainly by Piraeus Port Authority (PPA) and University of Piraeus Research Center (UPRC) with the active involvement and technical support of SingularLogic (SILO).

The valuable participation of the PPA, which is the Greek Port Community System (PCS), under the supervision of Cosco shareholder, has enhanced the evaluation process engaging a significant number of external users to try and test the MITIGATE functionality. Specifically, PPA organized one (1) bog International Conference on "***Security and Safety at the EU Ports / PPA EU Projects***" with the following topics:

- Security Policies in European Ports
- The Port Security Management Policies
- Presentation of the Port of Piraeus EU Projects

At this big event 143 people participated and were introduced of the MITIGATE project and the specifically of the MITIGATE system.

On the other hand, UPRC and SILO organized several training seminars, pilot events in the context of the CIP workshop, other workshops, face to face interviews, and pilot events in several Conferences, approaching:

- Senior and graduate students from the Department of Informatics, Erasmus students in the University
- PhD Candidates in Informatics and Business Engineering
- Military Authorities and other Governmental / International Agencies and organizations
- Representatives from the Maritime Industry
- Strategic think Tanks
- Board Members, Security Officers, Security Consultants, and IT Employers of big Private Companies and Public bodies
- and Individuals who is interested to try the system and services and to be trained on the MITIGATE Risk Assessment Methodology and Tool.

Targeting towards this direction, the following paragraphs describe all important issues that came out from the MITIGATE pilot operations plan performed in Greece. These include the identification of potential problems that need to be early solved in order to conclude with a successful implementation of pilot operations and the achievement of the expected results.

3.2 Pilot Plan with External Users

As mentioned before, PPA organized one big International Conference with different groups of users on "***Security and Safety at the EU Ports / PPA EU Projects***" with the following topics:

- Security Policies in European Ports
- The Port Security Management Policies
- Presentation of the Port of Piraeus EU Projects

Representatives many different companies and industries were participated. In total, 143 users were participated in this pilot event, while 20 of them are already registered in the MITIGATE system.

On the other hand, UPRC and SILO organized several training seminars, pilot events in NEMO Summer School, pilot evetns in the context of the CIP workshop, other workshops, face to face interviews, and pilot events in several Conferences. To this end, 229 participants were introduced to the MITIGATE system and many of them were trained on its services.

The following table summarizes the total number of events carried out in Greece and the number of completed evaluation reports and the registered and trained external pilot users.

Events		**Completed evaluation reports**		**Registered users**		**Trained users**	
# of events	*# participants*	*#port operators*	*#stakeholders / individuals*	*#port operators*	*#stakeholders / individuals*	*#port operators*	*#stakeholders / individuals*
39	372	22	43	30	141	19	107

Table 2: Pilot Results in Greece

3.3 Pilot Scenario(s)

Since, the involvement of the end-users in the pilot operations are mainly based on the pilot scenarios specified in WP2 and WP5, this section will briefly describe the final pilot scenario(s) selected for the specific pilot, highlighting any refinement required.

3.4 Problems & Barriers

In the scope of the internal MITIGATE pilot operations that have been organized by PPA and UPRC with the continuously support of SILO, the main issues that were identified as obstacle to pilot operations plan, as reported on D6.1, were the following:

- After an exgasted training and utilization section on the MITIGATE system and services, users provided unwillingness in performing the customization and proper re-production of evaluation reports, which were available via on-line questionnaires.
- MITIGATE services require in depth analysis of all cyber assets for examining and pilot a selected scenario. In order to successfully use these services, end-users must be very well trained and prepared. Obviously, the training curve required is considerable and require a significant amount of time. Therefore, there is a proven difficulty when trying to perform all these actions (training on and pilot operation of the MITIGATE system) in one given organized event.
- The nature of the MITIGATE system and Services requires all involved entities in Supply Chain Service to complete their tasks within the MITIGATE environment. Since its is difficult to organize and perform all these tasks simultaneously in a specific pilot event, it is quite impossible for a user to gain the full view of the MITIGATE system's value in one event session. Therefore, either you need a sequence of sessions with the same users or you need to have

prior to a pilot event already prepared some given scenarios and then try to complete them during the specific event.

The consortium take into account the aforementioned as well as other reported problems and barriers from all internal pilot operations and took the proper actions:

- All bugs were appropriately fixed and solved
- Fine-tuning pm the whole system was performed and as a result
  - the user interface became more friendly, while
  - many features were added in order to help the final user to better undertstand and use the MITIGATE services
- Many different ready templates were created in order for a participant to be able to in a short time period to build upon them. Specifically, in order to facilitate the involvement of external SCS business partners and individuals in the evaluation process, a Demo MITIGATE Port Authority Port Site, as well as other Sites were created. These Sites was created giving the opportunity to external users to evaluate the supported services creating and conducting real and "dummy" assessments. In our case the following sites were created:
  - DemoMitigate
  - DemoCustoms
  - MitigatePortAuthority
  - MitigateCustoms
  - Mitigate Ship Agent
  - Mitigate Carrier Agent
  - Mitigate Local Agent

To this end, in the scope of the external MITIGATE pilot operations that have been organized from all Greek Partners, not many broblems / barriers / issues appeard during their process. Those that came up have as follows:

- Many users were suspicious in using their real assets and infrastructures in the scenarios since they had to be sure that privacy issues and confidentiality is confirmed. The concept of participating in a Supply Chain Risk Assessment is very new, and what it's results mean in the real world for their current synergies and signed contracts looks frightening.
- On one hand they realized the real value of the MITIGATE system but on the other they stated that the results generated from a Supply Chain Risk Assessment need to be reviewed from a Security Consultant, who will immediately create a Risk Treatment plan for their organization. Only at this case the MITIGATE system has real value for them.

3.5 Visibility & Dissemination Actions

PPA, UPRC and SILO followed targeted efforts to contact and motivate a large number of end-users to participate in pilot operations in Greece, including the following:

- Sending personal and public invitations (both by post and e-mail);
- Publishing pilot operations program to national and local media and the web;
- Promoting workshop events to maritime communities and companies;

- inviting maritime stakeholders based on contact information that has been collected so far by networking in conferences and workshop events that both SILO and UPRC partners have participated;

The objectives and views of the MITIGATE pilot operations had been clearly specified and the appropriate actions were already planned so as to involve as many users as possible in order to achieve high impact and obtain the expected results.

To this extent, training material (online videos, documents, manuals, etc.) were developed, published and distributed via electronic and traditional (e.g. post) means to all different types of users in order to be able to use effectively the whole functionality of the provided MITIGATE services.

Evaluation instruments such as the MITIGATE online questionnaire tool is also further exploited with the aim to assess pilot operations by deploying online the evaluation forms of all services

On the other hand, UPRC continued to use academic publications in conference proceeding and international journals to achieve visibility to the young researchers.

Specifically, the plan of dissemination actions undertaken by PPA, SILO and UPRC can be summarised as follows:

- Creation of appropriate social media content, design and reproduction of paper-based dissemination material (i.e. flyers, posters) and constant provision of press releases that helped end-users know the schedule of MITIGATE pilot operations in Greece, acknowledge the use and value of MITIGATE platform and get familiar with the integrated interfaces and tools
- Enable pilot operations in Greece through the organisation of various events and one big Interantional Conference on the premises of the PPA in order to involve all types of users with different IT expertise (from IT experts to naive users);
- Make MITIGATE pilot operations as visible as possible to the general public though dissemination campaigns, web publications, press invitations and constant exploitation of networking and contacts;
- Collect valuable feedback and evaluation data by end-users that will participate in pilot operations, with the aim to validate the MITIGATE platform and services, assess user-acceptance, and proceed with fine-tuning operations that will enable the deployment of a successful, from the marketing perspective, final product.

Last but not least, as mentioned previously, in order to facilitate the involvement of external SCS business partners and individuals in the evaluation process, a Demo MITIGATE Port Authority Port Site, as well as other Sites (i.e. DemoMitigate, DemoCustoms, MitigatePortAuthority, MitigateCustoms, Mitigate Ship Agent, Mitigate Carrier Agent, Mitigate Local Agent) were created. These Sites was created giving the opportunity to external users to evaluate the supported services creating and conducting real and “dummy” assessments.

4 Spanish Pilot Operations

4.1 Introduction

In order to test and evaluate the Mitigate tool, some meetings/workshops have been held in Valencia with different external users taking into account their role along the supply chain.

In this sense, each user had a different profilein order to get feedback from different aspects of the platform.

4.2 Pilot Plan with External Users

In the port of Valencia, a workshop with different external users has been organized to evaluate the Mitigate tool. This workshop was organized with the people responsible for security from different organizations to analyze the need and utility of the tool. Furthermore, bilateral meetings were held with some stakeholders in the port of Valencia.

Similarly, a final workshop is planned with the last version of the platform before the end of the project.

The following table summarizes the total number of events carried out in Spain, the number of completed evaluation reports, and the registered and trained users.

Events		Completed evaluation reports		Registered users	
# of events	*# participants*	*#port operators*	*#stakeholders /individuals*	*#port operators*	*#stakeholders/individuals*
4	27	5	15	5	10

Table 3: Pilot Results in Spain

4.3 Problems & Barriers

In the scope of internal MITIGATE pilot operations that have been organized by VPORT, the main issues that were identified by the external users as an obstacle, are the following:

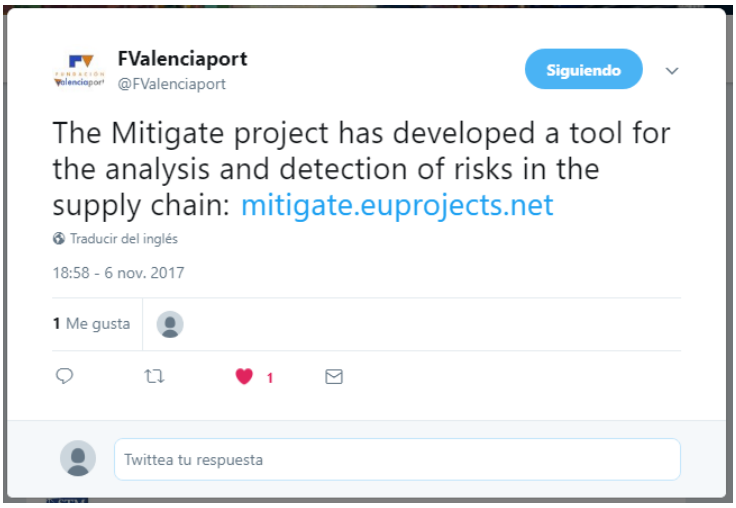
- The initial system configuration requires a lot of dedication to introduce and configure all the Sites, Networks, and Assets.
- In order to have the systemworking properly, all the actors in the supply chain should be registered and involved with the Mitigate tool. Otherwise only the own risks are evaluated and not the cascade effects. That would be difficult in the port enviroment.
- The platform connexion is http instead of https. Due is a security management platform, the access security should be high.
- Some technical comments detected by external users regarding the application are:
  - Remove the test data from the platform.
  - Change the number of elements in a list. From 10 to 20 or 50.

- Creating a vendor that already exists causes an unspecified (no message) error. Something else than "error" should be shown.
- Search vulnerabilities by selecting the asset.
- Responsive resizing window fails in some cases.
- Documentation explains how to do things, but not what they are.
- There are some error messages that the only message is error. More information should be provided.

4.4 Visibility & Dissemination Actions

The channels used to promote the Mitigate platform among the port community were social media and personal meetings with the people that could be interested in a platform to identify and mitigate risks.

Moreover, it has be held several face to face meetings in order to explain the MITIGATE PLATFORM



FVgaleraciaport

FValenciaport
@FValenciaport

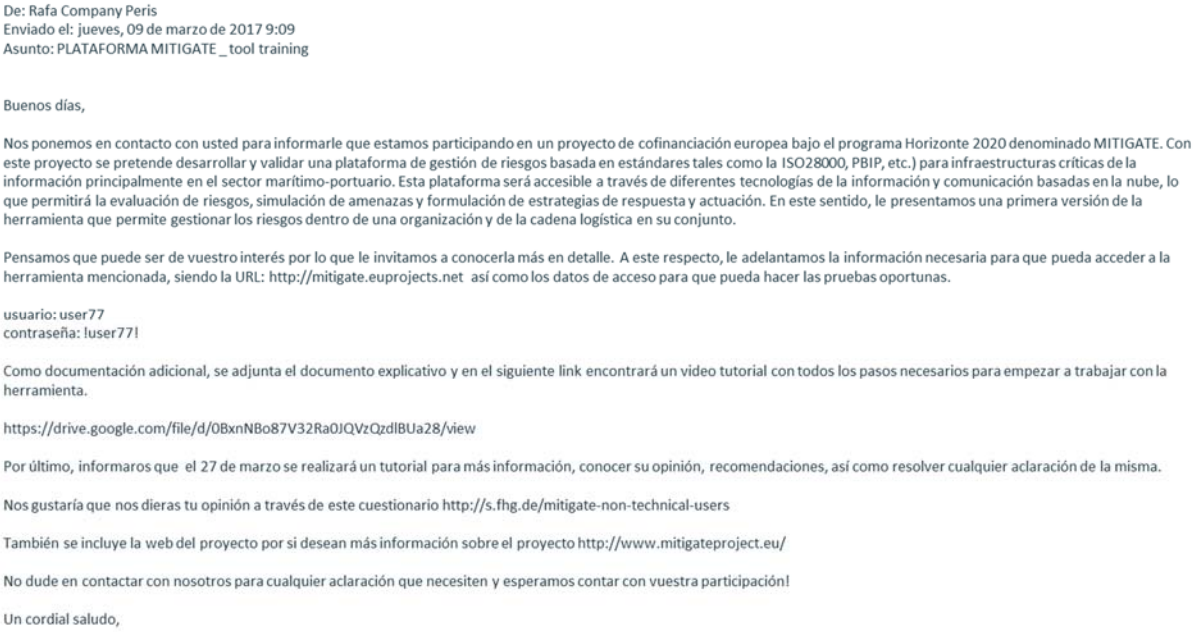
The Mitigate project has developed a tool for the analysis and detection of risks in the supply chain: mitigate.euprojects.net

18:58 - 6 nov. 2017

1 Me gusta

Figure 1. Tweet disseminating last platform version

In addition, emails were sent to several contacts in the port environment to inform about the project and inviting them to attend the tutorial workshop.



De: Rafa Company Peris
Enviado el: jueves, 09 de marzo de 2017 9:09
Asunto: PLATAFORMA MITIGATE _ tool training

Buenos días,

Nos ponemos en contacto con usted para informarle que estamos participando en un proyecto de cofinanciación europea bajo el programa Horizonte 2020 denominado MITIGATE. Con este proyecto se pretende desarrollar y validar una plataforma de gestión de riesgos basada en estándares tales como la ISO28000, PBIP, etc.) para infraestructuras críticas de la información principalmente en el sector marítimo-portuario. Esta plataforma será accesible a través de diferentes tecnologías de la información y comunicación basadas en la nube, lo que permitirá la evaluación de riesgos, simulación de amenazas y formulación de estrategias de respuesta y actuación. En este sentido, le presentamos una primera versión de la herramienta que permite gestionar los riesgos dentro de una organización y de la cadena logística en su conjunto.

Pensamos que puede ser de vuestro interés por lo que le invitamos a conocerla más en detalle. A este respecto, le adelantamos la información necesaria para que pueda acceder a la herramienta mencionada, siendo la URL: http://mitigate.euprojects.net así como los datos de acceso para que pueda hacer las pruebas oportunas.

usuario: user77
contraseña: !user77!

Como documentación adicional, se adjunta el documento explicativo y en el siguiente link encontrará un video tutorial con todos los pasos necesarios para empezar a trabajar con la herramienta.

https://drive.google.com/file/d/0BxnNBo87V32Ra0JQVzQzdlBUa28/view

Por último, informaros que el 27 de marzo se realizará un tutorial para más información, conocer su opinión, recomendaciones, así como resolver cualquier aclaración de la misma.

Nos gustaría que nos dieras tu opinión a través de este cuestionario http://s.fhg.de/mitigate-non-technical-users

También se incluye la web del proyecto por si desean más información sobre el proyecto http://www.mitigateproject.eu/

No dude en contactar con nosotros para cualquier aclaración que necesiten y esperamos contar con vuestra participación!

Un cordial saludo,

Figure 2. Email sent to the stakeholders

5 Italian Pilot Operations

5.1 Introduction

The external pilot operations operations in Italy were organized and coordinated by Port of Ravenna Authority (PRA) with the technical support of MAGG and IMSSEA.

The following paragraphs describe all important issues that came out from the MITIGATE external pilot operations plan performed in Italy. These include the identification of any potential issue / problem that need to be addressed in order to conclude with a successful implementation of pilot operations and the achievement of the expected results.

5.2 Pilot Scenario(s)

The selected scenarios for the external pilot operation in Italy are the Container Cargo Management and Bulk and General Cargo Transport. This scenarios and the purposes of the external pilots are described analytically in D5.1.

5.3 Problems & Barriers

During the external pilot tests different problems and barriers were identified and reported.

5.3.1 Business Aspects

Three main problems/issues were reported:

- Almost all of the participants noticed that to much administrative work is required: the asset mapping has to be done manually by an employee (with deep knowledge and skills in (cyber-security). In many organizations, in particular SMEs and Public Authorities, there is not such a personnel with the required skills and in general security officers have expertise only related to the physical security. Often in the medium-large companies the required information for the MITIGATE platform are already available and mapped in computer environments like Business Process Management Tools or in inventory tools. The collection of relevant information referring the cyber-related assets and the Supply Chain Services (SCS) can take a long time, depending on the size and business area of the organization. Based on the amount of different hardware, operating systems and applcations which are in use and especially the updates/patches which are installed nearly every, a manually hosting and maintainance of the MITIGATE system seems not possible without some kind of automatic functionality.
- The second problem, which is strictly related to the first point, is the need to employ further staff whith special skills when the system is in use. The MITIGATE system requires more than one skilled employee because there are many parameters correlated: (cyber-)security, ICT, logistics, port security standards and regulations, etc.
- The last comment concerns the involvement of the business partners that is considered not realistic mainly for the Public Authorities and large companies, such as the shipping lines, that normally have specific policies that prevent the transfer of (critical) data.

5.3.2 Involvement of Users

The involvement of external users was easer that the internal ones. While the internal events were more intensive, detailed and carried out in the form of trainings workshops, the external events were often based on live presentations/demo and dominated by Q&A sesssions and follow up – although in both events participants had the possibility to navigate the MITIGATE platform by themselves. Due to the fact that external users were not compensated for their partitipation in these beta tests and did that besides their normal work, the involvement of so high/senior managers and officers could be counted as an success.

5.3.3 Technical Aspects

The participants identified and mentioned two main aspects on the technical side.

- the first one is regards the missing import functionalities of assets and processes which are already modelled by the organizations using different tools. These interfaces must be implemented not only for the first and initial configuration in the MITIGATE system, but also for the import of changes which arise in small and medium sized environments many times a day, e.g. due to software updates or patches. These missing functionalities are currently a “show stopper” for the business side to establish the platform in a real environment.
- the second comment is related to the assessment reports. In general the reports were considered too poor mainly for the lack of informations about the actions that could be taken for the mitigation of the assessed vulnerabilities. The possibility to compare different risk assessments performed in different scenarios (using the same configuration of assets) was very appreciated.

5.4 Visibility & Dissemination Actions

Diffferent dissemination activities have been developed targeting institutional (external) stakeholders with the aim to increase awareness about the MITIGATE system, to strengthen and expand the involvement and mobilization of target groups, to facilitate and strengthen relations between the Italian project partners in order to achieve the expected results in other areas, to publicize the funding of the European Commission and its commitment relating to cyber risks.

The dissemination strategy was supported by a suitable visibility on media (websites, regualr email communication with target audience etc.). Moreover an evaluation of the impact on the target groups has been conducted with the request of feedback from stakeholders involved.

The actions arranged in Italy are summarized in the table below:

Event	Type	Date	Location
The First Italian Conference on Cyber Security (ITASEC’17)	Conference	17-18/01/2017	Venice
Port State Control IMO Course	Seminar	09/05/2017	Genoa

International Workshop on Supply Chain Security, Resilience and Accountability (SC-SRA'17) / within the ARES EU Projects Symposium	Workshop	29/08/2017	Reggio Calabria
4° Forum - Shipping Intermodal Forum Transport	Conference	20/11/2017	Genoa

Table 4: Visibility and Dissemination Actions

6 German Pilot Operations

6.1 Introduction

The external pilot operations in Germany were organized and coordinated by dbh Logistics IT AG (dbh) as a software manufacturer and operator of the port community system (PCS) of the ports in Bremen, Bremerhaven and Wilhelmshaven, by the Fraunhofer Centre for Maritime Logistics and Services (Fraunhofer) as well as the "Hansestadt Bremisches Hafenamt" (HBH) as a member of the User Advisory Board.

6.2 Pilot Plan with External Users

6.2.1 Pilot Scenario – High-Level-Description

The selected pilot scenario "*Road Transport and Entry of Goods at the Port Container Terminal*" for the external user operations in Germany is one of the four pilot scenarios, which are created by the different ports / partners and is as a process part of the Supply Chain Service "*Container Cargo Management*". As this scenario is already described in detail within section 3.1.4 of Deliverable 5.1 "*Pilot Sites Preparation and Detailed Operation Planning*", the following information will focus on a high level description of the process as well as to the main environmental parameters.

The process "*Road Transport and Entry of Goods at the Port Container Terminal*" is a part of the export of goods to foreign countries, wich is an main purpose of container terminals. To start such a shipment-process, the goods have to be declared to customs and need to be delivered to the port of departure. So the sub-process "Road Transport and Entry of Goods at the Port Container Terminal" involves the exchange of documents and cooperation between several actors with their own IT-systems such as exporter, freight forwarder, terminal operator, Port Community System (PCS)-operator, hauler, shipping company, customs and port authority. So in summary 8 different Stakeholder Groups are involved in this pilot scenario. Furthermore, the sub-process itself is subdivided into four process steps: the export customs declaration, the port order, the pre announcement and finally the container delivery.

On purpose, the pilot scenario was build up with "stakeholder groups" and not with the concrete company names of individual stakeholders. This makes the scenario more flexible and it could be used both for the internal as well as the external pilot operations, which various and partly competing companies from the stakeholder groups participated.

The IT-systems involved in this sub-process are different modules of the Port Community System (PCS), the German customs system for "automatic rate- and local customs handling" (ATLAS), the Advantage Customs (AC) system as a connection to the ATLAS system for other stakeholders and the freight forwarder's Advantage Local Port Order (ALPO) system. Moreover the port authority's "Bremen Ports Operating System" (BREPOS)-system, the Terminal and Gate Operating System (TOS and GOS) of the terminal operator are included in this sub-process. Generally the PCS is the main connecting link between the different stakeholder-systems. More precisely the electronic data interchange (EDI)-communication platform OSIS as a module of the PCS is involved in each data exchange process, e.g. between the shipping company's and hauler's systems. So in summary 13 IT-systems and their whole technical environments were involved in this pilot scenario.

The following graph illustrates the environment of the external pilot scenario.

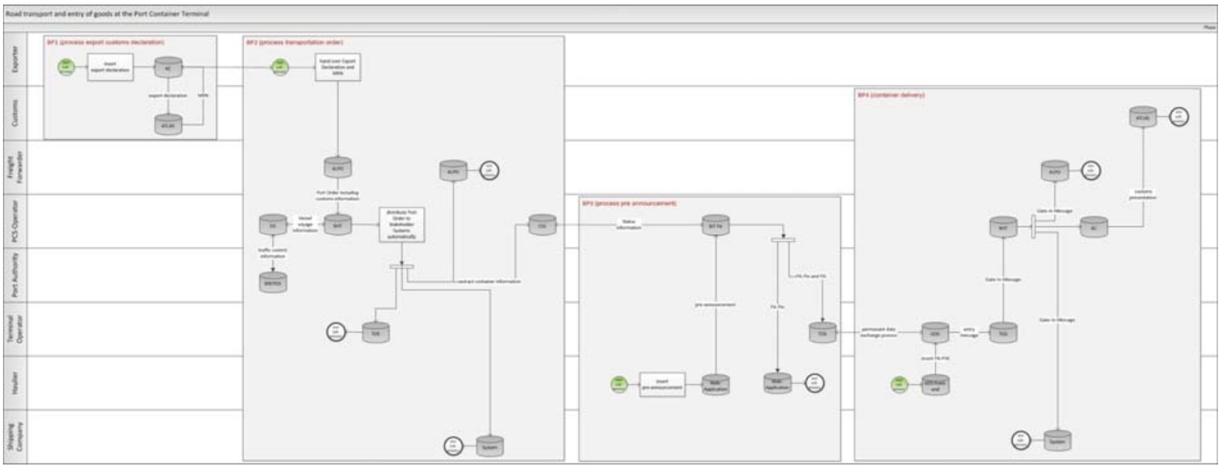

Road transport and entry of goods at the Port Container Terminal
Exporter
Customs
Freight Forwarder
PCS-Operator
Port Authority
Terminal Operator
Haulier
Shipping Company
BP1 (process export customs declaration)
BP2 (process transportation order)
BP3 (process pre announcement)
BP4 (container delivery)
System

Figure 3: Process description

6.3 Problems & Barriers

Although at the time when the events took place, the MITIGATE platform was in a development status and the final version wasn't deployed, the environment was in a good shape to present the main functions to external participants. Not only during the events but also afterwards in some networking discussions with the participants were different problems and barriers identified.

In the following sections some of the main findings will be highlighted divided in four main categories.

6.3.1 Business Aspects

Referenced to the business aspects primarily three obstacles were detected. As first topic here is to mention, that most of the participants - especially those who are dealing at a management level – have doubts that the platform needs to much administrative work. It seems that too many processes have to be done manually by an employee (e.g. a MITIGATE Administrator) instead automatically steered by a database-job or another time-based automatic interval.

In many companies, especially SME and large Logistic Service Provider, the primary foundation of the required information for the mitigate platform are already available and mapped in computer environments like Business-Process-Management-Tools as ADONIS or ARIS or with regard to the technical part of the asset collection in tools like QUADRIGA-IT. Just the collection of relevant information referring these assets and the SCS (Supply Chain Services) needs alone can take a long time in dependence to the size and the line of business of the company/institution, since an automatic import function wasn't implemented at the time of the events.

Based on the amount of different Hardware, Operating Systems and Software which are in use in a middle sized company and the updates/patches which are installed nearly every day or overnight and which are, especially in the software environment, mostly based on security aspects, a manually hosting and maintainance of the MITIGATE system seems for most of the participants not realistic without some kind of import functionality.

Based on the fact described above the second topic arise. Is there a need to employ further staff when the system is in use? And if this circumstance is happen, what special skills are needed for e.g. a system administrator and is this occupation a full-time employment or not? To find an answer for all these questions that fits to all in generally is not possible as too many environment parameter have a direct dependency to the mentioned doubts.

However the financial aspect, which is probably the main reason for these doubts, is a not insignificant factor in the decision to use the system in real live environments or not.

A third barrier from a business perspective is data security and confidentiality on every level of the system. The IT infrastructure and systems used herein are the lifeblood of a business today. To disclose information about that makes the company not only externally but also internally attackable and thus extremely vulnerable.

And although there is a contradiction that the MITIGATE platform should support a company in avoiding the risk of an attack by uncovering IT technical vulnerabilities and cyber threats, the detailed internal information required to run the MITIGATE system is expected to be not published by the institutions at all or only very hesitantly. There were doubts that unauthorized third parties e.g. like a possible "main administrator" of the MITIGATE system who is hosting in one physical environment not only his own company's information, but also the information of the other in the Supply Chain Service involved stakeholders, has access to this critical and sensitive information of business partners, too.

6.3.2 Involvement of Users

The involvement of users within the external pilots divided from the involvement of users during the internal pilot operations. While the internal events were more intensive, more detailed and carried out in the form of trainings, the external events were often based on live presentations and dominated by discussions – although in both events the participants have had the possibility to explore the MITIGATE platform by themselves. But as already mentioned, a big part of the external participants comes from the management layer of the companies or institutions what means, that they are located more on the decision level and less on the level of physical operations. Furthermore a detailed training of the MITIGATE system takes as it is planned as an expert tool, takes more than just a half or even one day. Due to the fact, that the external pilot users were not compensated for their partitipation in this time consuming beta tests and did that besides their normal work, the involvement of so much high paid managers and officers could be counted as an success, too.

However, the main obstacles were detected, highlighted and also discussed during the external pilot sessions and forwarded to the development team of the platform contemporary.

6.3.3 Technical Aspects

On the technical side three aspects were identified and mentioned by the participants. The first one is already mentioned in the business section and is dealing with the missing import functionalities of assets and processes which are already modelled by the companies with different tools like VISIO, ARIS, ADONIS (BPMN-tools) or QUADRIGA-IT (inventory management).

These interfaces must be implemented not only for the first and initial configuration in the MITIGATE system, but also for the import of changes which arise too in small and medium sized environments multiple per day, e.g. due to software updates or patches. These missing functionalities are currently a "show stopper" for the business side to establish the platform in a real environment. These aspects were discussed with the developers in real time, which led to a conception and examination of appropriate import possibilities.

The second topic which was mentioned by the participants is the improvement of graphical reports and overviews which has had on the time when the events took place more or less only basic functions. As an example zoom functionalities and more detailed information based on different layers are desirable according to the participants and with regard to the expected size of the reports or the length of the asset lists under productive conditions.

Last but not least the third aspect mentioned by the participants is dealing with the improvement of the usability, or UX (User Experience) and the integrated user guide / online manual. In terms of usability the MITIGATE system must be clearly arranged and the handling must be better adapted to the internal workflow of the MITIGATE system.

The user guide or manual should be improved in such a way that it does not follow the dialogues in the order but has to go through the sequence of the logical process, for example beginning with the logical steps during initial data collection up to run the first risk assessment. Furthermore, references should be made to the relationship between the respective step to other dependencies and what is the reason to collect information. So overall the user manual should be enriched with more detailed information and explanations of the internal system logic and structure.

6.3.4 Incidents

All incidents, obstacles and problems were reported to the technical partners both during the external pilot preparation phase as well as after the pilot events took place.

6.4 Visibility & Dissemination Actions

In order to mobilize as many and significant external pilot users and multipliers as possible, three main channels were used: an international transport and logistic trade fairy and an article in an international industry magazine to rise the awareness of the MITIGATE project in general and for the external user operations in special as well as the business contacts and an official mailing list of the participating partner organisations:

The MITIGATE project was introduced at a stand with face-to-face talks and presentations at the trade fairy “transport logistic 2017”, which took place from May 9 to 12, 2017 in Munich. According the organizers of the trade fair, it is the world´s largest sector gathering for the transport and logistics sector. With the help of the dissemination material, discussions and presentations, not only the MITIGATE project was presented the project, but also external testers were explicitly sought and addressed.

Another approach to get new and previously unknown external testers was an article published in the professional journal “Port Technology International Journal, Edition 74: Summer 2017”, which presented the project and also drew readers' attention to the external pilot phase.

The external events themselves were scheduled as late as possible to give the developing partners the time to check and discuss the feedback from the internal user operations and thus to further improve the system.

7 Conclusions

The MITIGATE system has been tested and evaluated by a number of external pilot users and maritime stakeholders. In particular, during the evaluation operation various Supply Chain Operators (such as Port operators, Ports' Security Officers, IT professionals, and Security and risk management experts) have been engaged in risk identification, assessment and mitigation based on the provided functionality of the MITIGATE system.

Representatives from four different countries participated in this External Pilot Operation phase in which 47 different events were organized and 446 individual participants were able either to be introduced of and / or to use the MITIGATE system and its services.

Events	
# of events	*# participants*
47	446

Table 5: Overview of Events

The number of events organized and the corresponding number of participants in each one of them is very satisfactory. The majority of external users participated identified and reported a significant value on the MITIGATE services and the MITIGATE system. During these events, very interesting discussions took place and useful outcomes were gathered from the consortium that will allow MITIGATE partners to successfully continue the project, as well as parameterize and build a more mature version of its services.

In the scope of the external MITIGATE pilot operations that have been organized from all Partners, not many broblems / barriers / issues appeard during their process, since many of them had been successfully identified and addressed during the pilot operations for internal users.

The most important from those that came up have as follows:

- Many users were suspicious in using their real assets and infrastructures in the scenarios since they had to be sure that privacy issues and confidentiality is confirmed. The concept of participating in a Supply Chain Risk Assessment is very new, and what it's results mean in the real world for their current synergies and signed contracts looks frightening.
- Almost all of the participants noticed that to much administrative work is required: the asset mapping has to be done manually by an employee (with deep knowledge and skills in (cyber-security). In many organizations, in particular SMEs and Public Authorities, there is not such a personnel with the required skills and in general security officers have expertise only related to the physical security. Therefore, on one hand they realized the real value of the MITIGATE system but on the other they stated that the results generated from a Supply Chain Risk Assessment need to be reviewed from a Security Consultant, who will immediately create a Risk Treatment plan for their organization. Only at this case the MITIGATE system has real value for them.

- In many companies, especially SME and large Logistic Service Provider, the primary foundation of the required information for the mitigate platform are already available and mapped in computer environments like Business-Process-Management-Tools as ADONIS or ARIS or with regard to the technical part of the asset collection in tools like QUADRIGA-IT. Just the collection of relevant information referring these assets and the SCS (Supply Chain Services) needs alone can take a long time in dependence to the size and the line of business of the company/institution, since an automatic import function wasn't implemented at the time of the events.