SPARTA

D12.7

Outermost regions engagement

Project number	830892
Project acronym	SPARTA
Project title	Strategic programs for advanced research and technology in Europe
Start date of the project	1st February, 2019
Duration	36 months
Programme	H2020-SU-ICT-2018-2020

Deliverable type	Report
Deliverable reference number	SU-ICT-03-830892 / D12.7 / V1.0
Work package contributing to the deliverable	WP12
Due date	Jan 2022 – M36
Actual submission date	31st January, 2022

Responsible organisation	INOV
Editor	Catarina Valente
Dissemination level	PU
Revision	V1.0

Abstract	This deliverable reports all the activities carried out in the scope of task 12.5: *Outermost Regions Engagement – “Go Cyber with SPARTA” campaign,* designed to encourage small businesses to adopt cybersecurity measures; stimulate young people to undertake studies or training at the university level within the area of cybersecurity; and engage with critical infrastructure operators to stimulate them to adopt state-of-the-art cybersecurity technology
Keywords	Diversity Gap, Outermost Regions of Europe, Awareness

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 830892.

Editor

Catarina Valente (INOV)

Contributors (ordered according to beneficiary numbers)

Elisabete Carreira (INOV)

Reviewers (ordered according to beneficiary numbers)

Philippe Massonet (CETIC)

Giuseppe Bianchi (CNIT)

Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Executive Summary

The present deliverable contains the report and evaluation of the activities developed in the scope of task 12.5 *Outermost Regions Engagement – "Go Cyber with SPARTA" campaign,* conceived to contribute to the EU strategy for the Outermost Regions on digital accessibility and ICT use, to help build a diverse workforce in cybersecurity, and to maximize the regional impact of SPARTA. It relied on the creation of one living lab in three Outermost Regions situated in different geographical locations (Indian Ocean; the Atlantic Ocean and the Caribbean).

Chapter 1 situates the present deliverable in the scope of the SPARTA activities, summarises the main goals of task 12.5 and describes the collaborative interactions between WP12 and the other WPs of the project, for the design and implementation of task activities.

Chapter 2 presents the *Go Cyber with SPARTA* campaign, its aims, goals and strategic approach. It provides an overview of the Outermost Regions of Europe and the SPARTA commitment to contribute to a more inclusive society, where diversity is at the foreground. This chapter also presents the partners contribution for the establishment of such campaign and its contribution to the overall project's KPIs.

Chapter 3 reports all the activities developed in the scope of task 12.5, organised by action: 1) *Encourage small businesses to adopt cybersecurity measures*; 2) *Stimulate cybersecurity studies or training at the university level;* 3) *Engage Critical Infrastructure operators with cybersecurity technology.*

Chapter 4 is a general evaluation of the activities carried out during the three years of the SPARTA project in the scope of task 12.5. It strives to provide a set of recommendations for projects wanting to pursue a similar approach. The evaluation follows the same structure as chapter 3: it will consider each action in particular.

Chapter 5 provides a brief summary and a conclusion of the main outcomes of this deliverable.

Table of Content

Chapter 1 Introduction ... 1

Chapter 2 The *Go cyber with SPARTA* strategy ... 2

2.1 Outermost Regions ... 2

2.2 SPARTA position ... 2

2.3 Action Strategy and goals ... 3

2.4 Partners contribution ... 4

2.5 Contribution to the overall project KPIs ... 4

Chapter 3 Activities report ... 6

3.1 Encourage small businesses to adopt cybersecurity measures ... 6

3.1.1 Martinique ... 6

3.1.2 Madeira ... 8

3.2 Stimulate cybersecurity studies or training at university level ... 11

3.3 Engage critical infrastructure operators with cybersecurity technology ... 12

3.3.1 La Reunions' Critical Water Infrastructure ... 13

3.3.2 La Reunion SMEs ... 16

Chapter 4 Evaluation ... 19

4.1 Encourage small businesses to adopt cybersecurity measures ... 19

4.2 Stimulate cybersecurity studies or training at university level ... 19

4.3 Engage critical infrastructure operators with cybersecurity technology ... 20

4.4 General recommendations ... 20

Chapter 5 Summary and Conclusion ... 22

Chapter 6 List of Abbreviations ... 23

Chapter 7 Bibliography ... 24

Annex 1 – Invitation for Go Cyber with SPARTA – Martinique ... 25

Annex 2 – Invitations signed for Go Cyber with SPARTA – Madeira ... 26

Annex 3 – "Go Cyber with SPARTA - Madeira" brochure ... 31

Annex 4 – List of attendees for the Go Cyber with SPARTA workshop at Madeira ... 34

Annex 5 – Cybersecurity for Water Critical infrastructures best-practices guide ... 35

Annex 6 – List of attendees of the introductory meeting with Office de l'eau La Reunion ... 37

Annex 7 – Attendance list of the Cybersecurity Training and Awareness workshop delivered to Office de l'eau La Reunion ... 38

Annex 8 – Attendance list of the "Go Cyber with SPARTA" workshop 39

List of Figures

Figure 1: E-mail flyer "Go Cyber with SPARTA" Martinique 7

Figure 2: Poster for dissemination of the "Go Cyber with SPARTA - Madeira" workshop 8

Figure 3: Presentation of the SPARTA project at "Go Cyber with SPARTA - Madeira" workshop ... 9

Figure 4: Coffee break of the "Go Cyber with SPARTA - Madeira" workshop................................. 9

Figure 5: "Threat Landscape" session at the "Go Cyber with SPARTA - Madeira" workshop 9

Figure 6: "Human Aspects of Cybersecurity" session at the "Go Cyber with SPARTA - Madeira" workshop.. 10

Figure 7: "Management and risk analysis" session at the "Go Cyber with SPARTA - Madeira" workshop.. 10

Figure 8: "Go Cyber with SPARTA - Madeira" Workshop... 10

Figure 9: "Go Cyber with SPARTA" workshop to the ULPGC.. 12

Figure 10: Cybersecurity Training and Awareness Workshop with Office de l'eau 2021, at la Reunion 16

Figure 11: Poster for the workshop "Go Cyber with SPARTA" dedicated to the SMEs in the digital sector, from La Reunion 17

Figure 12: "Go Cyber with SPARTA - La Reunion" workshop with SMEs on the digital sector 17

Figure 13: Sara Ricci on "Cryptography and Data Privacy" day 1 of thee "Go Cyber with SPARTA - La Reunion" workshop with SMEs on the digital sector 18

Figure 14: Lukas Malina on "System and Network Security" day 2 of the "Go Cyber with SPARTA - La Reunion" workshop with SMEs on the digital sector 18

List of Tables

Table 1: Contribution to the KPIs of objective 6.. 4

Table 2: Contribution to the KPIs of objective 3.. 5

Table 3: Program for Office de l'eau on-site workshop.. 14

Table 4: Program for Office de l'eau remote workshop 15

Table 5: Program for "Go Cyber with SPARTA" workshop for La Reunion SMEs......................... 16

Chapter 1 Introduction

The WP12 – Dissemination and communication – aims to plan, coordinate and execute all SPARTA activities related to dissemination and communication, and integrates a specific approach to the engagement of the Outermost Regions of Europe with the SPARTA project, its aims, activities, and results. Such approach is established in a dedicated task – 12.5 *Outermost regions engagement – “Go Cyber with SPARTA” campaign*.

Task 12.5 aims at engaging three Outermost Regions – situated in different geographic locations (Indian Ocean; the Atlantic Ocean and the Caribbean) – with the SPARTA project, through a specific approach that allows their direct participation in the project, creating knowledge through win-win cross-collaborations, where diversity and inclusion are at the foreground. To this end, the *Go Cyber with SPARTA* campaign embraces the design and placement of different actions in each chosen region while ensuring the diversity and representativeness of the education, business and critical infrastructure sectors to which the SPARTA project is dedicated to. The campaign aimed at creating cybersecurity awareness on the Outermost Regions of Europe and at influencing good cybersecurity practices.

The achievement of this task relied on ongoing interactions with other relevant SPARTA WP’s and partners to receive inputs that allowed for the implementation of the planned activities, namely WP9 – Cybersecurity training and awareness – and WP1 – CCN Governance and assessment.

Chapter 2 The *Go cyber with SPARTA* strategy

This chapter presents the *Go Cyber with SPARTA* campaign, its aims, goals and strategic approach. It provides an overview of the Outermost Regions and the SPARTA commitment to contribute to a more inclusive society, where diversity is at the foreground. This chapter also presents the partners contribution for the establishment of such campaign and its contribution to the overall project's KPIs.

2.1 Outermost Regions

Guadeloupe, French Guiana, Martinique, Saint Martin, Réunion, Mayotte (France); the Canary Islands (Spain); and the Azores and Madeira (Portugal) are an integral part of the European Union Territory, despite the thousands of kilometres separating them from the European continent. These nine Outermost Regions (ORs)[1] are under the same rights and obligations of the European Treaties[2] for their 4.8 million citizens. They are islands and archipelagos located in the Caribbean basin, in the western Atlantic and in the Indian Ocean or landlocked territory in the Amazonian Forest.

Over the last years, the ORs were very active in reducing the gap in digital accessibility and ICT use. Ambitious programmes at the national and regional levels have been set up to support infrastructure deployment as well as the development of digital services. In 2017, an expert group on digital accessibility and ICT use contributed to assess the current situation and identifying the key challenges for the future in the perspective of the renewed EU strategy[3]. Several recommendations were made, with a strong focus on the need to strengthen local infrastructures and promote digital skills and the local ICT sector. It is only possible to ensure digital security and the strategic autonomy of the EU if all actors are included. Awareness and enforcement of cyber security are crucial to prevent cybercrime and ensure Europe's digital sovereignty.

In this context, the SPARTA project designed task 12.5 *Outermost Regions Engagement – "Go Cyber with SPARTA" campaign,* aimed at engaging these regions with the SPARTA project ambitions, activities and results, and bringing them cybersecurity knowledge.

2.2 SPARTA position

SPARTA is committed to contributing to a more inclusive society. As such, during the project's lifetime, the SPARTA consortium addressed diversity in its multiple forms by promoting the engagement of associated partners, stakeholders, and end-users, considering geographical, cultural, societal, and sectoral diversity.

The creation and set-up of task 12.5 *Outermost Regions Engagement – "Go Cyber with SPARTA" campaign* concretized such commitment. It aimed at contributing to the European Commission objectives set for the OR's – strengthen local infrastructures and promote digital skills and the local ICT sector – and to maximize the regional impact of SPARTA. The strategy and goals of the *Go Cyber with SPARTA* campaign are detailed below.

[1] http://ec.europa.eu/regional_policy/sources/policy/themes/outermost-regions/pdf/rup_2017/rup_eu_lands_world_en.pdf

[2] http://ec.europa.eu/regional_policy/index.cfm/en/policy/themes/outermost-regions/

[3] http://ec.europa.eu/regional_policy/sources/policy/themes/outermost-regions/pdf/ict_report_en.pdf

2.3 Action Strategy and goals

The *Go Cyber with SPARTA* campaign was designed to contribute to the EU strategy for the ORs on digital accessibility and ICT use, to help build a diverse workforce in cybersecurity, and to maximize the regional impact of SPARTA. It relied on the creation of one living lab in three OR's geographical regions (Indian Ocean; the Atlantic Ocean and the Caribbean). Each living lab action targeted a different (yet common) goal, described as follows:

1. Encourage small businesses to adopt cybersecurity measures (the Caribbean and South America ORs)
2. Stimulate young people to undertake studies or training at the university level within the area of cybersecurity (Atlantic Ocean ORs)
3. Engage with critical infrastructure operators to stimulate them to adopt state-of-the-art cybersecurity technology (Indian Ocean ORs).

The strategy that sustained each action was grounded in a coordinated approach, involving SPARTA partners and the region's community, aiming to forge a win-win collaboration where diversity is at the foreground, ensuring that each action is deployed taking into account the institution's specific needs at the cybersecurity level.

To that end, the methodology used to develop this approach relied on the theoretical basis of Design Science Research[4]. This methodology allows for a rigorous process to design artefacts to solve observed problems, to make research contributions, to evaluate the designs, and to communicate the results to appropriate OR audiences. Techniques such as focus groups and surveys were selected to evaluate the cybersecurity informational needs of each chosen institution (SMEs, universities and Critical Infrastructures) as well as to evaluate the artefacts previously designed and developed in SPARTA, to be deployed within each action. In the final stage, surveys and semi-structured interviews were applied to evaluate the results of the different artefacts. Such procedures are described in more detail in Chapter 3.

For the long and short run, the SPARTA impact will be maximised through the connections between the selected regions/institutions and the stakeholders of other ORs in the same region of the world, for dissemination and communication of the SPARTA solutions. These awareness and communications activities were designed to include innovative and appealing ways to communicate SPARTA solutions (hands-on activities and demonstrators) to foster the interest of stakeholders in the importance of cybersecurity themes.

The three interdependent strategic axes established in deliverable 12.1 serve as the grounding basis to conduct and develop all the activities conducted in the scope of the WP12, and are highlighted below:

Awareness: making the project and its aims acknowledged.

Participation: engaging target groups and enabling them to understand SPARTA concepts and results achieved.

Action: promoting action from target groups influencing practices, products and standards.

The "Go Cyber with SPARTA" campaign was designed and developed regarding these three strategic axes. During the first year of the project, the activities mainly focused on awareness building through the presentation of the SPARTA project to the selected regions' institutions, SME's or Critical Infrastructures. The second year foresaw the engagement of these entities with the SPARTA concepts and results achieved, trough the initiation of the *Go Cyber with SPARTA* campaign activities. The last period of the project was dedicated to the call for action from these bodies to

[4] Dresch A., Lacerda D.P., Antunes J.A.V. (2015) Design Science Research. In: Design Science Research. Springer, Cham. https://doi.org/10.1007/978-3-319-07374-3_4

adopt cybersecurity measures and aquire a safer behaviour in the cyberspace through tailored training and awareness workshops.

2.4 Partners contribution

As this activity heavily relies on the correct and timely deployment of the SPARTA results, which the regions will engage with and use, all SPARTA partners were essential in the collaboration that ranged from ensuring the availability of results and tools, identifying the entities, assessing their cybersecurity informational needs and creating appropriate training and awareness workshops.

Cooperation with WP9 – Cybersecurity Training and Awareness – was of foremost importance for the success of this task, which relied on the deployment of several cybersecurity training and awareness workshops. The Brno University of Technology and SMILE contributions were essential to the efficient concretization of the *Go Cyber with SPARTA* campaign and are described in more detail in Chapter 3.

Cooperation with WP1 – CCN Governance and Assessment – was equally important for the establishment of the *Go Cyber with SPARTA* campaign, for bridging the state of the activities developed in each WP to the resources needed for the campaign, and for supporting all the activities development.

2.5 Contribution to the overall project KPIs

The task 12.5 *Outermost Regions Engagement – "Go Cyber with SPARTA" campaign* contributed to the achievement of specific project KPIs, through the deployment of several workshops and awareness building. This section provides the achieved results on enhancing awareness, training capabilities and cybersecurity skills, measured as follows:

Objectives with WP9:	M12		M24		M36	
	Expected	Achieved	Expected	Achieved	Expected	Achieved
6.3 - number of directly addressed people (through participation at conferences, workshops, trainings, etc.) by the awareness program by the end of the project.	> 500	> 1000	> 2250	> 2452	> 5000	>6574* + 2132** = 8706
6.4 - number of indirectly addressed people (through advertisements, social media) by the awareness program by the end of the project.	> 2000	> 10 000	> 20000	> 22300	> 50000	>80 000 (Higher reach of a post)

Table 1: Contribution to the KPIs of objective 6

***** Total of KNOWN numbers of attendees of the several conferences, workshops and trainings promoted by SPARTA. The total number of attendees related to participation at bigger events where SPARTA participated exceeds this number.

** Total of participants at cybersecurity awareness training events, simulation exercises, and specifics courses, special SMILE cybersecurity events, Letz Cybersecurity Challenge, and specific missions provided and reported by WP9.

Build sustained collaboration with academic, industrial, governmental and community stakeholders, which will be measured as:

Objectives with WP3 and WP8:	M12		M24		M36	
	Expected	Achieved	Expected	Achieved	Expected	Achieved
3.1 - number of workshops organized and number of attendees per workshop	> 12 > 20	> 8 > 30	> 24 > 20	> 17 > 120	> 36 > 50	39 > 120

Table 2: Contribution to the KPIs of objective 3

Chapter 3 Activities report

Chapter 3 reports all the activities developed in the scope of task 12.5 *Outermost Regions Engagement – "Go Cyber with SPARTA" campaign* during the project's lifetime.

3.1 Encourage small businesses to adopt cybersecurity measures

The first year of the project foresaw the design phase of each action, and, in line with the strategic axes established in deliverable 12.1 – *Dissemination and communication plan, updates and evaluation* – envisioned the set-up of the "Awareness building" axis. During this period, WP12 strived for selecting and contacting one outermost region per location (the Caribbean and South America, Atlantic Ocean, and the Indian Ocean). The first action – *Encourage small businesses to adopt cybersecurity measures* – was planned to be delivered in an outermost region located in the Caribbean or South America through the following activities:

Step 1: Select 10 SMEs to go onboard the *Go cyber with SPARTA* campaign through participation in a cybersecurity training and awareness workshop tailored to their informational needs. The directives for choosing the small enterprises were the following:

- The small business enterprise must follow the EU definition parameters;
- The small business enterprise must ground its business on the computer and the internet. Such as having a website or depending on the internet to develop part of their business;
- Have superficial or poor knowledge of cybersecurity.

Step 2: Send an invitation to participate in the *Go Cyber with SPARTA* campaign and briefly introduce the SMEs to the SPARTA project. A non-disclosure agreement is provided to ensure the confidentiality of information to the SMEs. Both the invitation letter and the non-disclosure agreement are translated into French and provided by CEA.

Step 3: Collect their cybersecurity informational needs via a **questionnaire** specifically developed for this action by WP9 *Cybersecurity training and awareness.* The questionnaire allows for an in-depth analysis of such inputs.

Step 4: Analyse the collected information and build a cybersecurity training and awareness workshop that fulfils the encountered needs.

Step 5: Prepare a **Training and Awareness workshop** for non-cyber security professionals on cyber threats, cybersecurity hygiene and best practices.

3.1.1 Martinique

WP12 selected Martinique and during the first year several contacts have been made to different entities in Martinique to foster collaborations, such as the direction of Technopole Martinique, who then forwarded to the Direction du Développement Economique et des Entreprises, who directed to Ms. Laury Latchoumanaya, at the Chambre du Commerce et L'Industrie. Ms. Laury Latchoumanaya established contacts between INOV and Arobase 972, Centre d'Affaires Californie, mediated by Ms. Clotilde Marcellin.

Year two foresaw the start of the "participation" axis and the development of collaborations with Arobase 972, Centre d'Affaires Californie, created by the Chamber of Commerce and Industry of Martinique, with the mission of supporting the development and structuring of an effective technological and digital innovation ecosystem in Martinique. They provide a structure that promotes the development of projects (i.e., promotion of workshops to develop in the world of digital and technological innovation; have a central co-working space for all entrepreneurs, researchers, followers of an innovative and creative setting, among others).

As a first step, INOV organised a meeting with Arobase 972, Centre d'Affaires Californie to present the SPARTA project and the *Go Cyber with SPARTA* campaign, its goals and proposed actions. This meeting took place on the 26th of October 2020, online, with the following agenda:

1) Presentation of the SPARTA project;
2) Presentation of the *Go cyber with SPARTA* campaign;
3) Invitation for participation on the *Go cyber with SPARTA* campaign through the following actions:
   a) Arobase 972, Centre d'Affaires Californie, because of its proximity with SMEs in the digital sector, responsible for selecting 10 SMEs entitled to participate in the campaign;
   b) INOV sends a formal invitation – Annex1 – to the selected SMEs for participating in the *Go Cyber with Sparta* campaign, along with a graphic image of the campaign – Figure1.
   c) Participants are to answer a questionnaire form aiming to assess their informational needs;
   d) Analysis of the questionnaire results and preparation of a training action to highlight measures and solutions to mitigate the problems and needs encountered.
   e) Deployment of the cybersecurity training and awareness workshop either online or offline, depending on the necessary restrictions imposed by the COVID-19 pandemic;
   f) The contents of this cybersecurity training and awareness workshop are to be provided to CCI Martinique in the form of best practices and rules on cyber-hygiene;
4) Preparation and deployment of a Non-disclosure Agreement to ensure the confidentially of such activity;
5) Invitation to be part of the SPARTA project, as an "Associate" or "Friend".

An online follow-up meeting on the 28th of January, 2021, occurred to provide the materials needed and set the ground for starting the proposed activities, assessing any constraints that could have appeared (language, covid-19, etc.). SPARTA provided some guidance on how to obtain a cybersecurity certification with the ANSSI and their cybersecurity pole.

Even though INOV, in cooperation with CEA, had provided all the materials and had the necessary resources set for the deployment of the workshop, the COVID-19 pandemic impacted the natural flow of activities, impeding in-person meetings and possibly delaying commitments. INOV had never received the list of ten SMEs to whom the workshop could have been delivered, having received the feedback that the SMEs were not being receptive to the workshop.

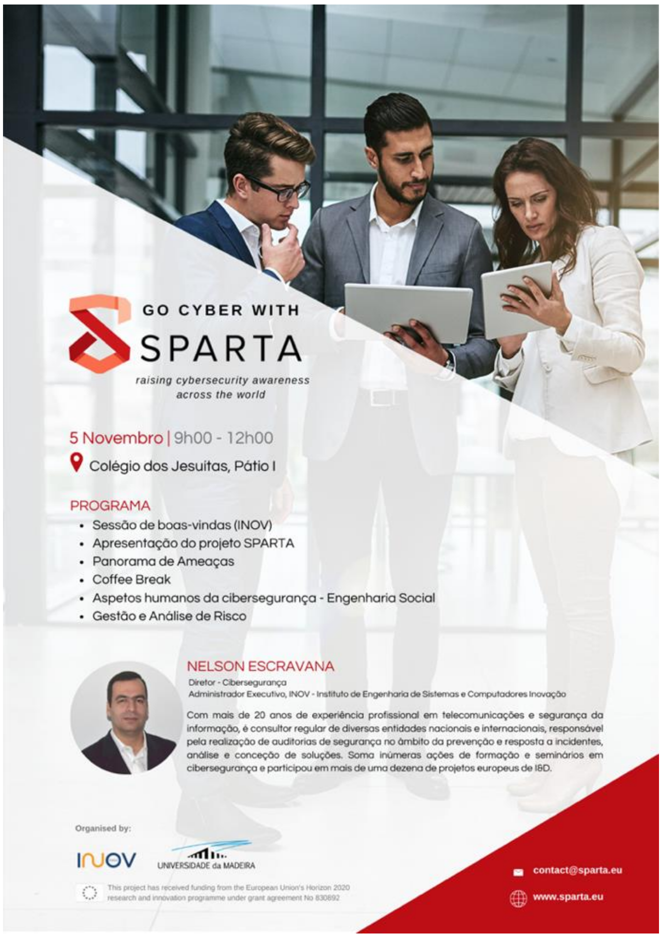
GO CYBER WITH
SPARTA
raising cybersecurity awareness across the world
CONTACT
contact@sparta.eu
www.sparta.eu
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892

Figure 1: E-mail flyer "Go Cyber with SPARTA"
Martinique

3.1.2 Madeira

On July 2021 (M29), as WP12 had not yet (after several attempts) received any positive feedback from Arobase 972, INOV opted for fostering communications with Madeira, a Portuguese OR, as a backup plan to deliver such action. As INOV has a strong link with universities in the country, the first online meeting was with the University of Madeira, represented by Professor Frederica Margarida Camacho Gonçalves, on the 19th of July, and followed the agenda below:

1) Presentation of the SARTA project;
2) Presentation of the *Go Cyber with Sparta* campaign;
3) Invitation for participation on the *Go cyber with Sparta* campaign through the following actions:
   a) Selection of 5 SMEs in the Tourism sector to participate in the campaign;
   b) Send a formal invitation to participate – Annex 2;
   c) Participants will be asked to fill in a questionnaire for assessing their cybersecurity informational needs;
4) Preparation and deployment of a Non-disclosure Agreement to ensure the confidentially of such activity;
5) Presentation to the University of Madeira of the SPARTA Cybersecurity Curricula Designer and the SPARTA Cybersecurity Education Map tools;
6) Invitation to be part of the SPARTA project, as an "Associate" or "Friend".


GO CYBER WITH
SPARTA
raising cybersecurity awareness across the world

5 Novembro | 9h00 - 12h00
Colégio dos Jesuitas, Pátio I

PROGRAMA
- Sessão de boas-vindas (INOV)
- Apresentação do projeto SPARTA
- Panorama de Ameaças
- Coffee Break
- Aspetos humanos da cibersegurança - Engenharia Social
- Gestão e Análise de Risco

NELSON ESCRAVANA
Diretor - Cibersegurança
Administrador Executivo, INOV - Instituto de Engenharia de Sistemas e Computadores Inovação

Com mais de 20 anos de experiência profissional em telecomunicações e segurança da informação, é consultor regular de diversas entidades nacionais e internacionais, responsável pela realização de auditorias de segurança no âmbito da prevenção e resposta a incidentes, análise e conceção de soluções. Soma inúmeras ações de formação e seminários em cibersegurança e participou em mais de uma dezena de projetos europeus de I&D.

Organised by:
INOV
UNIVERSIDADE da MADEIRA

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892

contact@sparta.eu
www.sparta.eu

Figure 2: Poster for dissemination of the "Go Cyber with SPARTA - Madeira" workshop

In a cooperative effort, Professor Frederica Margarida Camacho Gonçalves selected five SMEs from Madeira, from the tourism sector, and INOV sent the invitations for participation in the campaign, along with a brochure explaining its concept and aims – Annex 3. The option for SMEs in the tourism sector relies on their importance for the regions' economic stability and development.

The selected SMEs were receptive and enthusiastic about the campaign, and all signed the invitations. They filled in the questionnaire form, allowing INOV to develop a tailored cybersecurity and training awareness workshop. The workshop was at Colégio dos Jesuítas building, Funchal, Madeira, on the 4th of November 2021, led by Nelson Escravana, Cybersecurity Director at INOV and involved in the SPARTA WP4 – T-Shark programme.

To maximise SPARTA impact in this region, and because the SMEs' cybersecurity knowledge was not extensive, INOV and the University of Madeira agreed to make the workshop public for a wider audience. To this end, INOV prepared the communication materials – Figure 2 –disseminated through the University of Madeira communication channels (social media, mailing list and website). In total, the "Go Cyber with SPARTA – Madeira" workshop had 31 attendees – Annex 4 – both from the SMEs and from the University of Madeira. The workshop respected the following agenda:

- Welcome Session
- SPARTA Project presentation

- Threat landscape
- Human aspects of cybersecurity – social engineering
- Management and risk analyses

This workshop was an opportunity to present the SPARTA project, create awareness on the cybersecurity issues - not only to the SMEs but also to several university students - and provide guidance on how to protect a business from cyber-attacks. Images 3 to 8 illustrate the workshop. The University of Madeira became an associate of the SPARTA project.

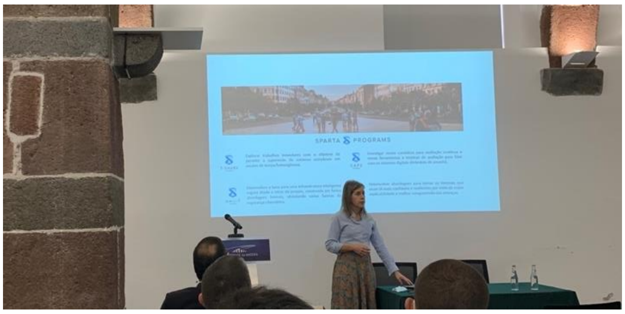


Figure 3: Presentation of the SPARTA project at "Go Cyber with SPARTA - Madeira" workshop

Figure 4: Coffee break of the "Go Cyber with SPARTA - Madeira" workshop

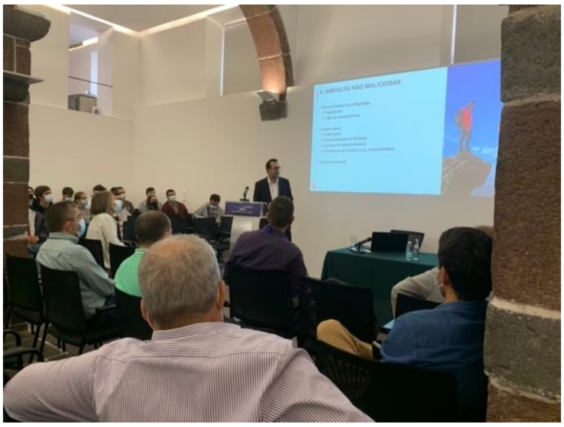


Figure 5: "Threat Landscape" session at the "Go Cyber with SPARTA - Madeira" workshop

Figure 6: "Human Aspects of Cybersecurity" session at the "Go Cyber with SPARTA - Madeira" workshop

Figure 7: "Management and risk analysis" session at the "Go Cyber with SPARTA - Madeira" workshop

Figure 8: "Go Cyber with SPARTA - Madeira" Workshop

3.2 Stimulate cybersecurity studies or training at university level

During the first year of the project, WP12 designed the scope of this action in close collaboration with WP9 – Cybersecurity Training and Awareness. The selected OR at the Atlantic Ocean location was Las Palmas de Gran Canaria.

WP12 and WP9 reached a common understating that for stimulating cybersecurity studies at the university level the work developed within the WP9 – namely the SPARTA cybersecurity curricula designer and the SPARTA cybersecurity study programs map – should be leveraged through the engagement of a university (in this region, the University of Las Palmas de Gran Canaria – ULPGC) with such tools.

The SPARTA project intends to re-think the EU cybersecurity curricula at multiple levels to design new and improve existing curricula for bachelor degrees and master degrees in computer security across Europe, making that content available to be used as necessary by universities, including ULPGC.

To this end, action 2 - Stimulate cybersecurity studies or training at the university level – foresaw the following activities, to be developed in close coordination and cooperation between WP12, WP9 and ULPGC, leveraging from the activities that were already being developed within WP9[5]:

1. Define the essentials of computer security that should be present in all computer science curricula, with the contribution of ULPGC.
2. Design new and improve existing curricula for bachelor degrees in computer security based on the ULPGC needs.
3. Provide a training workshop on how to use the SPARTA curricula designer and the SPARTA cybersecurity study programs map.

INOV contacted the ULPGC and organized a meeting at the University premises to present the SPARTA project and the *Go cyber with SPARTA* campaign. This meeting was on the 23rd of October 2019.

ULPGC accepted to participate in the campaign and help WP9 build the Cybersecurity Study Programs map by making available the courses they provide related to cybersecurity, which now feature the map.

WP9 proceeded with the analysis of the existing "Degree in Computer Engineering" and its potential for creating a specialized program on cybersecurity. The results were delivered to the ULPGC through an online workshop on how to design and implement a bachelor study program on cybersecurity. The workshop was online on the 2nd of June 2021.

The first session of the workshop started with a brief presentation of the SPARTA project, the *Go Cyber with SPARTA* campaign and the far-reaching work of the WP9 - that already counts with the deployment of a Cybersecurity Skills Framework, a user-friendly Cybersecurity Education Map and an intuitive Cybersecurity Curricula Designer (a tool that connects education providers with the cybersecurity job market).

The second session, led by Edmundas Piesarskas, was dedicated to explaining the challenges that the EU is facing in the cybersecurity domain and how a Cybersecurity Skills Framework is part of the response to the skills gap challenge. Here we explained how the NICE framework was used as the input material (having a high level of detail, consisting of over 1000 “tasks” and 600 “knowledges”), along with the JCR Taxonomy, and adapted to the EU landscape. We explained how the applicability to academia and the industry were tested by practical applications for analysing and creating curricula. More was explored in detail, such as the recommendations of national bodies, computational associations, standardization organizations, ENISA, ECSO, CyBOK, etc.

[5] For more detailed information about the activities developed within WP9 – Cybersecurity training and education – see D9.1: Cybersecurity skills framework and D9.2: Curricula descriptions.

The third session, led by Jan Hajny, was a practical workshop on how to use the Education Map application for searching and getting information about cybersecurity education providers worldwide.

Sara Ricci led the fourth session on how to create a successful cybersecurity study program, taking into account the current courses that the ULPGC has to offer and their needs. Sara presented the results of the team's Curricula Statistical Analyses to the ULPGC and presented what was needed to create a good-practice cybersecurity bachelor degree on cybersecurity. This involved (1) a review on curricula's good practices, (2) a set of recommendations on courses to be included in bachelors, and a (3) presentation of examples on how to adapt current courses and expertise domains to a bachelor on Cybersecurity. Sara made a practical example, using the data about the ULPGC courses imported to the Curricula Designer.

The workshop ended with the common will to establish a Cybersecurity bachelor degree on ULPGC in a collaborative effort with SPARTA.

Hajný Jan (89784)
Francisca Candelaria Quintana Domínguez
Subdirector de Relaciones Institucionales y Movilidad - EII
01:46:01
Subdirección de Calidad e Innovación
AN
AC
CR
MA
RS

Figure 9: "Go Cyber with SPARTA" workshop to the ULPGC

3.3 Engage critical infrastructure operators with cybersecurity technology

The scope of action 3 – Engage Critical Infrastructure operators with cybersecurity technology – was planned to be delivered in an outermost region located in the Indian Ocean, through the following designed activities:

1. Implement an awareness campaign to encourage employees from a critical infrastructure to adopt cybersecurity measures, taking into account their cybersecurity informational needs.
2. Identification of solutions for specific problems using knowledge developed within SPARTA, namely within the JCCI.
3. Organisation of a cybersecurity training and awareness workshop for non-cybersecurity professionals

INOV targeted at promoting this action at La Reunions' Critical Water Infrastructure – Office de l'eau – for its remote location, representativeness, and critical importance for the wellbeing of La Reunion' population.

3.3.1 La Reunions' Critical Water Infrastructure

Contacts with the director of Office de l'eau Réunion, Gilbert Sam Yin Yang, were established and led to the organisation of a first meeting on the 14th of November 2019, at Office de l'eau premises, in La Réunion. The meeting was conducted in French language and had the following agenda:

- SPARTA Project presentation;
- Go cyber with SPARTA campaign presentation;
- Invitation to be part of the SPARTA project, as an "Associate" or "friend", to stay aware of the results of the project or to participate more actively through "workshops" that are organized regularly;
- Deployment of a brochure – Annex 5 – with a best-practices guide on how to protect a critical infrastructure from cybersecurity attacks;
- Discussion / Q&A / Next-Steps.

At the meeting were present the Office de l'eau Director, Gilbert Sam Yin Yang, the Deputy Director, Faiçal Badat, the IT Manager, Olivier Chane Kane, and his team, Olivier Sampoil and Yohann Cimbaro – List of attendees in annex 6. As there was a common will to be part of the *Go Cyber with SPARTA* campaign, the next-steps were agreed as follows:

- Formalise Office de l'eau participation in the *Go Cyber with SPARTA* campaign, through a Non-Disclosure Agreement, signed by both parts;
- Provide a Cybersecurity risk assessment to Office de l'eau aiming to understand their cybersecurity state-of-art and training needs;
- Build a training and awareness workshop that tackles such needs;

Office de l'eau showed interested on the SPARTA project, was willing to participate in the campaign, and became part of the Associates Program to actively engaged with the project.

In a collaborative approach, Security Made in Luxembourg, a SPARTA partner, proceeded with the cybersecurity risk assessment of Office de l'eau, and provided a complete report that guided the next steps of this action. One of the considerations made in the report was a cybersecurity training workshop with Office de l'eau employees to raise awareness of cybersecurity and cyber hygiene in the work environment.

Such workshop was developed by WP9 – in specific by the Brno University of Technology – during the third year of the project, leveraging on the work that was being developed within the SPARTA project and bridging with the infrastructure needs, highlighted in the report provided by Security Made in Luxembourg.

The Cybersecurity Training Workshop was a hybrid workshop (on-site and online), with one week duration, from the 15th to the 19th of November, provided to the IT team of Office de l'eau. Figure 10 provides an evidence of this workshop, held at their premises, and annex 7 is the attendance list of this event. Tables 1 and 2 highlight the contents covered on the workshop:

DAY 1 – Cryptography and Data Privacy (November 15th – 4 hours)	
Lecturer	Sara Ricci
Content	Terminology, Basic Mathematical Foundations, Symmetric Cryptography, Asymmetric Cryptography, Protocols, Data privacy, Anonymization
DAY 2 – Legal Aspects of Privacy and Personal Data Protection (November 16th – 5 hours)	
Lecturer	František Kasl
Content	Personal data - principles, EU framework - GDPR, other frameworks worldwide (US, UK, China, Africa, Australia) Privacy - principles and concept of privacy, privacy in workplace (case-law of European court of human rights regarding permissible monitoring of employees), practice worldwide (US, UK, China, Africa, Australia) Examples and practical cases - application of the legal frameworks, risk assessment for personal data, determination of appropriate measures, relevance of context, available use cases (case-law / examples from methodologies etc.), sources for further guidance and understanding
Lecturer	Pavel Loutocký
Content	Cybersecurity requirements - EU law and NIS directive, recommended measures and procedures / other legal regulation (US, China) Authentication and access control, identity management Cross-border aspects and contract law with practical implications
DAY 3 – System Security (November 17th – 4 hours)	
Lecturer	Petr Dzurenda
Content	OS security (MS Windows, Linux, macOS): focus on MS Windows security, user authentication, data security (File and Folder Permissions, Encryption), Windows Firewall
DAY 4 – System and Network Security (November 18th – 4/5hours)	
Lecturer	Petr Dzurenda and Lukas Malina
Content	Ethical hacking, penetration testing, vulnerabilities L2-L7 security protocols (MACSec, IPsec, TLS), VPN, FW, IDS/IPS, logging and monitoring
DAY 5 – Network Security in Practice (November 19th – 4 hours)	
Lecturer	Lukas Malina
Content	Secure configuration (hardening) of network devices (switches, AAA, routers, firewalls, IPS) in practices, focused on CISCO (packet tracer)

Table 3: Program for Office de l’eau on-site workshop

Awareness – Network Security in Practice (November 10th – 2 hours)	
Lecturer	Jerome Jacob
Content	Introduction: - Threats (internal/external) and vulnerabilities: where they come from, and how to recognize them - How to protect yourself from threats and vulnerabilities - The cyber risk Adopting initial reflexes: - Be aware: the first protective barrier - Survival kit: passwords, smartphone, social network updates ... Protecting yourself: - Human factor: strong link and weak link - Social engineering, phishing: protecting your personal, family and social unit - Sing messaging, means of communication, social networks (in your private/professional life), etc. Managing your security: - Security incidents: malicious acts, attacks, negligent actions, accidents, impacts, etc. - Prevention and protection: how to set up the right measures - Mobility: safe use of smartphones, tablets, laptops, etc.
ICS Security (In French) – November 25th, all day	
Lecturer	Alexandre Delab
Content	**Concepts principaux des systèmes industriels:** - Définitions, les différents types de systèmes industriels; - Composition d'un système industriel; - Les langages de programmation d'un PLC; - Les protocoles et bus de terrain; - Les architectures réseaux classiques; - Introduction à la sûreté de fonctionnement; - Panorama des normes et standards. **Étude de la cybersécurité des systèmes industriels:** - Enjeux; - État des lieux, historique; - Dualité sûreté de fonctionnement et cybersécurité; - Exemples d'incidents; - Les vulnérabilités et vecteurs d'attaques classiques; - Panorama des normes et standards; - En France, la LPM; - Le projet de cybersécurité du système industriel; - Les recommandations.

Table 4: Program for Office de l'eau remote workshop

Figure 10: Cybersecurity Training and Awareness Workshop with Office de l'eau 2021, at la Reunion

3.3.2 La Reunion SMEs

Aiming at maximising the SPARTA impact, efforts and resources in this region, WP12 and WP9 organised a cybersecurity training and awareness workshop to be deployed to SMEs based in La Reunion, working on the digital sector. This workshop was built leveraging from the contents prepared for the workshop deployed to Office de l'eau, and contains the following program:

DAY 1 – Cryptography and Data Privacy (November 16th – 4 hours)	
Lecturer	Sara Ricci
Content	Terminology, Basic Mathematical Foundations, Symmetric Cryptography, Asymmetric Cryptography, Protocols, Data privacy, Anonymization
DAY 2 – System and Network Security (November 18th – 4/5hours)	
Lecturer	Lukas Malina
Content	Ethical hacking, penetration testing, vulnerabilities L2-L7 security protocols (MACSec, IPsec, TLS), VPN, FW, IDS/IPS, logging and monitoring

Table 5: Program for "Go Cyber with SPARTA" workshop for La Reunion SMEs

To that end, INOV established contacts with Digital Reunion, an association that brings together market players, directly and indirectly, involved in the digital sector (companies, start-ups, groups, trade unions, institutions, training organizations, etc.), intending to participate in the creation of economic, legislative and competitive conditions essential to the proper development of the sector.

Claire Alanoix was our contact point and showed a keen interest in being part of the "Go Cyber with SPARTA" campaign and thus in being involved within the SPARTA project. Digital Reunion became part of the Associate program.

Collaborations started for gathering several SMEs in the digital sector, interested in receiving the lecturers highlighted above and inviting them to participate in the *Go Cyber with SPARTA* campaign.

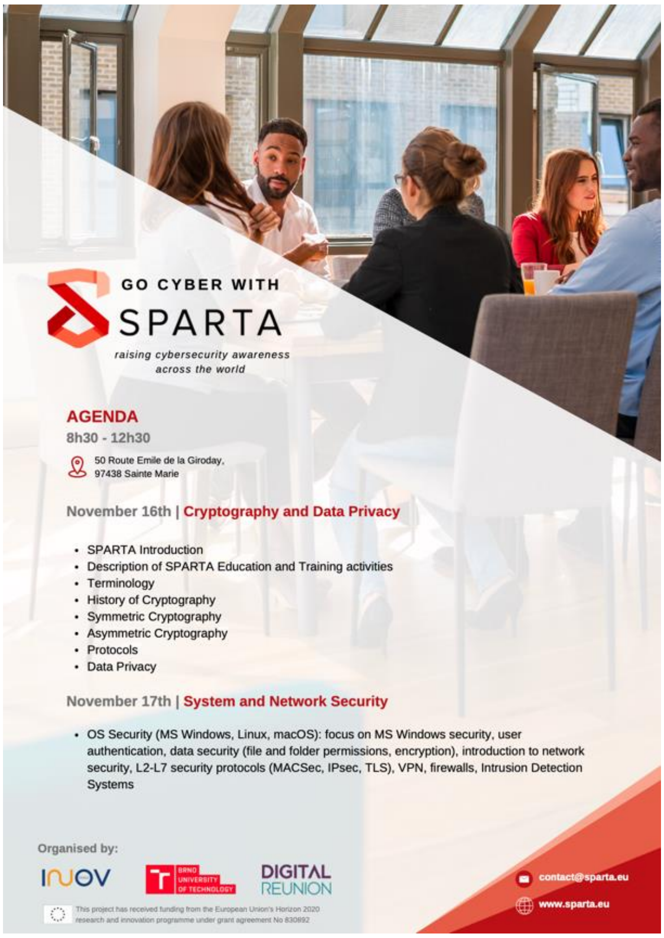
In In total, we were able to gather nine SMEs to attend the two-day workshop through an advertisement campaign promoted by Digital Reunion and INOV – Image 11. To ensure there would not be any constraints regarding the language, Digital Reunion invited a professional for conducting a simultaneous translation during the entire workshop.

The workshop was held on the 16th and 17th of November, from 8h30 to 12h30, at the 50 Route Emile de la Giroday building.

These SMEs filled in a participation form that permitted to assess their relative knowledge in the subjects of the workshop, hence tailoring the information deployed.

The shreds of evidence of this workshop are in images 12 to 14, and the attendees' list is available in Annex 8.

Attempting to maximise the SPARTA outreach and impact, WP9 and WP12 deployed efforts to organise a workshop with the University of La Reunion. The workshop focused on how to create a cybersecurity bachelor or master degree based on existing courses – similar to the one provided in action 2, to the Universidad de Las Palmas de Gran Canara. The University of La Reunion did not have the opportunity to meet with SPARTA as it has been facing some adversities caused by the COVID-19 pandemic.



GO CYBER WITH SPARTA

raising cybersecurity awareness across the world

AGENDA

8h30 - 12h30

50 Route Emile de la Giroday,
97438 Sainte Marie

November 16th | Cryptography and Data Privacy

- SPARTA Introduction
- Description of SPARTA Education and Training activities
- Terminology
- History of Cryptography
- Symmetric Cryptography
- Asymmetric Cryptography
- Protocols
- Data Privacy

November 17th | System and Network Security

- OS Security (MS Windows, Linux, macOS): focus on MS Windows security, user authentication, data security (file and folder permissions, encryption), introduction to network security, L2-L7 security protocols (MACSec, IPsec, TLS), VPN, firewalls, Intrusion Detection Systems

Organised by:

INOV BRNO UNIVERSITY OF TECHNOLOGY DIGITAL REUNION

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892

contact@sparta.eu
www.sparta.eu

Figure 11: Poster for the workshop "Go Cyber with SPARTA" dedicated to the SMEs in the digital sector, from La Reunion

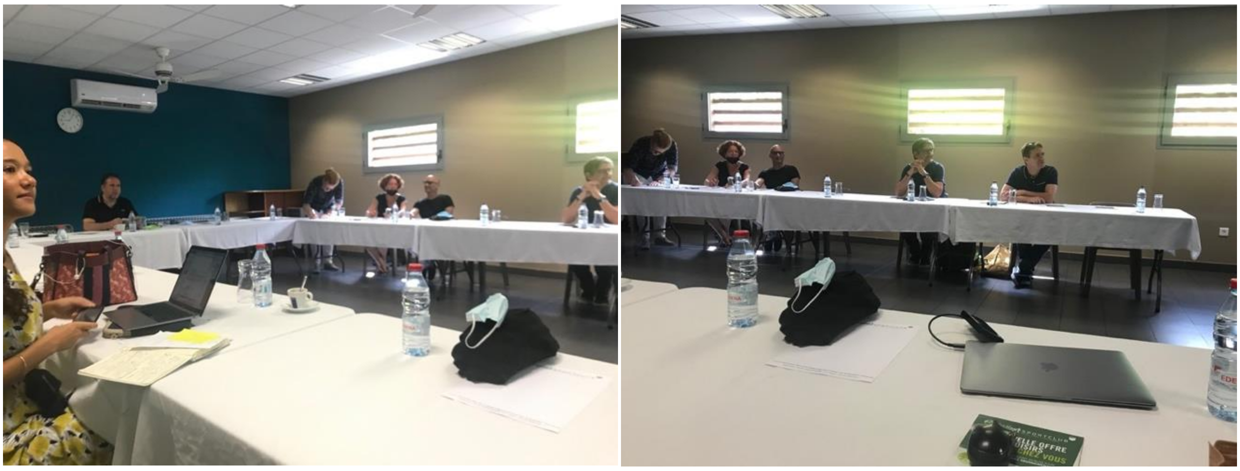


Figure 12: "Go Cyber with SPARTA - La Reunion" workshop with SMEs on the digital sector

Figure 13: Sara Ricci on "Cryptography and Data Privacy" day 1 of thee "Go Cyber with SPARTA - La Reunion" workshop with SMEs on the digital sector

Figure 14: Lukas Malina on "System and Network Security" day 2 of the "Go Cyber with SPARTA - La Reunion" workshop with SMEs on the digital sector

Chapter 4 Evaluation

This chapter provides a general evaluation of the activities carried out during the three years of the SPARTA project in the scope of task 12.5. It strives to provide a set of recommendations for projects wanting to pursue a similar approach. The evaluation follows the same structure as chapter 3: it will consider each action in particular.

4.1 Encourage small businesses to adopt cybersecurity measures

Action 1 – Encourage small businesses to adopt cybersecurity measures – aimed at promoting awareness of the cyber threats and risks that a business can be exposed to, leading to an attitudinal change in what concerns cybersecurity behaviour. Considering the roadblocks encountered during the planning and arrangement of this action – mostly triggered by the impacts caused by the COVID-19 pandemic and, to some extent, the remote location and the time zone differences between the European Continent and the ORs located in the Caribbean – WP12 had to prepare a back-up plan that allowed to achieve the same goals but in a different region. Overall, the action-outcome was positive and the SPARTA project had a direct impact on the cybersecurity training and awareness building of the five Madeira' SMEs that attended the *Go Cyber with SPARTA* workshop. It also had a direct impact on the lessons learned by the students that attended the workshop, whose interest in the subject was keen. Promoting workshops that target raising awareness and knowledge about the threat landscape, human aspects of cybersecurity, social engineering, and management and risk analyses have proven to be welcoming and of utmost interest for the SMEs in the tourism sector. The risk perception promotes cybersecurity attitudes to protect any business whose highly dependent on the well-function and safety of cyberspace and information and communication technologies.

From this action, it was possible to understand the need for anticipating constraints such as the language barrier (translation from English to French was needed for every document that would be provided to the Martinique SMEs), the different and relative perceptions of needs and urgencies over locations and cultures (perhaps the SMEs from Martinique were not foremost concerned about cybersecurity as other issues may have appeared more important) and the uprising of a pandemic, that heavily influenced the natural flow of activities around the globe, delaying commitments and restructuring priorities.

4.2 Stimulate cybersecurity studies or training at university level

Action 2 – Stimulate cybersecurity studies or training at the university level – aimed at providing the necessary means for creating cybersecurity curricula, ensuring that students at the university level have access to education on cybersecurity, a subject of growing critical importance.

Overall, this action achieved its goal as the University of Las Palmas de Gran Canaria showed a keen interest in establishing a Cybersecurity bachelor degree, after the deployment of the workshop provided by WP9 – namely by Jan Hajny and Sara Ricci from the Brno University of Technology and Edmundas Piesarskas, from L3CE.

Moreover, concrete recommendations were provided to the Universidad de Las Palmas de Gran Canaria (ULPGC). An analysis of their current bachelor study program in Computer Engineering was run using the SPARTA curricula designer. This dynamic tool allowed the identification of cybersecurity knowledge that would need to be added to make the curriculum compliant with existing cybersecurity study programs. A specific adaptation of their curriculum was proposed

This action can, in future, be replicated in different European locations and beyond, as it has proven to be efficient and received positive feedback from ULPGC.

4.3 Engage critical infrastructure operators with cybersecurity technology

Action 3 – Engage critical infrastructure operators with cybersecurity technology – aimed at building awareness on the cybersecurity issues of critical infrastructure with the employees of Office de l'eau, the Water Critical Infrastructure of La Reunion. The action had positive feedback and impacted on the will to promote cybersecurity actions: *"It's up to us, at Office de l'eau Réunion, to transform all these new knowledge and information materials into security actions for/towards our employees and stakeholders".*

The resources and efforts of this action were maximised by a second on-site workshop with SMEs on the digital sector from La Reunion, expanding the reach and impact of the SPARTA project. The workshop took place both virtually and physically. Topics included modern cryptography, privacy protection, system security, network security, legal aspects, awareness strategies, industrial security and more. Critical infrastructure body and young digital companies were involved in the training. The workshop was very well perceived and suggestions for follow-up activities were made. Lectures were provided by BUT, IMT, SMILE and covered from their SPARTA budgets. Overall, we received positive feedback from the participants both on the format and on the content. The only issue to report was the retention from registration. Some people who registered for participating in the workshop did not attend any of the days. Claire Alanoix explained that *"one thing that probably played a part was the location I managed to book as it was not super well-known by all and slightly remote"* and suggested that an incentive for people who registered to actually participate would be to provide a *"kind of certificate or label delivered to participants at the end of the sessions, one they can post on their resume or Linkedin".*

4.4 General recommendations

Overall, the lessons learned and/or recommendations for projects wanting to pursue a similar approach and actively engage the ORs with its concepts, aims, values, activities and results are the following:

1. Anticipating constraints is keen for the timely, efficient and effective development of planned activities. Constraints may be related to the language (it may be relevant to translate documents and workshops, and it may help translate the first contact e-mails),
2. Different needs, perceptions and urgencies over locations and cultures call for the active involvement of all the entities in the design of the activities. It also calls for flexibility for changing the action route when needed.
3. Another constraint that we all are more aware of is the uprising of a pandemic that heavily influenced the natural flow of activities around the globe, delaying commitments and restructuring priorities.
4. Resources and efforts should be as maximised as much as possible within a region. Always search for ways to extend the outreach and impact of the project and its activities.
5. Ensuring that all entities involved with the action are fully aware of the planned activities and allowing their active participation in the design and deployment is of utmost importance.
6. A strong, coherent, and ongoing communication is key for sharpened collaborations. All the entities part of the *Go Cyber with SPARTA* campaign receive the monthly internal SPARTA newsletter.
7. If possible, establish cross-collaborations within and beyond the project.
8. Create strategies to ensure that people who register in the workshops do not lose interest and actually attend the workshop. Strategies can involve sending reminder e-mails and/or provide certification or diploma to the attendees after the training.

Strong communication, intercultural sensitivity, flexibility, anticipation and maximising resources are the keywords drawn from three years of experience of the SPARTA project on the engagement of the Outermost Regions of Europe.

Chapter 5 Summary and Conclusion

The present deliverable summarizes all the activities developed in the scope of task 12.5 *Outermost Regions Engagement – "Go Cyber with SPARTA" campaign.* The deliverable also carries an evaluation of such activities, and draws a set of recommendations which are expected to be useful for projects who plan to engage in similar initiatives.

Overall, the activities designed and implemented to create cybersecurity awareness and engage the outermost regions of Europe with the SPARTA project values, goals, activities, and results had a positive outcome and impact. As main results/impacts:

1. The University of Las Palmas de Gran Canaria, Spain, is willing to create a cybersecurity bachelor degree in cybersecurity, in a collaborative effort with SPARTA, after the deployment of the workshop provided by WP9 on how to use the SPARTA Cybersecurity Curricula Designer and the Cybersecurity Education Map;
2. Office de l'eau is committed to delivering their employees the knowledge received during the one-week cybersecurity training and awareness workshop delivered to the IT team;
3. Ten SMEs in the digital sector, based in La Reunion, France, have received a two-day cybersecurity training and awareness workshop;
4. Five SMEs in the tourism sector, based in Madeira, Portugal, have received a cybersecurity training and awareness workshop, tailored to their informational needs. Some university students also attended the event.

These activities relied on ongoing and strong collaborations between WP1, WP9 and WP12, essential for deploying these activities.

Chapter 6 List of Abbreviations

Abbreviation	Translation
C&D	Communication and Dissemination
OR’s	Outermost Regions of Europe
CCN	Cyber Competence Network

Chapter 7 Bibliography

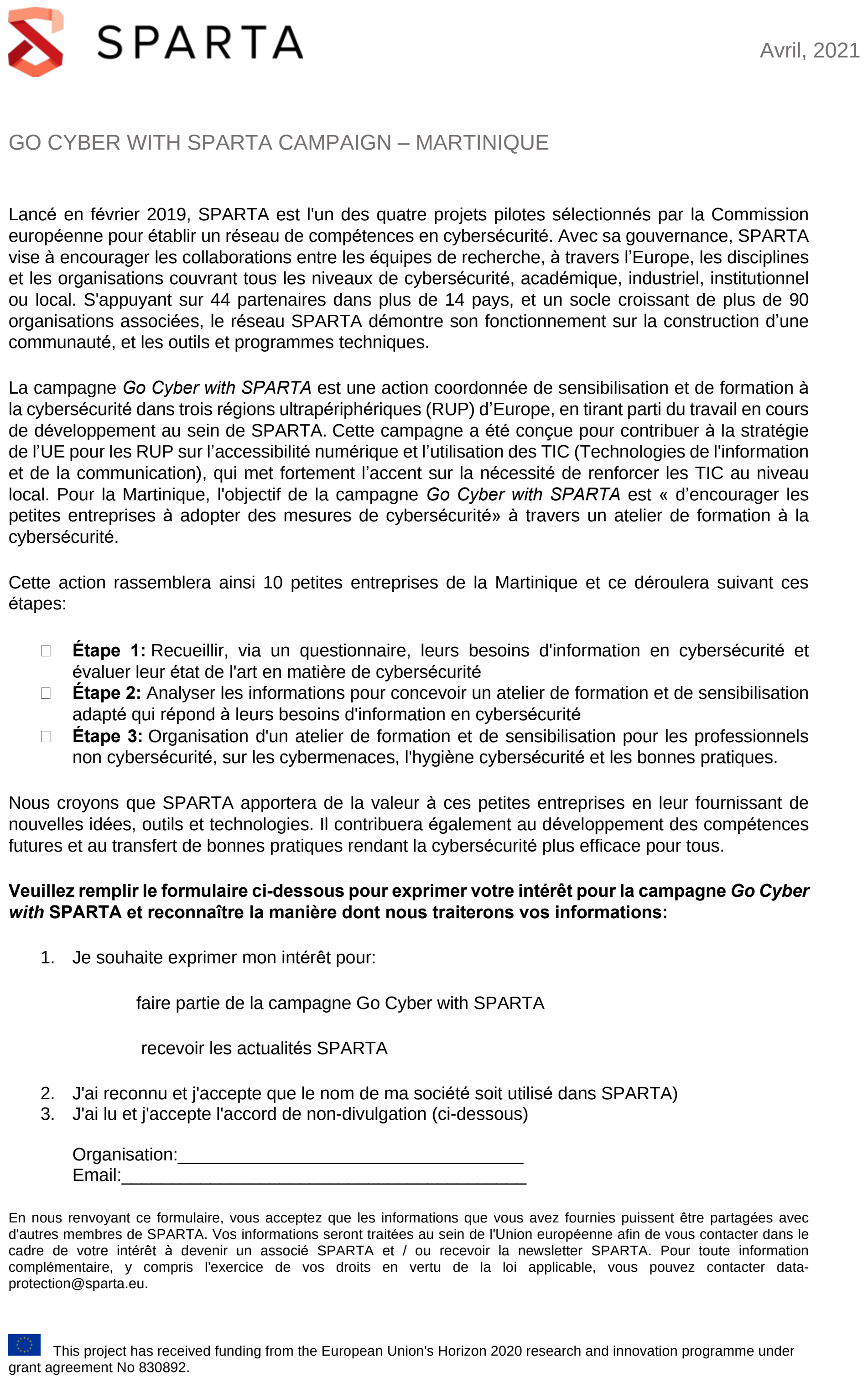
Baudouin, P., 2017. *FINAL REPORT ON DIGITAL ACCESSIBILITY AND ICT (COVERAGE AND USE) FOR THE OUTERMOST REGIONS*. REPORT ON DIGITAL ACCESSIBILITY AND ICT. [online] European Commission. Available at: <https://ec.europa.eu/regional_policy/sources/policy/themes/outermost-regions/pdf/ict_report_en.pdf>

Ec.europa.eu. 2021. *EU & outermost regions*. [online] Available at: <https://ec.europa.eu/regional_policy/index.cfm/en/policy/themes/outermost-regions/>

Monfret, A., 2017. *THE OUTERMOST REGIONS - EUROPEAN LANDS IN THE WORLD*. [ebook] European Union. Available at: <http://ec.europa.eu/regional_policy/sources/policy/themes/outermost-regions/pdf/rup_2017/rup_eu_lands_world_en.pdf>

Chapter 8 Annexes

8.1 Annex 1 – Invitation for Go Cyber with SPARTA – Martinique



SPARTA

Avril, 2021

GO CYBER WITH SPARTA CAMPAIGN – MARTINIQUE

Lancé en février 2019, SPARTA est l'un des quatre projets pilotes sélectionnés par la Commission européenne pour établir un réseau de compétences en cybersécurité. Avec sa gouvernance, SPARTA vise à encourager les collaborations entre les équipes de recherche, à travers l'Europe, les disciplines et les organisations couvrant tous les niveaux de cybersécurité, académique, industriel, institutionnel ou local. S'appuyant sur 44 partenaires dans plus de 14 pays, et un socle croissant de plus de 90 organisations associées, le réseau SPARTA démontre son fonctionnement sur la construction d'une communauté, et les outils et programmes techniques.

La campagne *Go Cyber with SPARTA* est une action coordonnée de sensibilisation et de formation à la cybersécurité dans trois régions ultrapériphériques (RUP) d'Europe, en tirant parti du travail en cours de développement au sein de SPARTA. Cette campagne a été conçue pour contribuer à la stratégie de l'UE pour les RUP sur l'accessibilité numérique et l'utilisation des TIC (Technologies de l'information et de la communication), qui met fortement l'accent sur la nécessité de renforcer les TIC au niveau local. Pour la Martinique, l'objectif de la campagne *Go Cyber with SPARTA* est « d'encourager les petites entreprises à adopter des mesures de cybersécurité» à travers un atelier de formation à la cybersécurité.

Cette action rassemblera ainsi 10 petites entreprises de la Martinique et ce déroulera suivant ces étapes:

□ **Étape 1:** Recueillir, via un questionnaire, leurs besoins d'information en cybersécurité et évaluer leur état de l'art en matière de cybersécurité
□ **Étape 2:** Analyser les informations pour concevoir un atelier de formation et de sensibilisation adapté qui répond à leurs besoins d'information en cybersécurité
□ **Étape 3:** Organisation d'un atelier de formation et de sensibilisation pour les professionnels non cybersécurité, sur les cybermenaces, l'hygiène cybersécurité et les bonnes pratiques.

Nous croyons que SPARTA apportera de la valeur à ces petites entreprises en leur fournissant de nouvelles idées, outils et technologies. Il contribuera également au développement des compétences futures et au transfert de bonnes pratiques rendant la cybersécurité plus efficace pour tous.

Veuillez remplir le formulaire ci-dessous pour exprimer votre intérêt pour la campagne *Go Cyber with* SPARTA et reconnaître la manière dont nous traiterons vos informations:

1. Je souhaite exprimer mon intérêt pour:

   faire partie de la campagne Go Cyber with SPARTA

   recevoir les actualités SPARTA

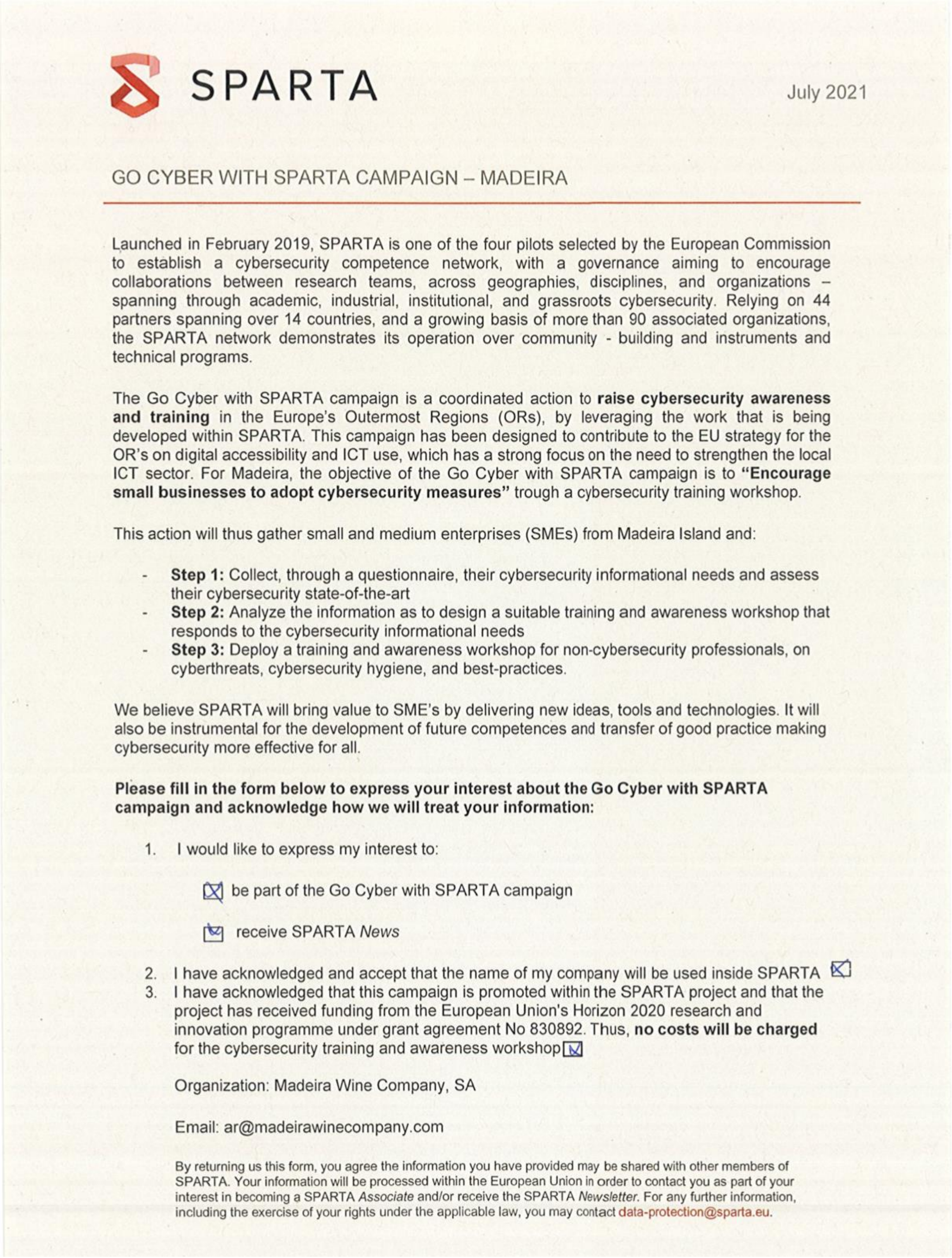
2. J'ai reconnu et j'accepte que le nom de ma société soit utilisé dans SPARTA)
3. J'ai lu et j'accepte l'accord de non-divulgation (ci-dessous)

   Organisation:___________________________________
   Email:____

En nous renvoyant ce formulaire, vous acceptez que les informations que vous avez fournies puissent être partagées avec d'autres membres de SPARTA. Vos informations seront traitées au sein de l'Union européenne afin de vous contacter dans le cadre de votre intérêt à devenir un associé SPARTA et / ou recevoir la newsletter SPARTA. Pour toute information complémentaire, y compris l'exercice de vos droits en vertu de la loi applicable, vous pouvez contacter data-protection@sparta.eu.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892.

8.2 Annex 2 – Invitations signed for Go Cyber with SPARTA – Madeira



SPARTA

July 2021

GO CYBER WITH SPARTA CAMPAIGN – MADEIRA

Launched in February 2019, SPARTA is one of the four pilots selected by the European Commission to establish a cybersecurity competence network, with a governance aiming to encourage collaborations between research teams, across geographies, disciplines, and organizations – spanning through academic, industrial, institutional, and grassroots cybersecurity. Relying on 44 partners spanning over 14 countries, and a growing basis of more than 90 associated organizations, the SPARTA network demonstrates its operation over community - building and instruments and technical programs.

The Go Cyber with SPARTA campaign is a coordinated action to **raise cybersecurity awareness and training** in the Europe's Outermost Regions (ORs), by leveraging the work that is being developed within SPARTA. This campaign has been designed to contribute to the EU strategy for the OR's on digital accessibility and ICT use, which has a strong focus on the need to strengthen the local ICT sector. For Madeira, the objective of the Go Cyber with SPARTA campaign is to **"Encourage small businesses to adopt cybersecurity measures"** trough a cybersecurity training workshop.

This action will thus gather small and medium enterprises (SMEs) from Madeira Island and:

- **Step 1:** Collect, through a questionnaire, their cybersecurity informational needs and assess their cybersecurity state-of-the-art
- **Step 2:** Analyze the information as to design a suitable training and awareness workshop that responds to the cybersecurity informational needs
- **Step 3:** Deploy a training and awareness workshop for non-cybersecurity professionals, on cyberthreats, cybersecurity hygiene, and best-practices.

We believe SPARTA will bring value to SME's by delivering new ideas, tools and technologies. It will also be instrumental for the development of future competences and transfer of good practice making cybersecurity more effective for all.

Please fill in the form below to express your interest about the Go Cyber with SPARTA campaign and acknowledge how we will treat your information:

1. I would like to express my interest to:

   ☒ be part of the Go Cyber with SPARTA campaign

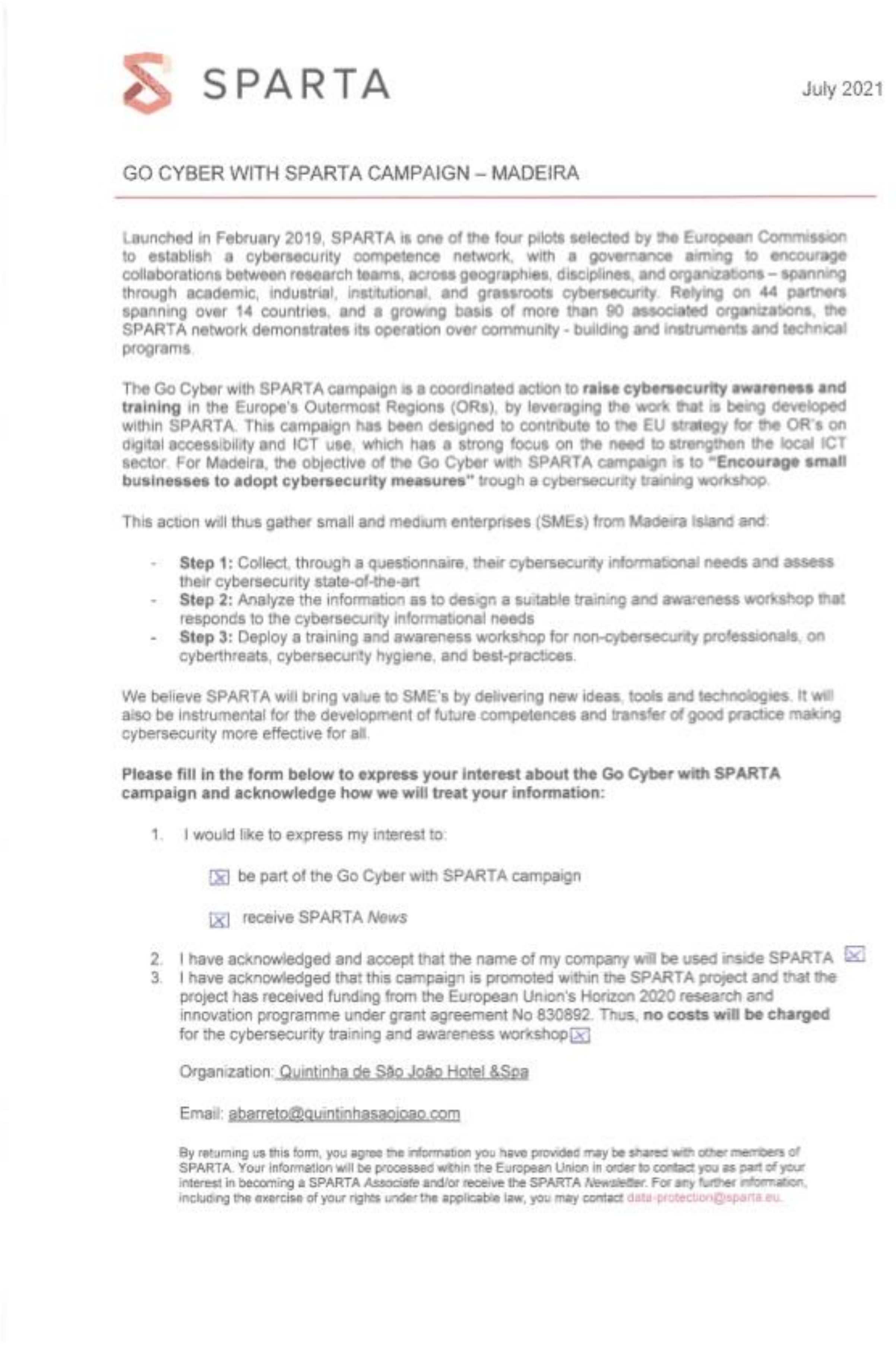
   ☑ receive SPARTA *News*

2. I have acknowledged and accept that the name of my company will be used inside SPARTA ☒
3. I have acknowledged that this campaign is promoted within the SPARTA project and that the project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892. Thus, **no costs will be charged** for the cybersecurity training and awareness workshop ☑

Organization: Madeira Wine Company, SA

Email: ar@madeirawinecompany.com

By returning us this form, you agree the information you have provided may be shared with other members of SPARTA. Your information will be processed within the European Union in order to contact you as part of your interest in becoming a SPARTA *Associate* and/or receive the SPARTA *Newsletter*. For any further information, including the exercise of your rights under the applicable law, you may contact data-protection@sparta.eu.



SPARTA

July 2021

GO CYBER WITH SPARTA CAMPAIGN – MADEIRA

Launched in February 2019, SPARTA is one of the four pilots selected by the European Commission to establish a cybersecurity competence network, with a governance aiming to encourage collaborations between research teams, across geographies, disciplines, and organizations – spanning through academic, industrial, institutional, and grassroots cybersecurity. Relying on 44 partners spanning over 14 countries, and a growing basis of more than 90 associated organizations, the SPARTA network demonstrates its operation over community - building and instruments and technical programs.

The Go Cyber with SPARTA campaign is a coordinated action to **raise cybersecurity awareness and training** in the Europe's Outermost Regions (ORs), by leveraging the work that is being developed within SPARTA. This campaign has been designed to contribute to the EU strategy for the OR's on digital accessibility and ICT use, which has a strong focus on the need to strengthen the local ICT sector. For Madeira, the objective of the Go Cyber with SPARTA campaign is to **"Encourage small businesses to adopt cybersecurity measures"** trough a cybersecurity training workshop.

This action will thus gather small and medium enterprises (SMEs) from Madeira Island and:

- **Step 1:** Collect, through a questionnaire, their cybersecurity informational needs and assess their cybersecurity state-of-the-art
- **Step 2:** Analyze the information as to design a suitable training and awareness workshop that responds to the cybersecurity informational needs
- **Step 3:** Deploy a training and awareness workshop for non-cybersecurity professionals, on cyberthreats, cybersecurity hygiene, and best-practices.

We believe SPARTA will bring value to SME's by delivering new ideas, tools and technologies. It will also be instrumental for the development of future competences and transfer of good practice making cybersecurity more effective for all.

Please fill in the form below to express your interest about the Go Cyber with SPARTA campaign and acknowledge how we will treat your information:

1. I would like to express my interest to:

   ☒ be part of the Go Cyber with SPARTA campaign

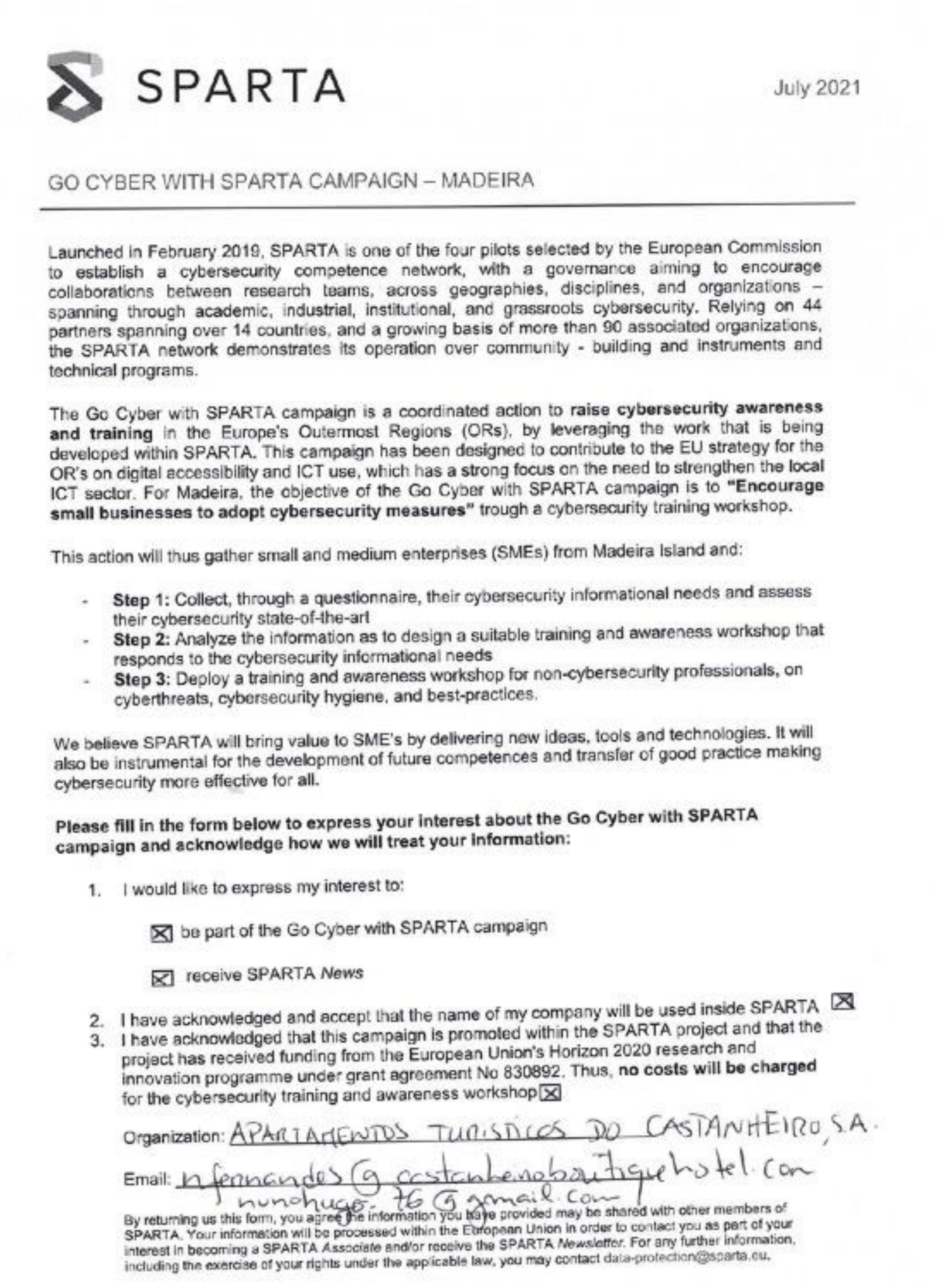
   ☒ receive SPARTA *News*

2. I have acknowledged and accept that the name of my company will be used inside SPARTA ☒
3. I have acknowledged that this campaign is promoted within the SPARTA project and that the project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892. Thus, **no costs will be charged** for the cybersecurity training and awareness workshop ☒

Organization: Quintinha de São João Hotel &Spa

Email: abarreto@quintinhasaojoao.com

By returning us this form, you agree the information you have provided may be shared with other members of SPARTA. Your information will be processed within the European Union in order to contact you as part of your interest in becoming a SPARTA Associate and/or receive the SPARTA *Newsletter*. For any further information, including the exercise of your rights under the applicable law, you may contact data-protection@sparta.eu.



SPARTA

July 2021

GO CYBER WITH SPARTA CAMPAIGN – MADEIRA

Launched in February 2019, SPARTA is one of the four pilots selected by the European Commission to establish a cybersecurity competence network, with a governance aiming to encourage collaborations between research teams, across geographies, disciplines, and organizations – spanning through academic, industrial, institutional, and grassroots cybersecurity. Relying on 44 partners spanning over 14 countries, and a growing basis of more than 90 associated organizations, the SPARTA network demonstrates its operation over community - building and instruments and technical programs.

The Go Cyber with SPARTA campaign is a coordinated action to **raise cybersecurity awareness and training** in the Europe's Outermost Regions (ORs), by leveraging the work that is being developed within SPARTA. This campaign has been designed to contribute to the EU strategy for the OR's on digital accessibility and ICT use, which has a strong focus on the need to strengthen the local ICT sector. For Madeira, the objective of the Go Cyber with SPARTA campaign is to **"Encourage small businesses to adopt cybersecurity measures"** trough a cybersecurity training workshop.

This action will thus gather small and medium enterprises (SMEs) from Madeira Island and:

- **Step 1:** Collect, through a questionnaire, their cybersecurity informational needs and assess their cybersecurity state-of-the-art
- **Step 2:** Analyze the information as to design a suitable training and awareness workshop that responds to the cybersecurity informational needs
- **Step 3:** Deploy a training and awareness workshop for non-cybersecurity professionals, on cyberthreats, cybersecurity hygiene, and best-practices.

We believe SPARTA will bring value to SME's by delivering new ideas, tools and technologies. It will also be instrumental for the development of future competences and transfer of good practice making cybersecurity more effective for all.

Please fill in the form below to express your interest about the Go Cyber with SPARTA campaign and acknowledge how we will treat your information:

1. I would like to express my interest to:

   ☒ be part of the Go Cyber with SPARTA campaign

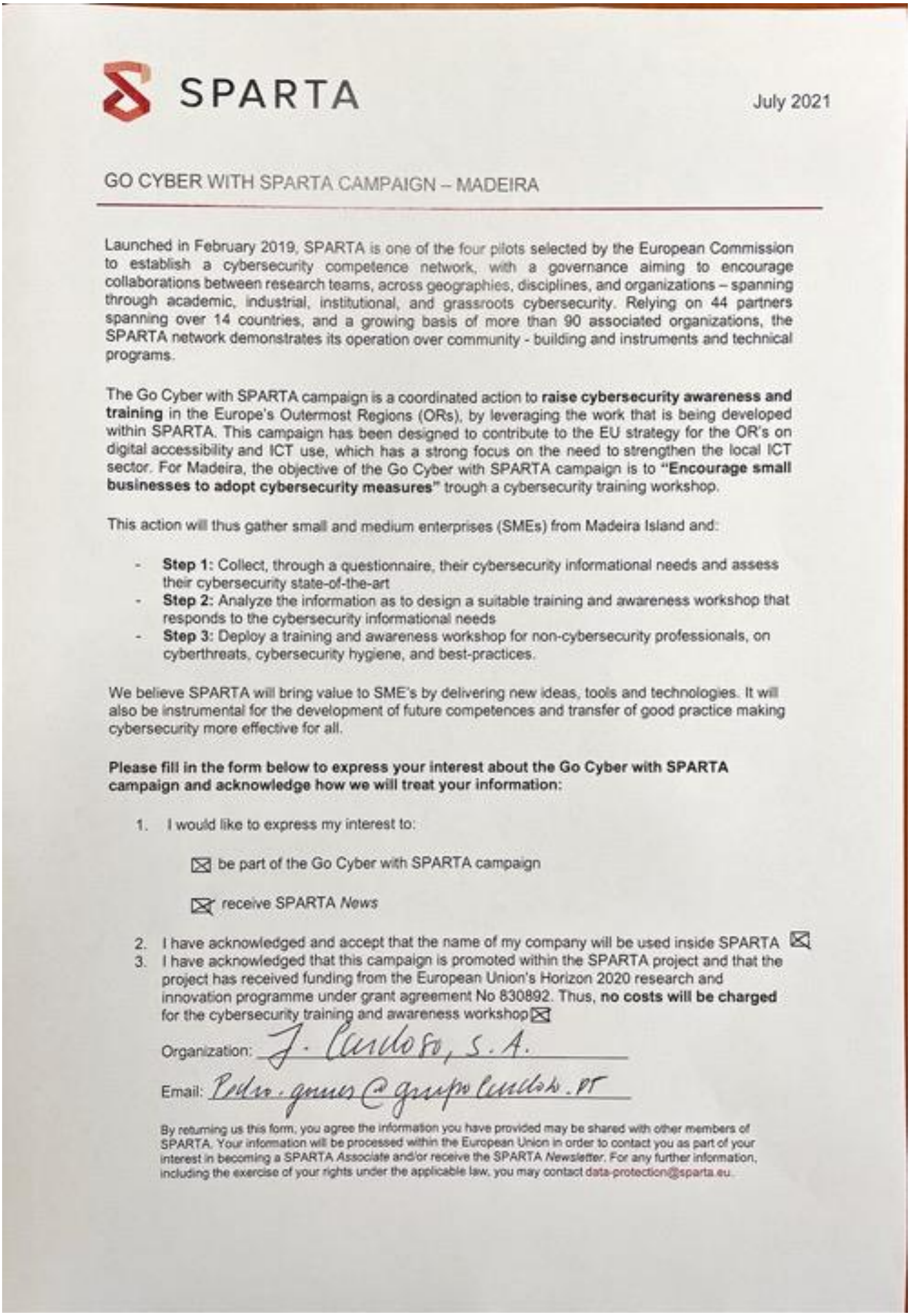
   ☒ receive SPARTA *News*

2. I have acknowledged and accept that the name of my company will be used inside SPARTA ☒
3. I have acknowledged that this campaign is promoted within the SPARTA project and that the project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892. Thus, **no costs will be charged** for the cybersecurity training and awareness workshop ☒

Organization: APARTAMENTOS TURISTICOS DO CASTANHEIRO, S.A.

Email: nfernandes@castanheiroboutiquehotel.com
nunohugo.76@gmail.com

By returning us this form, you agree the information you have provided may be shared with other members of SPARTA. Your information will be processed within the European Union in order to contact you as part of your interest in becoming a SPARTA *Associate* and/or receive the SPARTA *Newsletter*. For any further information, including the exercise of your rights under the applicable law, you may contact data-protection@sparta.eu.



SPARTA

July 2021

GO CYBER WITH SPARTA CAMPAIGN – MADEIRA

Launched in February 2019, SPARTA is one of the four pilots selected by the European Commission to establish a cybersecurity competence network, with a governance aiming to encourage collaborations between research teams, across geographies, disciplines, and organizations – spanning through academic, industrial, institutional, and grassroots cybersecurity. Relying on 44 partners spanning over 14 countries, and a growing basis of more than 90 associated organizations, the SPARTA network demonstrates its operation over community - building and instruments and technical programs.

The Go Cyber with SPARTA campaign is a coordinated action to **raise cybersecurity awareness and training** in the Europe's Outermost Regions (ORs), by leveraging the work that is being developed within SPARTA. This campaign has been designed to contribute to the EU strategy for the OR's on digital accessibility and ICT use, which has a strong focus on the need to strengthen the local ICT sector. For Madeira, the objective of the Go Cyber with SPARTA campaign is to **"Encourage small businesses to adopt cybersecurity measures"** trough a cybersecurity training workshop.

This action will thus gather small and medium enterprises (SMEs) from Madeira Island and:

- **Step 1:** Collect, through a questionnaire, their cybersecurity informational needs and assess their cybersecurity state-of-the-art
- **Step 2:** Analyze the information as to design a suitable training and awareness workshop that responds to the cybersecurity informational needs
- **Step 3:** Deploy a training and awareness workshop for non-cybersecurity professionals, on cyberthreats, cybersecurity hygiene, and best-practices.

We believe SPARTA will bring value to SME's by delivering new ideas, tools and technologies. It will also be instrumental for the development of future competences and transfer of good practice making cybersecurity more effective for all.

Please fill in the form below to express your interest about the Go Cyber with SPARTA campaign and acknowledge how we will treat your information:

1. I would like to express my interest to:

   ☒ be part of the Go Cyber with SPARTA campaign

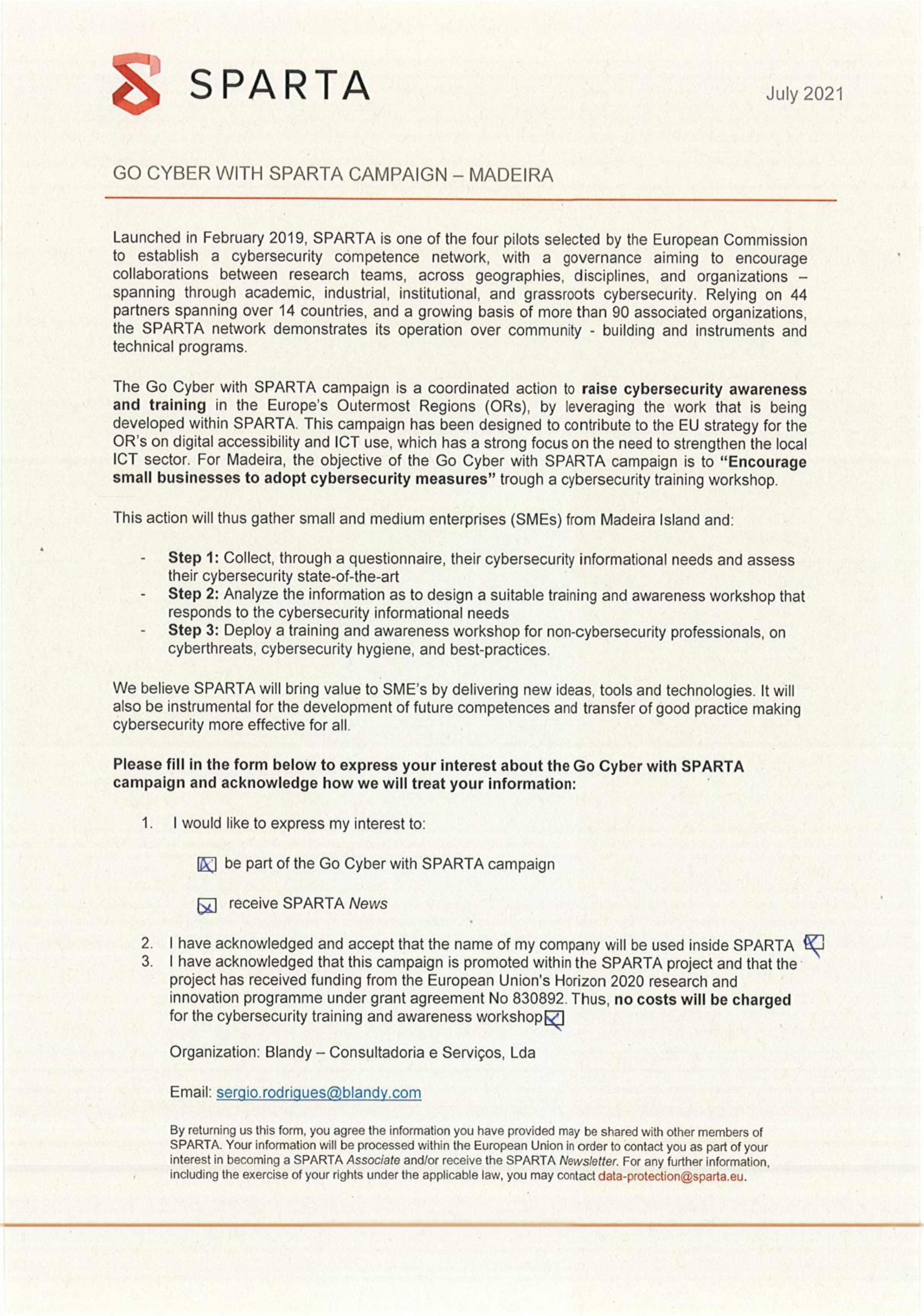
   ☒ receive SPARTA *News*

2. I have acknowledged and accept that the name of my company will be used inside SPARTA ☒
3. I have acknowledged that this campaign is promoted within the SPARTA project and that the project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892. Thus, **no costs will be charged** for the cybersecurity training and awareness workshop ☒

Organization: J. Cardoso, S.A.

Email: Pedro.gomes@grupocardoso.PT

By returning us this form, you agree the information you have provided may be shared with other members of SPARTA. Your information will be processed within the European Union in order to contact you as part of your interest in becoming a SPARTA *Associate* and/or receive the SPARTA *Newsletter*. For any further information, including the exercise of your rights under the applicable law, you may contact data-protection@sparta.eu



SPARTA

July 2021

GO CYBER WITH SPARTA CAMPAIGN – MADEIRA

Launched in February 2019, SPARTA is one of the four pilots selected by the European Commission to establish a cybersecurity competence network, with a governance aiming to encourage collaborations between research teams, across geographies, disciplines, and organizations – spanning through academic, industrial, institutional, and grassroots cybersecurity. Relying on 44 partners spanning over 14 countries, and a growing basis of more than 90 associated organizations, the SPARTA network demonstrates its operation over community - building and instruments and technical programs.

The Go Cyber with SPARTA campaign is a coordinated action to **raise cybersecurity awareness and training** in the Europe's Outermost Regions (ORs), by leveraging the work that is being developed within SPARTA. This campaign has been designed to contribute to the EU strategy for the OR's on digital accessibility and ICT use, which has a strong focus on the need to strengthen the local ICT sector. For Madeira, the objective of the Go Cyber with SPARTA campaign is to **"Encourage small businesses to adopt cybersecurity measures"** trough a cybersecurity training workshop.

This action will thus gather small and medium enterprises (SMEs) from Madeira Island and:

- **Step 1:** Collect, through a questionnaire, their cybersecurity informational needs and assess their cybersecurity state-of-the-art
- **Step 2:** Analyze the information as to design a suitable training and awareness workshop that responds to the cybersecurity informational needs
- **Step 3:** Deploy a training and awareness workshop for non-cybersecurity professionals, on cyberthreats, cybersecurity hygiene, and best-practices.

We believe SPARTA will bring value to SME's by delivering new ideas, tools and technologies. It will also be instrumental for the development of future competences and transfer of good practice making cybersecurity more effective for all.

Please fill in the form below to express your interest about the Go Cyber with SPARTA campaign and acknowledge how we will treat your information:

1. I would like to express my interest to:

   ☒ be part of the Go Cyber with SPARTA campaign

   ☒ receive SPARTA *News*

2. I have acknowledged and accept that the name of my company will be used inside SPARTA ☑
3. I have acknowledged that this campaign is promoted within the SPARTA project and that the project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892. Thus, **no costs will be charged** for the cybersecurity training and awareness workshop ☑

Organization: Blandy – Consultadoria e Serviços, Lda

Email: sergio.rodrigues@blandy.com

By returning us this form, you agree the information you have provided may be shared with other members of SPARTA. Your information will be processed within the European Union in order to contact you as part of your interest in becoming a SPARTA *Associate* and/or receive the SPARTA *Newsletter*. For any further information, including the exercise of your rights under the applicable law, you may contact data-protection@sparta.eu.

8.3 Annex 3 – “Go Cyber with SPARTA - Madeira” brochure

GO CYBER WITH SPARTA

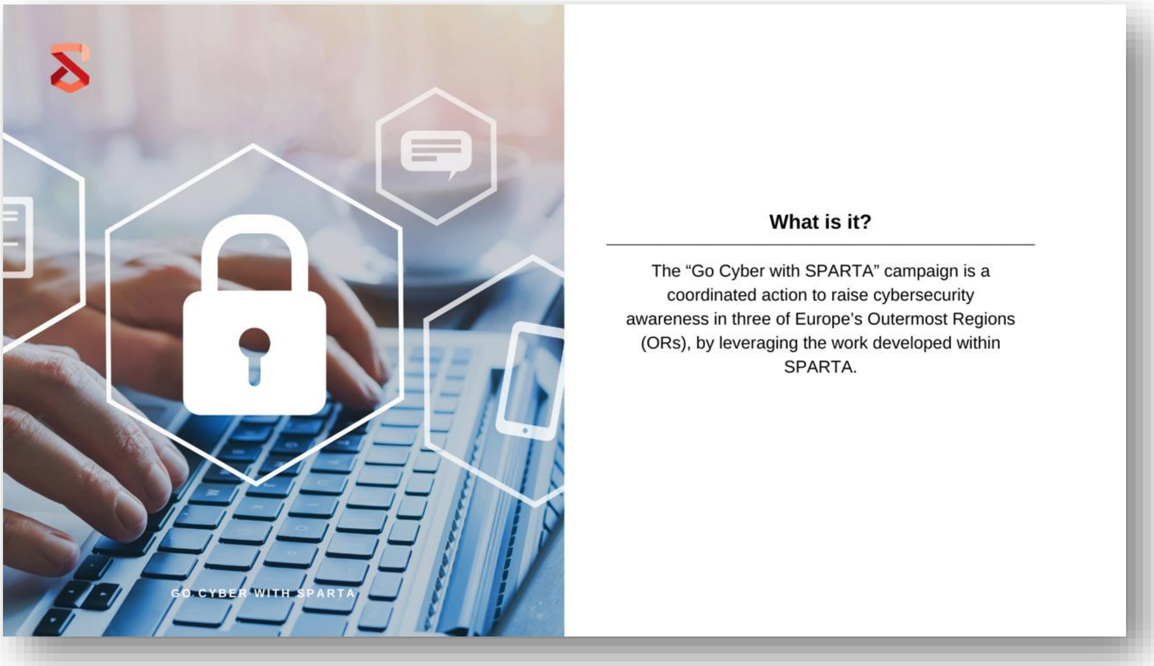
raising cybersecurity awareness across the world

CONTACT

contact@sparta.eu

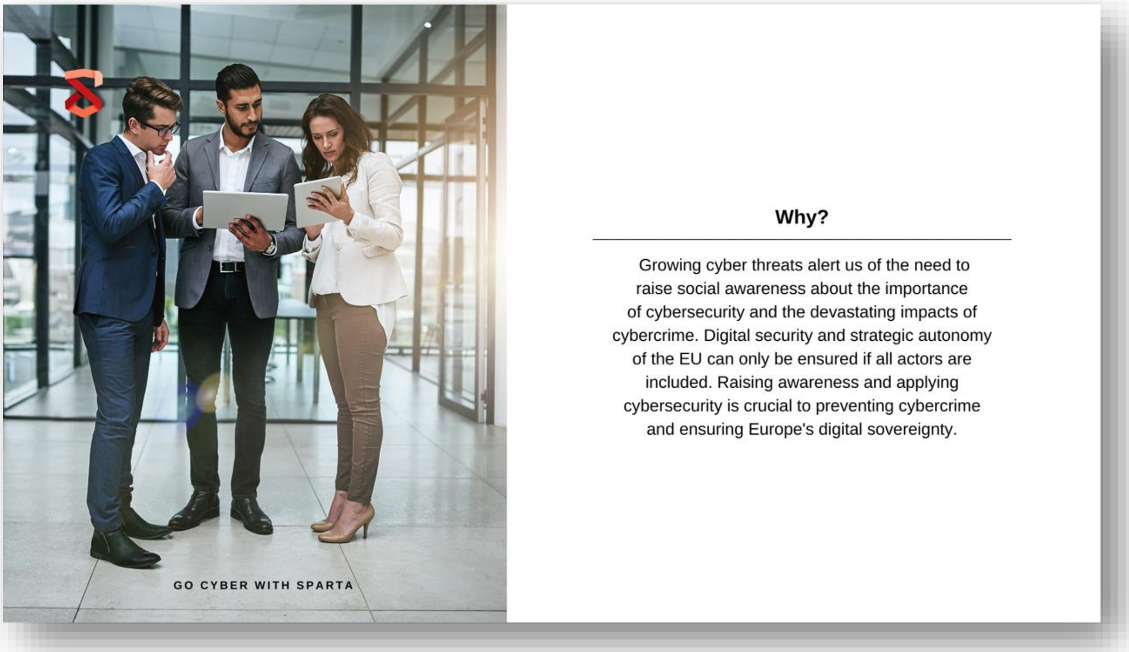
www.sparta.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892



What is it?

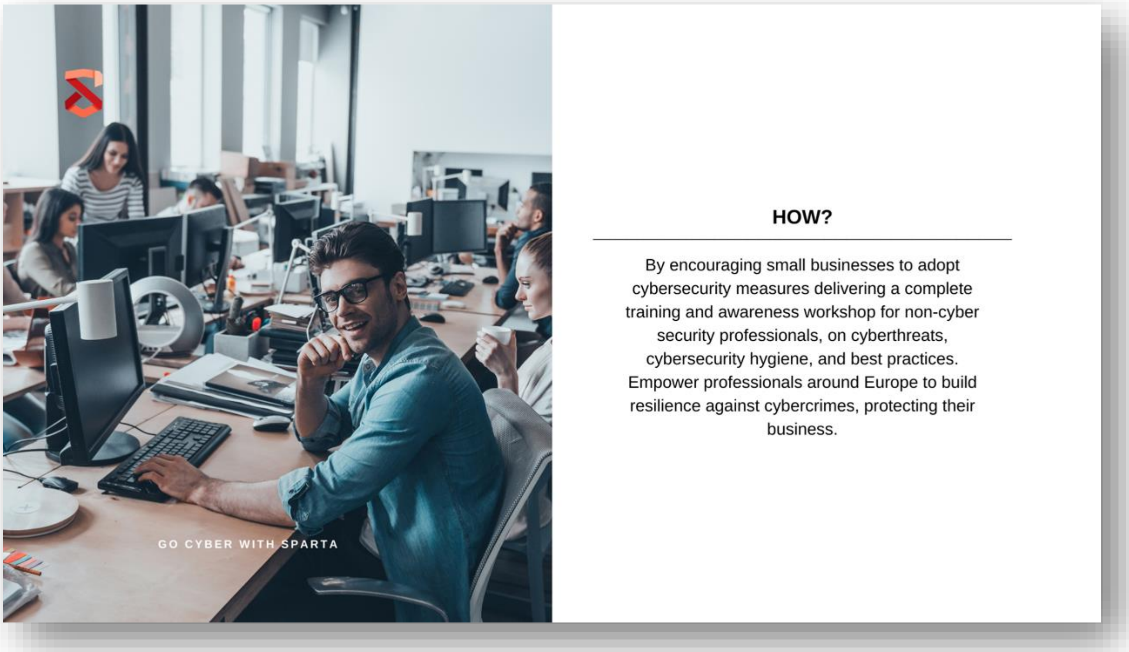
The “Go Cyber with SPARTA” campaign is a coordinated action to raise cybersecurity awareness in three of Europe’s Outermost Regions (ORs), by leveraging the work developed within SPARTA.



GO CYBER WITH SPARTA

Why?

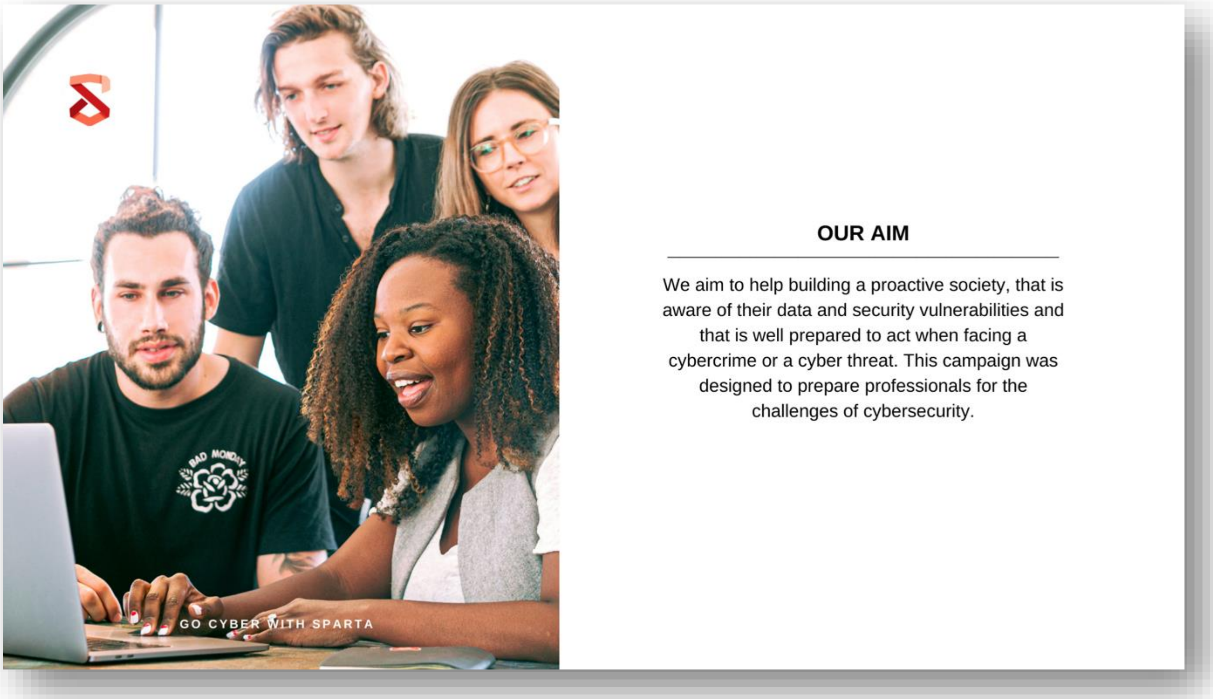
Growing cyber threats alert us of the need to raise social awareness about the importance of cybersecurity and the devastating impacts of cybercrime. Digital security and strategic autonomy of the EU can only be ensured if all actors are included. Raising awareness and applying cybersecurity is crucial to preventing cybercrime and ensuring Europe's digital sovereignty.



GO CYBER WITH SPARTA

HOW?

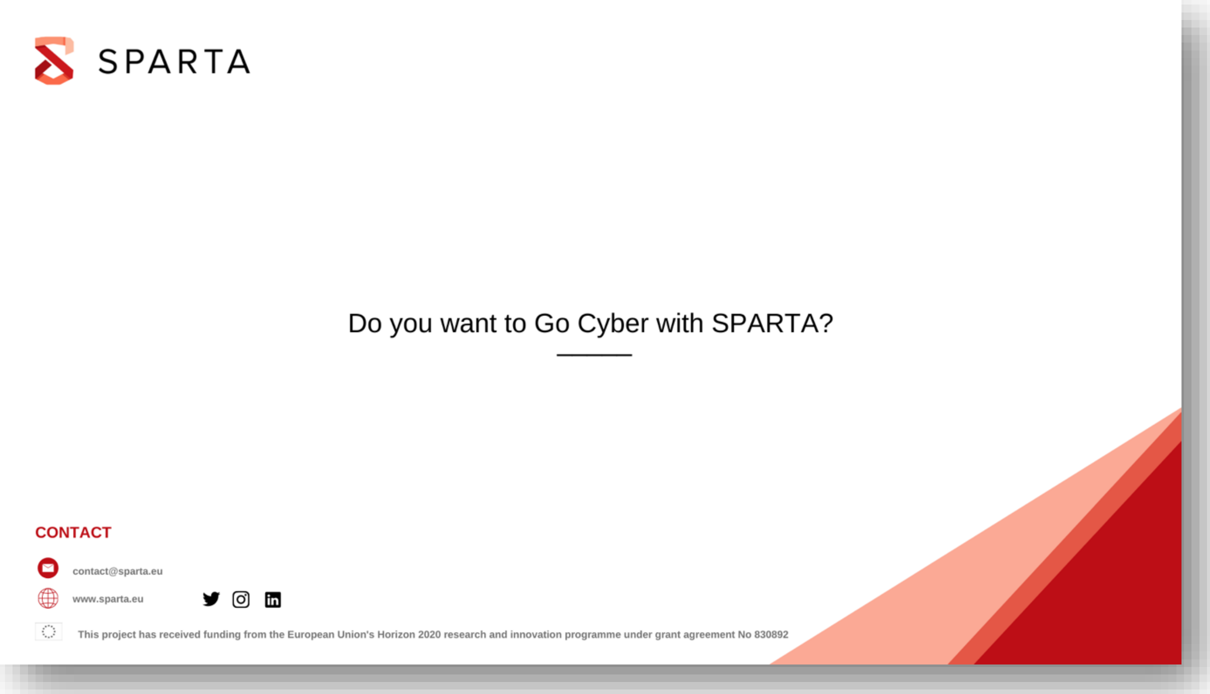
By encouraging small businesses to adopt cybersecurity measures delivering a complete training and awareness workshop for non-cyber security professionals, on cyberthreats, cybersecurity hygiene, and best practices. Empower professionals around Europe to build resilience against cybercrimes, protecting their business.



GO CYBER WITH SPARTA

OUR AIM

We aim to help building a proactive society, that is aware of their data and security vulnerabilities and that is well prepared to act when facing a cybercrime or a cyber threat. This campaign was designed to prepare professionals for the challenges of cybersecurity.



SPARTA

Do you want to Go Cyber with SPARTA?

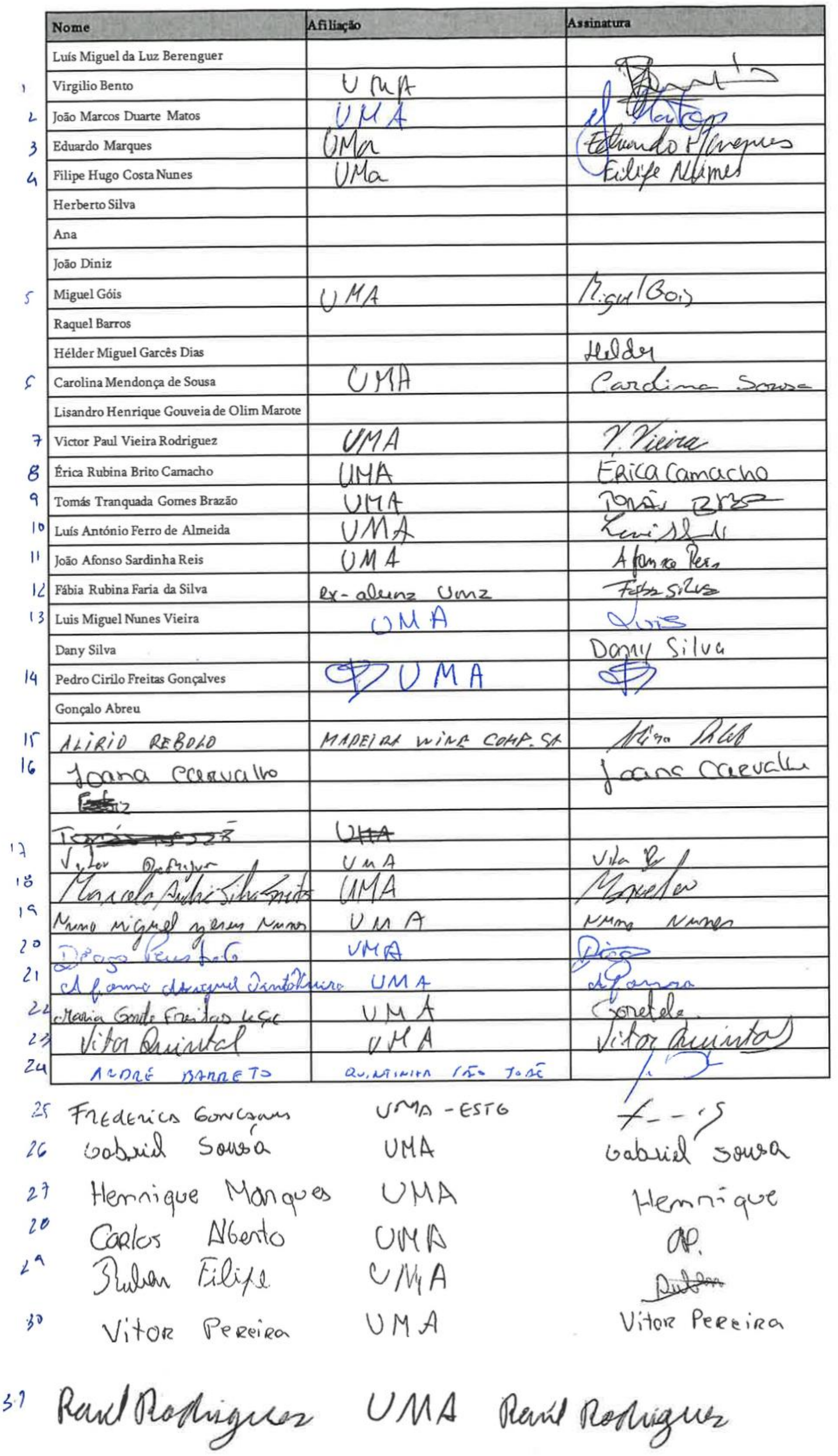
CONTACT

contact@sparta.eu

www.sparta.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892

8.4 Annex 4 – List of attendees for the Go Cyber with SPARTA workshop at Madeira



	Nome	Afiliação	Assinatura
	Luís Miguel da Luz Berenguer		
1	Virgilio Bento	UMA	
2	João Marcos Duarte Matos	UMA	Matos
3	Eduardo Marques	UMa	Eduardo Marques
4	Filipe Hugo Costa Nunes	UMa	Filipe Nunes
	Herberto Silva		
	Ana		
	João Diniz		
5	Miguel Góis	UMA	Miguel Gois
	Raquel Barros		
	Hélder Miguel Garcês Dias		Helder
6	Carolina Mendonça de Sousa	UMA	Carolina Sousa
	Lisandro Henrique Gouveia de Olim Marote		
7	Victor Paul Vieira Rodriguez	UMA	V. Vieira
8	Érica Rubina Brito Camacho	UMA	ÉRica Camacho
9	Tomás Tranquada Gomes Brazão	UMA	Tomás Brazão
10	Luís António Ferro de Almeida	UMA	
11	João Afonso Sardinha Reis	UMA	Afonso Reis
12	Fábia Rubina Faria da Silva	ex-aluna Uma	Fábia Silva
13	Luis Miguel Nunes Vieira	UMA	Luis
	Dany Silva		Dany Silva
14	Pedro Cirilo Freitas Gonçalves	UMA	
	Gonçalo Abreu		
15	ALIRIO REBOLO	MADEIRA WINE COMP. SA	Alírio Rebolo
16	Joana Carvalho		Joana Carvalho
	~~[illegible]~~		
	~~Tomás Brazão~~	~~UMA~~	
17	[illegible]	UMA	[illegible]
18	Marcelo André Silva [illegible]	UMA	Marcelo
19	Nuno Miguel Gomes Nunes	UMA	Nuno Nunes
20	Diogo [illegible]	UMA	Diogo
21	Afonso Miguel Pinto Ribeiro	UMA	Afonso
22	Maria [illegible] Freitas [illegible]	UMA	[illegible]
23	Vitor Quintal	UMA	Vitor Quintal
24	ANDRÉ BARRETO	QUINTINHA SÃO JOSÉ	
25	Frederica Gonçalves	UMA - ESTG	
26	Gabriel Sousa	UMA	Gabriel Sousa
27	Henrique Marques	UMA	Henrique
28	Carlos Alberto	UMA	AP.
29	Julian Filipe	UMA	
30	Vitor Pereira	UMA	Vitor Pereira
31	Raul Rodrigues	UMA	Raul Rodrigues

8.5 Annex 5 – Cybersecurity for Water Critical infrastructures best-practices guide

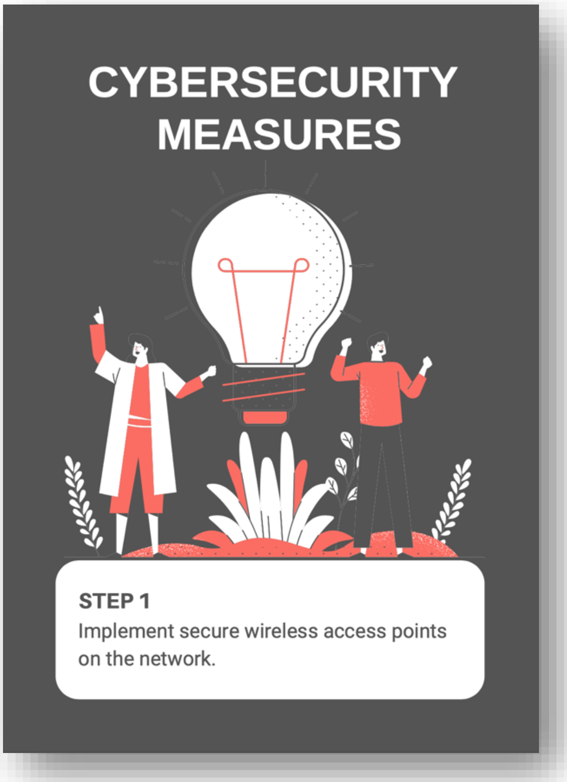
CYBERSECURITY

for Water Critical Infrastructures

CYBER THREATS

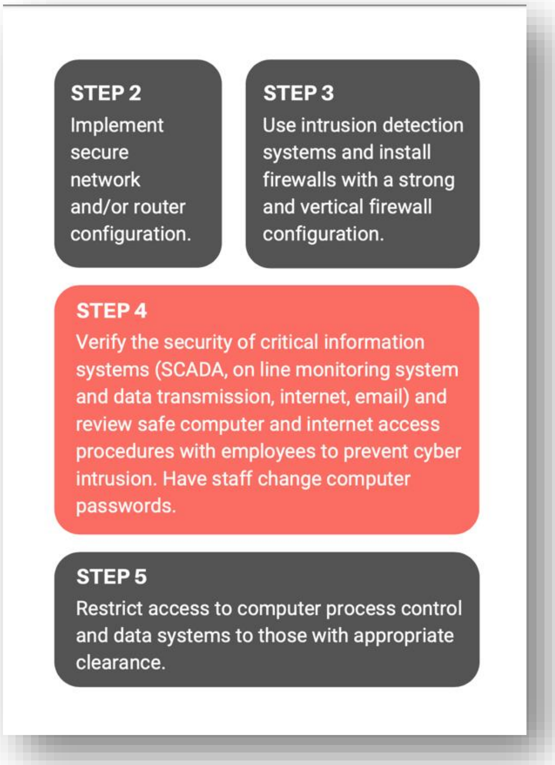
Unauthorised access to the control software system

Packet access to the network segments hosting SCADA devices and one's ability to control or interrupt critical operation



CYBERSECURITY MEASURES

STEP 1
Implement secure wireless access points on the network.

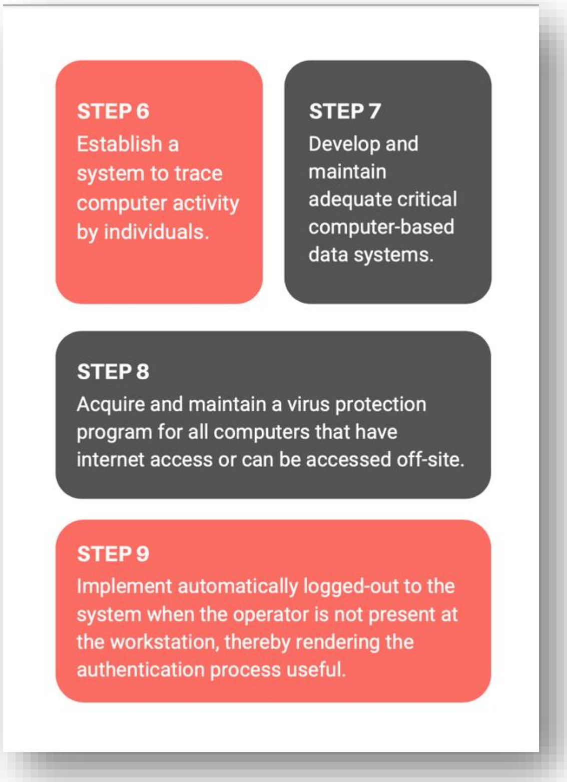


STEP 2
Implement secure network and/or router configuration.

STEP 3
Use intrusion detection systems and install firewalls with a strong and vertical firewall configuration.

STEP 4
Verify the security of critical information systems (SCADA, on line monitoring system and data transmission, internet, email) and review safe computer and internet access procedures with employees to prevent cyber intrusion. Have staff change computer passwords.

STEP 5
Restrict access to computer process control and data systems to those with appropriate clearance.



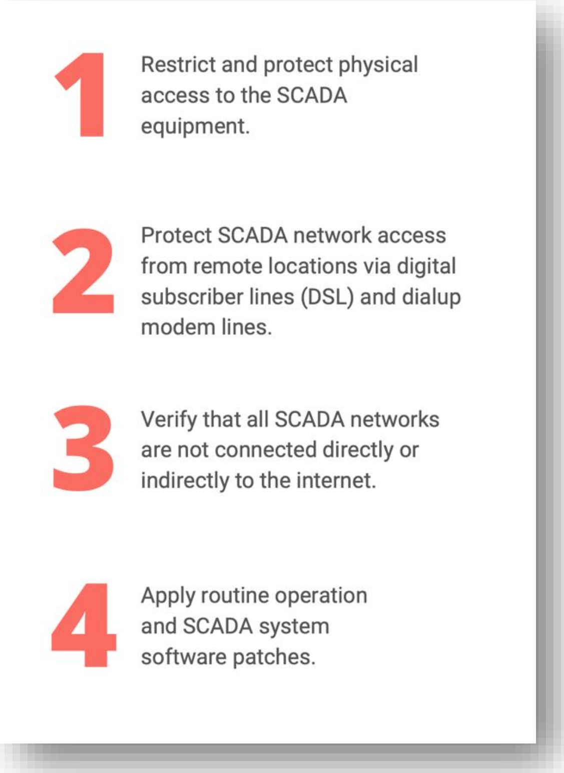
STEP 6
Establish a system to trace computer activity by individuals.

STEP 7
Develop and maintain adequate critical computer-based data systems.

STEP 8
Acquire and maintain a virus protection program for all computers that have internet access or can be accessed off-site.

STEP 9
Implement automatically logged-out to the system when the operator is not present at the workstation, thereby rendering the authentication process useful.

Supervisory Control And Data Acquisition



1 Restrict and protect physical access to the SCADA equipment.

2 Protect SCADA network access from remote locations via digital subscriber lines (DSL) and dialup modem lines.

3 Verify that all SCADA networks are not connected directly or indirectly to the internet.

4 Apply routine operation and SCADA system software patches.

CONTACT

Florent Kirchner
Project Coordinator CEA
France

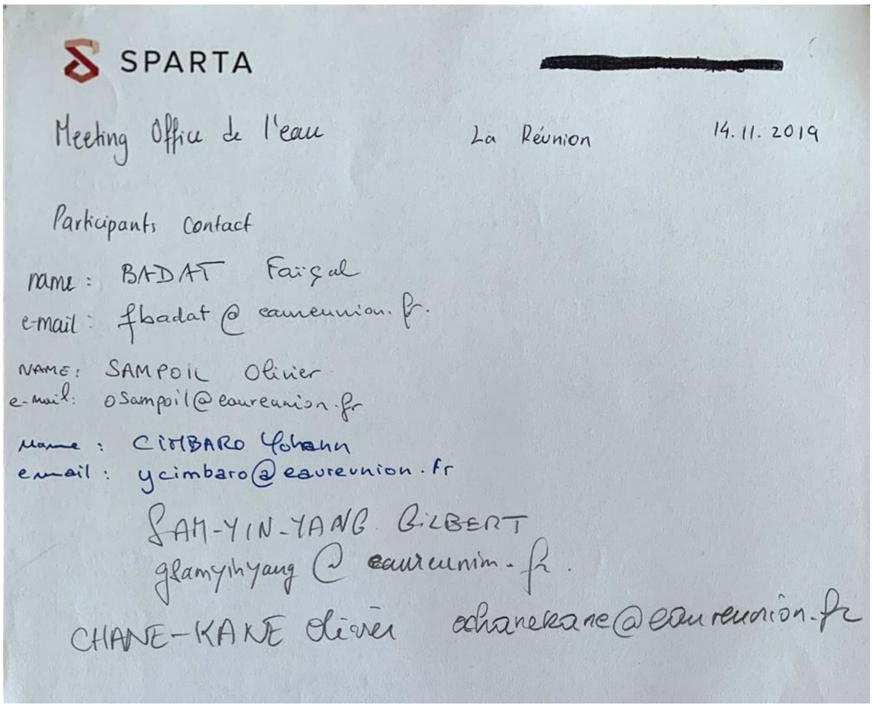
contact@sparta.eu
www.sparta.eu

Join Us!
The SPARTA roadmap process is open to partners. Communicate your challenges and take part in shaping future European research in cybersecurity.

Source | JRC Technical Reports: *Guidance for production of a Water Security Plan in drinking water supply* (in publication phase)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892

8.6 Annex 6 – List of attendees of the introductory meeting with Office de l'eau La Reunion



SPARTA [redacted]

Meeting Office de l'eau La Réunion 14. 11. 2019

Participants contact

name : BADAT Faïçal
e-mail : fbadat @ eaureunion. fr.

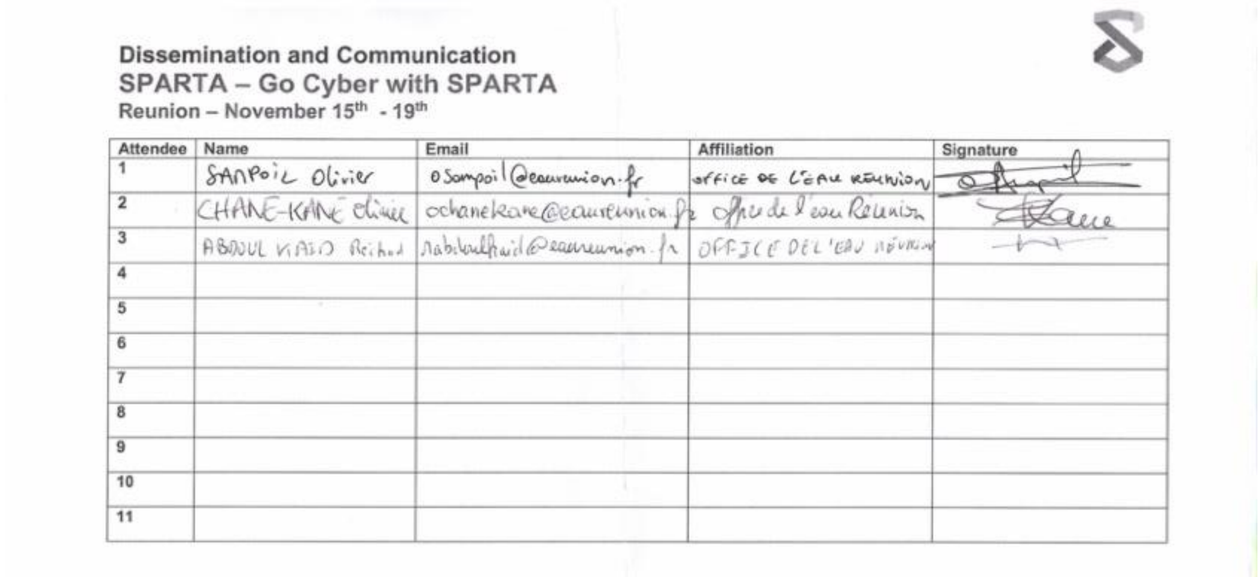
NAME : SAMPOIL Olivier
e-mail : oSampoil@eaureunion.fr

Name : CIMBARO Yohann
email : ycimbaro@eaureunion.fr

SAM-YIN-YANG GILBERT
glamyinyang @ eaureunion. fr.

CHANE-KANE Olivier ochanekane@eaureunion.fr

8.7 Annex 7 – Attendance list of the Cybersecurity Training and Awareness workshop delivered to Office de l’eau La Reunion



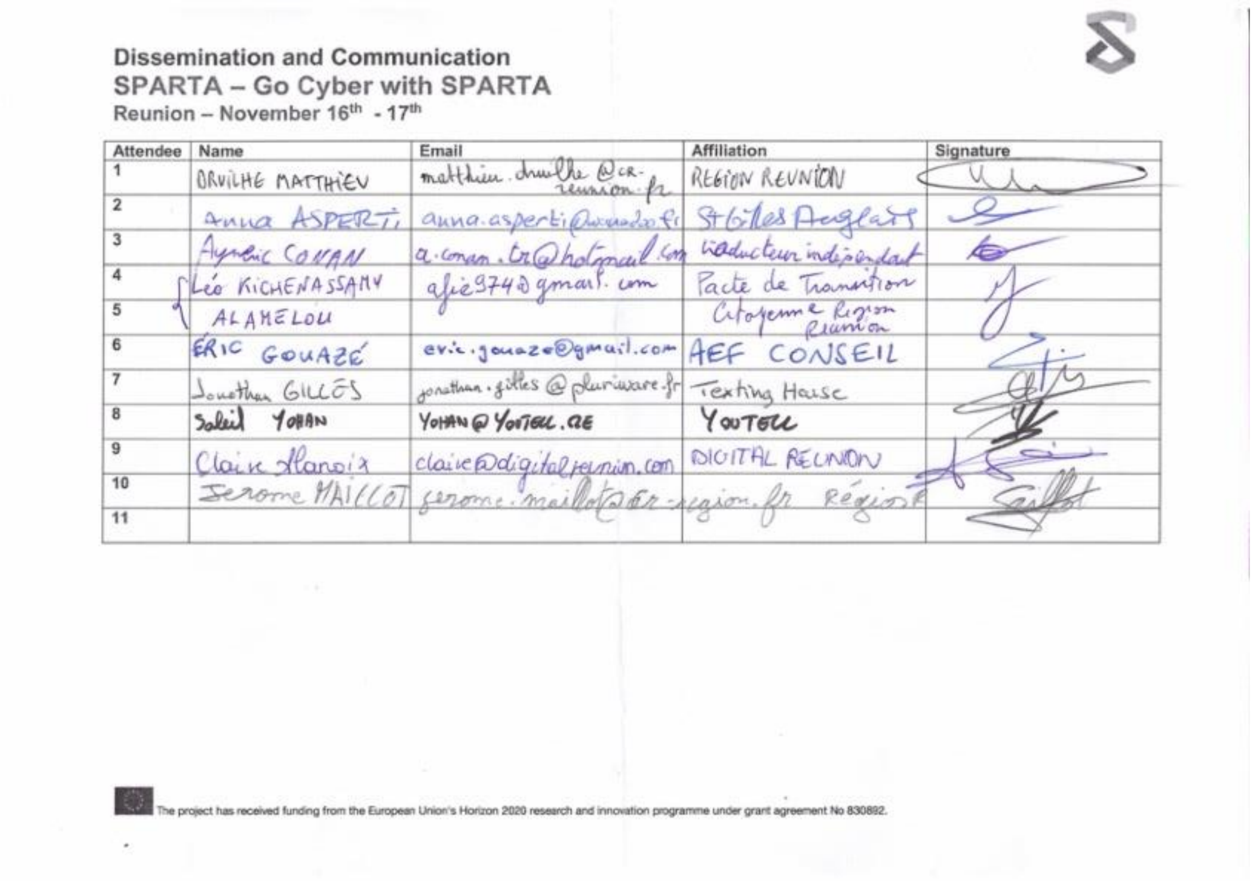
Dissemination and Communication

SPARTA – Go Cyber with SPARTA

Reunion – November 15th - 19th

Attendee	Name	Email	Affiliation	Signature
1	SANPOIL Olivier	osampoil@eaureunion.fr	OFFICE DE L'EAU REUNION	
2	CHANE-KANE Olivier	ochanekane@eaureunion.fr	Office de l'eau Reunion	
3	ABDOUL KAID Reihad	nabiloulkaid@eaureunion.fr	OFFICE DE L'EAU RÉUNION	
4				
5				
6				
7				
8				
9				
10				
11				

8.8 Annex 8 – Attendance list of the “Go Cyber with SPARTA” workshop



Dissemination and Communication

SPARTA – Go Cyber with SPARTA

Reunion – November 16th - 17th

Attendee	Name	Email	Affiliation	Signature
1	DRUILHE MATTHIEU	matthieu.druilhe@cr-reunion.fr	REGION REUNION	
2	Anna ASPERTI	anna.asperti@wanadoo.fr	St Gilles Anglais	
3	Aymeric CONAN	a.conan.tr@hotmail.com	traducteur indépendant	
4	Léo KICHENASSAMY	afie974@gmail.com	Pacte de Transition	
5	ALAMELOU		Citoyenne Région Réunion	
6	ÉRIC GOUAZÉ	eric.gouaze@gmail.com	AEF CONSEIL	
7	Jonathan GILLES	jonathan.gilles@pluriware.fr	Texting House	
8	Soleil YOHAN	YOHAN@YOUTELL.RE	YOUTELL	
9	Claire Flanoix	claire@digitalreunion.com	DIGITAL REUNION	
10	Jerome MAILLOT	jerome.maillot@cr-region.fr	Région R	
11				

The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892.