SPARTA

D12.3

Updated dissemination and communication plan and evaluation – v1

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 / D12.3/ V1.0
Work package contributing to the deliverable	WP12
Due date	February 2020 – M12
Actual submission date	31st January, 2020

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

Abstract	The present deliverable contains the updates and evaluation of the work carried out in each stage of the dissemination and communication planned actions in the D12.1. Updates have been designed aiming at leverage efficient actions, promoting audiences' awareness, participation and action in SPARTA, and cybersecurity realm.
Keywords	Communication and dissemination strategy, Awareness and participation, Monitoring and evaluation

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)

Vanessa Moreira, Elisabete Carreira (INOV)

Reviewers (ordered according to beneficiary numbers)

Diane Bahrami (CEA)

Rayna Stamboliyska (YWH)

Disclaimer

Executive Summary

The present deliverable contains the updates and evaluation of the work carried out in each stage of the dissemination and communication plan. Updates have been designed aiming at leveraging efficient actions, promoting audiences' awareness, participation and action in SPARTA and the cybersecurity realm.

Chapter 1 introduces the context for the development of the present deliverable and highlights the most relevant relations that allow WP12 to receive inputs to implement the C&D plan. Here, one can find a brief explanation about the execution of the communication and dissemination plan regarding inputs, deliverables and outcomes, and its main objectives.

Chapter 2 reviews the strategic axes established in deliverable 12.1, considering SPARTA's main objectives: Awareness, Participation and Action. This chapter defines the communication and dissemination strategy for the second year. The contribution of communication and dissemination to the KPIs of the project is also reviewed and updated.

Chapter 3 contains the updated information about the management of Communication and Dissemination actions, such as scientific publications, monthly workshops and other relevant events. A brief evaluation of each action is made. Here is also included the presentation, assessment and future actions of the SPARTA campaigns for diversity in cybersecurity – Closing the Gender Gap and the Engagement of the Outermost Regions of Europe.

Chapter 4 reviews the effectiveness of the Communication and Dissemination instruments deployed during the first year. The chapter provides a focus on the website and social media platforms.

Chapter 5 describes the methodology for monitoring and evaluating the implementation of the plan, defining the processes and responsibilities for reporting of activities to WP12.

Table of Content

List of Figures

List of Tables

Chapter 1 Introduction

SPARTA's WP12 – Communication and Dissemination, conceived to plan, coordinate and execute all the activities related to dissemination and communication, foresees the yearly update of the strategic plan designed within the deliverable 12.1 – Dissemination and Communication Plan – jointly with the evaluation of the work carried out during the previous year of the project.

The present deliverable aims to evaluate all the communication and dissemination activities carried out during the first year of the project and develop the adequate methods to correct possible deviations of the plan, providing suitable updates.

Table 1 from Deliverable 12.1 is here duplicated to highlight the most relevant relations that allow WP12 to receive inputs to implement the C&D plan.

The interaction between WP12 and WP1 – CCN Governance and assessment – has been of utmost importance to align the communication activities with the overall needs of the project.

The relations with WP3 – Roadmap Design and WP8 – Clustering, platforms and ecosystems have been crucial to the production of communication materials to the events as well as its dissemination on SPARTA social media accounts.

Interactions between SPARTA programs within the scope of WP4 to WP7 (T-SHARK, CAPE, HAII-T, and SAFAIR) and WP12 have not been fully implemented during the first year of the project due to the programs still short duration.

WP1 Governance model for the network **WP 3 & WP8** Workshops, conferences, trade shows **WP4 – WP7** SPARTA programs **WP11** Certification **All partners & WPs**	**D12.1** Dissemination and communication plan, updates and evaluation (M03, INOV) **D12.2** Internal and external IT communication infrastructure and project website (M03, TNK) **D12.3** Updated dissemination and communication plan and evaluation (M12, INOV) **D12.4** Updated dissemination and communication plan and evaluation (M24, INOV) **D12.5** Final report on dissemination and communication and evaluation (M36, INOV) **D12.6** Closing the gender and diversity gap (M36, INOV) **D12.7** Outermost regions engagement (M36, INOV)	Materials Events Internal and external IT communication infrastructures

Table 1 - WP12 in SPARTA

Chapter 2 Communication Strategic Approach

This chapter reviews the strategic axes established in deliverable 12.1, contains the evaluation of the strategy planned for the first year and defines the communication and dissemination strategy for the second year.

2.1 Strategic axes

The communication and dissemination plan is currently being developed considering the three different, interdependent strategic axes established in the deliverable 12.1:

Awareness building: making the project and its aims known.

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

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

The first version of the plan defined the Awareness building axis as the first-year approach, designed to be sustained during the entire project. Awareness is at the foreground of all our actions to build audiences that are informed about the project and aware of the impact it aims to achieve. A first-year general evaluation follows to monitor the achievement of the communication objectives proposed for the **Awareness** axis:

a) Give visibility to SPARTA to:
   - Inform the various key audiences about SPARTA project;
   - Enhance awareness about cybersecurity and the importance of this project;
   - Engage the audiences with SPARTA project.

b) Promote efficient communication between all partners.

The **Participation** axis started to emerge by the end of the first year of the project through collaborations being held in WP8, WP9, and WP12. The second year of the project foresees the rising of the **Participation** axis among audiences that are aware of SPARTA and the continuous efforts to maintain the **Awareness** axis.

The communication efforts for the second year of the SPARTA project aim to promote higher levels of audiences' engagement with the project, such as:

a) Higher attendance in SPARTA events
b) Contacts from media
c) Invitation for speaking at external events
d) Demonstrations of interest and commitment with the project (e.g. through Associates and Friends Programs)

These objectives will be possible to achieve if coordinated actions between all the SPARTA project partners are sustained and nourished as proposed in this deliverable.

2.2 Key Audiences and Messages

SPARTA audiences have been previously identified and characterized and are still relevant. A mixed-channel approach was also considered aiming to reach the identified audiences through different channels and supports. Such an approach has shown to be efficient and accurate because SPARTA was able to achieve the communication objectives defined in the previous deliverable.

The messages developed to allow the transmission of a strong and guided message based on the project objectives and according to its progress are being delivered in multiple formats and through multiple channels. Three Videos were produced aiming to deliver these messages and shared on SPARTA social media accounts. The specific messages per strategic axes are still accurate.

Because the M12 – M24 period foresees the emergence of the participation axis, the following messages will have a greater focus:

1. Cybersecurity is a global phenomenon and a complex challenge for governments both at social and technical levels.
2. Because it is an issue with impact in citizens' everyday lives, the involvement of individuals is necessary to raise awareness and promote societies' resilience to cybersecurity risks and threats.
3. The project will create value among cybersecurity ecosystems, from end-users to solution providers, from governmental bodies to ethical hacking communities. It will leverage expertise from several audiences, in various locations in the EU, to raise awareness and to foster conversations ranging from cutting-edge research advances to accurate problem identification.

2.3 Contribution to the KPI's of the project

The previous deliverable anticipated the direct contributions of the communication and dissemination activities to specific project KPIs. The present deliverable provides the achieved results. Enhance awareness and training capabilities and develop cybersecurity skills, which will be 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		>5000	
6.4 - number of indirectly addressed people (through advertisements, social media) by the awareness program by the end of the project.	>2000	>10 000 (average of impressions of awareness posts)	>20000		> 50000	

Table 2 - KPIs measures for the objectives with 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	1st MW – ? 2nd MW – 30 3rd MW – 27 4th MW – 19 5 – 8 MW's - TBD	> 24 >30		> 36 >50	

Table 3 - KPIs measures for the objectives with WP3 and WP8

The KPI regarding number of workshop was only partially achieved during this first year mainly due to the time needed to ramp up the project and the creation of the workshop and partnership infrastructure.

2.4 Cybersecurity Competence Network – 4 Pilot Projects

The coordinated work leveraged within the scope of the EU H2020 Cybersecurity pilot projects - Cyber Competence Network - deployed in articulation with the European Commission and the other three pilots resulted in the creation of a common website, released on the 5th of June, under the lead of ECHO.

SPARTA contributed with the production and dissemination of communication materials developed within WP12, prepared to raise awareness and ensure CCN's visibility :

- An official CCN Presentation Video
- An official CCN Infographic

SPARTA prepared the website launch campaign to disseminate through each project pilot's social media accounts. The campaign was able to reach up to 5,967 impressions on Twitter, 644 impressions on LinkedIn and 114 on Instagram.

During the first year, SPARTA made an effort to engage with all the shared contents related to CCN's events and achievements, aiming to leverage their visibility among the scientific community – our primary audience on social media.

CCN's Communication Management From January 2020 to June 2020 SPARTA project will chair the CCN's communication and dissemination management and strategy.

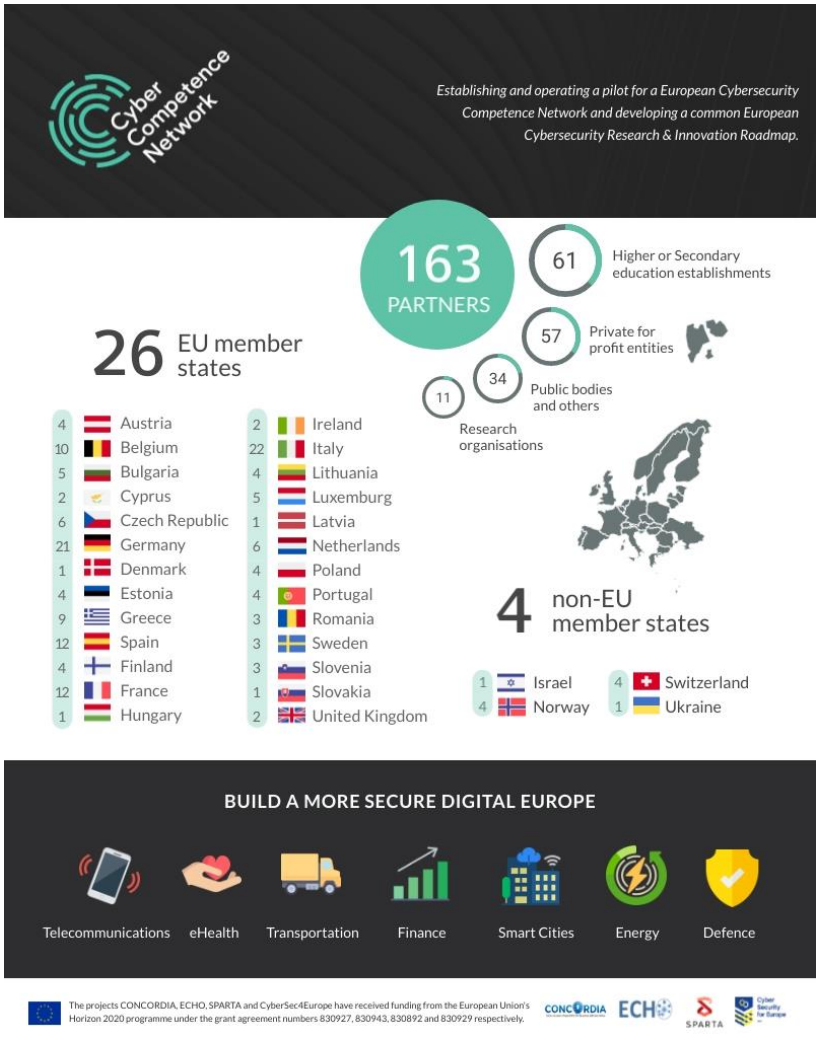


Figure 1 - Official CCN Infographic

Chapter 3 Communication and Dissemination actions

This chapter highlights the actions developed by SPARTA partners during the first year of the project to disseminate project results by giving talks at conferences, workshops and trade shows, and writing articles for technical and academic publications. Task 12.4 and 12.5 – *Closing the Gender and Diversity Gap* and *Engagement of the Outermost Regions of Europe* – are addressed in this chapter, both are calling for a coordinated action aimed to enhance diversity and inclusion in the cybersecurity field.

3.1 Conferences and events, including trade shows and exhibitions

Through the several communication actions promoted - such as workshops, SPARTA Days, conferences, and talks - it has been possible to inform the various key audiences about the SPARTA project, to enhance awareness about cybersecurity and the importance of this project and to engage the audiences with the project. The SPARTA presence in such events was instrumental in fostering sustained collaborations with academic, industrial, governmental, and community stakeholders.

The following table is an updated list of potential events for the dissemination activities during 2020:

Name of the event	Frequency
The 35th ACM/SIGAPP Symposium On Applied Computing 2020	Annual
Conference on Computer Privacy and Data Protection (CPDP)	Annual
Conference on Cryptographic Hardware and Embedded Systems	Annual
Conference on Ethics of Computing (ETHICOMP)	Annual
EAFS – European Academy of Forensic Science Conference (2021)	Bi-three yearly
European Cybersecurity Challenge (ECSC)	Annual
European Symposium on Research in Computer Security (ESORICS)	Annual
IEEE European Symposium on Security and Privacy (Euro S&P)	Annual
Int. Conference on Cyber Situational Awareness, Data Analytics and Assessment IEEE	Annual
IEEE Industrial Electronics Society (IES)	Annual
FMCAD Student Forum 2020	Annual
Int. Conference on the Theory and Applications of Cryptographic Techniques Eurocrypt 2020	Annual
International Conference on Availability, Reliability and Security (ARES)	Annual

Name of the event	Frequency
International Conference on Dependable Systems and Networks (DSN)	Annual
8th International Conference on Information Technology and Science (ICITS 2020)	Annual
22nd International Conference on Enterprise Information Systems (ICEIS 2020)	Annual
13th International Conference on Security and its Applications (CNSA 2020)	Annual
17th International Conference on Security and Cryptography (SECRYPT 2020)	Annual
Interactive Workshop on the Industrial Application of Verification and Testing (InterAVT)	Annual
MobiQuitous - EAI International Conference on Mobile and Ubiquitous Systems.	Annual
Privacy Enhancing Technologies Symposium (PETS)	Annual
IFIP SEC 2020: 35th IFIP TC-11 SEC 2020 International Information Security and Privacy Conference	Annual
IT-Security conference of the German Informatics Society (GI-Sicherheit)	Biannual
International Conference on Computational science (iccs) 2020	Annual

Table 4 - Updated list of possible events

To facilitate partners' perception of the events' occurrence a calendar of the potential events for dissemination listed above is updated in the project's SVN:

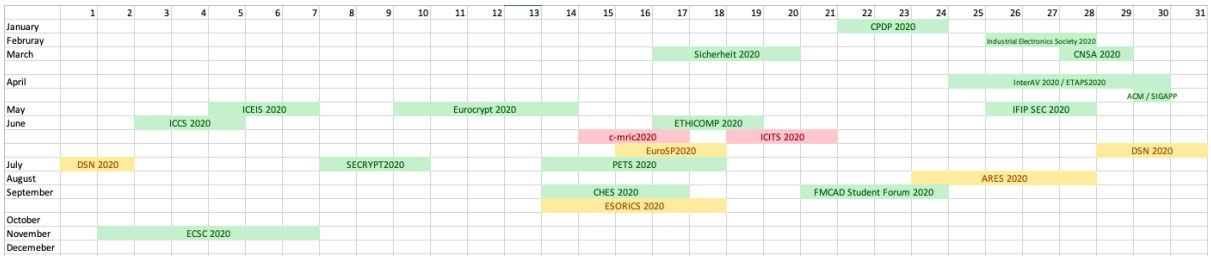


Figure 2 - Calendar of potential events for dissemination 2020

3.2 Scientific Publications

The list of possible scientific journals, conferences, workshops, symposiums for SPARTA dissemination of scientific results proposed on the D12.1 is duly updated in tables 2 and 3. More incisive dissemination of the scientific publications will be possible, at the beginning of January 2020,

through accessing the SPARTA website *Results* page, where all these contents are stored and organised to facilitate the search process.

The C&D team established the necessity to make these contents understandable for the broader audience that is not familiar with the kind of language used in scientific publications. Having this necessity established, an **"Abstract for all"** approach is currently being implemented by the SPARTA partners that are about to publish scientific results. It consists in giving the possibility for a broader audience to understand the content of the results, by writing a simplified abstract of the scientific publication.

Name of the scientific Journal	Main Dissemination Aspects
ACM Transactions on Information and System Security (TISSEC)	Devoted to the study, analysis, and application of information and system security. TISSEC topics include: security technologies; secure systems; secure applications; and security policies.
ACM Transactions on Privacy and security	Publishes high-quality research results in the fields of information and system security and privacy. Studies are ranging from technologies, systems, applications and policies.
Elsevier Computer Fraud & Security	Every month Computer Fraud & Security enables to see the threats to user's IT systems before they become a problem. It focuses on providing practical, usable information to manage and control computer and information security effectively.
Elsevier Computer Law & Security Review	International journal of technology law and practice providing a major platform for publication of research, policy and legal analysis within the field of IT law and computer security.
Elsevier Computers & Security	Provides a unique blend of leading-edge research and sound practical management advice. It is aimed at the professional involved with computer security, audit, control and data integrity in all sectors - industry, commerce and academia.
IEEE security and privacy	Stimulates and tracks advances in security, privacy, and dependability and presents these advances in a form that can be useful to a broad cross-section of the professional community, ranging from academic researchers to industry practitioners.
IEEE Technology & Society Magazine	The impact of technology on society, the impact of society on the engineering profession, the history of the societal aspects of electrotechnology, and professional, social, and economic responsibility in the practice of engineering and its related technology.

Name of the scientific Journal	Main Dissemination Aspects
IEEE Transactions Dependable and Secure Computing (TDSC)	Dependability and security, including the joint consideration of these issues and their interplay with system performance.
IEEE Transactions on forensics and security	Covers sciences, technologies, and applications relating to information forensics, information security, biometrics, surveillance and systems applications that incorporate these features.
IEEE Access	IEEE Access is an award-winning, multidisciplinary, all-electronic archival journal, continuously presenting the results of original research or development across all of IEEE's fields of interest.
Springer Ethics and Information Technology	Dedicated to advancing the dialogue between moral philosophy and the field of information and communication technology (ICT).
Springer Journal of Cryptographic Engineering (JCEN)	Offers high-quality scientific articles presenting methods, techniques, tools, implementations, and applications of research in cryptographic engineering, including cryptographic hardware, cryptographic embedded systems and embedded security.
Springer Journal of Cryptology	It is a forum for results in all areas of modern information security. Both cryptography and cryptanalysis are covered, including information-theoretic and complexity-theoretic perspectives as well as implementation, application, and standards issues.
Proceedings on Privacy Enhancing Technologies (PoPETs)	PoPETs is an open access journal for timely research papers on privacy that has been established as a way to improve reviewing and publication quality while retaining the highly successful PETS community event. PoPETs is published by Sciendo, part of De Gruyter, which has over 260 years of publishing history.
IETF Datatracker	The IETF Datatracker is the day-to-day front-end to the IETF database for people who work on IETF standards. It contains data about the documents, working groups, meetings, agendas, minutes, presentations, and more, of the IETF.
SoftwareX	SoftwareX aims to acknowledge the impact of software on today's research practice, and on new scientific discoveries in almost all research domains. SoftwareX also aims to stress the importance of the software developers who are, in part, responsible for this impact.

Name of the scientific Journal	Main Dissemination Aspects
Journal of Automated Reasoning	The interdisciplinary Journal of Automated Reasoning balances theory, implementation and application.

Table 5 - Updated List of potential Scientific Journals for dissemination

3.3 Monthly SPARTA workshops

Within the scope of WP3 and WP8, the consortium was able to organize several SPARTA workshops, where a diverse multiplicity of actors come together to get involved with the project. The C&D team was involved in the event's promotion and dissemination through the SPARTA social media accounts. Nonetheless, the C&D activities related to the SPARTA Monthly Workshop can be maximized if the communication between partners is ensured. This is a challenge that will be addressed through a mitigation strategy that includes the use of *Stackfield*, a tool that allows for simplified methods of collaboration, further explained in the *SPARTA project communications* section of this document.SPARTA project communications

3.4 Campaigns for Diversity in Cybersecurity

3.4.1 Closing the Gender Gap

SPARTA has been researching the issues that may be at the backbone of the gender gap faced in the cybersecurity field, striving to understand what kind of activities could enhance the inclusion and attraction of women into the cybersecurity workforce. As a result, a set of actions are currently being prepared to promote awareness of the current situation, ultimately aiming to attract women to the field.

Communication objectives are:

- Address female public in dissemination activities
- Incentive female participation, involvement and uptake in cybersecurity, namely in SPARTA
- Promote awareness of the need for a gender-balanced and diverse workforce in cybersecurity

The following tables summarize the planned activities for the M12 – M14:

SPARTA Partners up with Women4Cyber	
Target	Women in cybersecurity Community and SPARTA partners
Objectives	Understand the reasons beyond the gender gap in cybersecurity and cooperate with Women4Cyber to help achieving a more diverse cybersecurity workforce.
Calendar	On going
Description	The framework for our joint cooperation is yet to be stablished.

Table 6 - Women4Cyber Program

SPARTA Women Campaign On Social Media	
Target	Female audience aged between 16 and 30 Cybersecurity and Tech community
Objectives	Raise awareness on the need for a diverse workforce on cybersecurity Raise awareness on the importance of cybersecurity Engage women of the EU in cybersecurity
Calendar	From March 2020 to March 2021
	From March 2020 to March 2021, SPARTA will have weekly publications about: - Achievements of women in cybersecurity - SPARTA commitment to increase the number of women in cybersecurity - Reach 100 female followers - SPARTA Women events - SPARTA state of the art regarding female participation in cybersecurity - Set of interviews to highlight the work of women participating in SPARTA - Best practices on how to attract and retain women in the cybersecurity field Related re-tweets
Evaluation	By the end of March 2021, SPARTA social media should have decreased its audience gender gap.

Table 7 - Women Campaign On Social Media

SPARTA goes to high school	
Target	Female students who are finishing high school and about to enter university
Objectives	Raise awareness on the importance of cybersecurity and on the need for a diverse workforce.
Calendar	1 day – September 2020
Description	The main idea behind this action is to raise awareness on the importance of cybersecurity, among the future university students, who may opt for a cybersecurity related field of study. **Program** 10h00 | SPARTA Presentation This presentation should be creative and able to catch the student's attention. It should not be longer than 20 minutes.

SPARTA goes to high school	
	It should focus on the main, global aspects of the project and its impact for the society. 10h30 | Coffee break (Goodies time) 10h45 | Cybersecurity Workshop + Challenges For this workshop, a registration will be needed as to ensure we will have a 60% female presence at the workshop. 10h45 | The importance of a diverse workforce in cybersecurity and the current statistics. 11h15 | Workshop 13h00 | Group photo to spread on social media **Women in Cybersecurity - Exhibition** As to prolongate the SPARTA impact at school, an exhibition about cybersecurity importance will be set up. The exhibition should contain: 1. Story of the first female coders with photos; 2. Small sentences about the importance of a diverse workforce in cybersecurity + statistics. 3. Our goal, to "reduce the gender gap in cybersecurity" The photos of the workshop.
Evaluation	How many registrations for the workshop / attendees? How many new followers on social media? Monitor Kahoot answers to understand the students' engagement and workshop success.
Materials	- SPARTA Roll-up - SPARTA Merchandise (bags and stickers) - Coffee, fruit, and pastéis de nata. For the exhibition: - Photos and text printed. - SPARTA leaflet/ poster. Infographics about women in cybersecurity.

Table 8 - SPARTA goes to high school

A **SPARTA Women Mentorship Program** is expected to be deployed in the beginning of the third year of the project. The main objective is to promote the engagement of EU women in cybersecurity and their inclusion. The main lines of this Program will be to prioritize female participation in all training related activities during the 3rd year of the project, as to address and incentive female participation, involvement and uptake.

3.4.2 Engagement of the Outermost Regions of Europe

Advances were made during the first year of the project, allowing the timely progress of the *Go Cyber with SPARTA* campaign.

The regions and institutions/organizations/companies in which the campaign will be settled are established as well as the exact proceedings and activities that will be held within each context/ region.

Regarding **action 1** – *Encourage small businesses to adopt cybersecurity measures* (the Caribbean and South America OR) – interactions with Technopole Martinique - an organization that supports innovation initiatives to make Martinique a territory of excellence and offer businesses a favourable environment – will be held to promote Martinique island's engagement with the *Go Cyber with SPARTA* campaign.

Regarding **action 2** – *Stimulate young people to undertake studies or training at the university level within the area of cybersecurity* (Atlantic Ocean OR) **–** collaborations with the Universidad de Las Palmas de Gran Canaria are established and will proceed in a coordinated action with the SPARTA **Cybersecurity Training and Awareness Program (WP9)** to:

1. Define the essentials of computer security that should be present in all computer science curricula
2. Design new and improve existing curricula for bachelor degrees in computer security based on the Universidad de Las Palmas de Gran Canaria needs
3. Implement an awareness campaign to stimulate students to undertake studies in the cybersecurity field, taking into account the student's characteristics and necessities of Las Palmas de Gran Canaria.

It is important to note that the Universidad de Las Palmas de Gran Canaria is willing to be part of the Associates and Friends Program.

Regarding **action 3** – *Engage with critical infrastructure operators to stimulate them to adopt state-of-the-art cybersecurity technology* (Indian Ocean OR): Office de L'eau, La Réunion's Water Critical Infrastructure will also integrate the campaign, which will be developed in a coordinated action with the SPARTA **Cybersecurity Training and Awareness Program (WP9)** and can be summarized in the following (and potential) actions/outputs:

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

For the coming year, the C&D plan foresees the creation of stronger relationships with these entities as to foster sustainable and successful collaborations. The main objectives to be achieved between M12 and M24 are:

- Have Technopole Martinique as part of the "Go Cyber with SPARTA" campaign
- Build sustained collaborations with *Office de L'eau* and *Universidad de las Palmas de Gran Canaria*, by ensuring strong communicational bounds
- Communicate to the wider audience the "Go Cyber with SPARTA" campaign through SPARTA social media accounts and website.

3.5 Contribution of partners to communication and dissemination activities

Partners' contribution to dissemination and communication activities has been of utmost importance to achieve the C&D objectives and to guide the project through the strategic axes established: awareness, participation and action. Partners have been acting accordingly to what was proposed in D.12.1, enabling the establishment of collaborations and promoting awareness of the SPARTA project.

The second year of the project foresees the maximization of SPARTA partners' contribution through their direct participation in the creation of contents to be shared on social media accounts and on the website. Such novelty aims to improve the frequency, diversity and quality of information shared on these C&D channels. A high-level strategy was designed to meet such need, thus keeping the audiences updated and informed about several aspects related to the SPARTA project and cybersecurity field, leveraging audiences' engagement and participation. This strategy will be implemented in February 2020 and information is now updated on the C&D Guidelines for partners.

Chapter 4 Communication and dissemination Instruments

This chapter considers the C&D instruments that have been updated to improve their efficiency, ensuring that the project's communication objectives have a strong instrumental base to be correctly addressed.

4.1 SPARTA Website

The website is currently available and constantly being worked on to introduce improvements, leaded by CEA and INOV, aiming to provide a dynamic and evolving platform where visitors can have an holistic understanding of SPARTA project, access SPARTA results, be updated with the projects' latest achievements and events. The new version of the website is available since the beginning of January at www.sparta.eu.

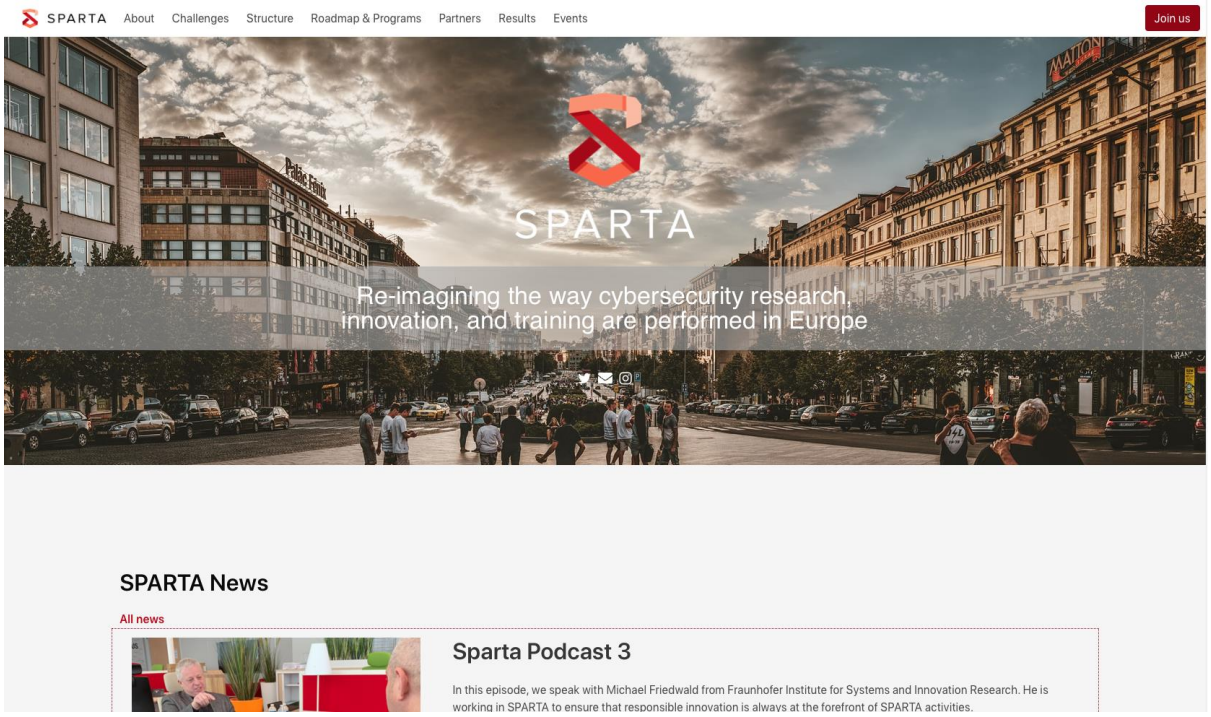


Figure 3 - SPARTA Website homepage

4.2 SPARTA project communications

Due to the complexity and large number of partners involved in the project, the internal communication among partners faces some challenges that have been identified and addressed. As a result, the following tools will be deployed aiming to leverage a simple and fluid communication among all partners, thus allowing for cohesion and awareness of the overall project achievements.

4.2.1 Bi-monthly internal newsletter

The main objective for the creation of the newsletter is to promote the communication among partners, ensuring everyone is updated with what is happening in the different project's WPs.

WPs leaders will provide a text with the WP latest news/ achievements. Some of these contents will be selected – based on their relevance to the broader audience – to feed the SPARTA official website and social media.

The newsletter will be structured with a section to highlight more significant events or achievements, a section dedicated to the SPARTA Roadmap, a section devoted to the four programs and an "Abstract for all" section (to have scientific publications understandable for everyone).

4.2.2 Stackfield

The use of *Stackfield*, a tool that allows easier collaboration among partners, sharing tasks and documents will facilitate internal communication. *Stackfield* is already implemented and provides rooms dedicated to each WP, thus simplifying the exchange of ideas and practical information.

4.3 SPARTA Social Media

A **social media content management tool** will be selected to coordinate and manage all publications efficiently. These tools allow for a streamlined teamwork to organize, schedule and publish content effortlessly to all SPARTA social media accounts, whenever a conference, meeting or any public event occurs.

4.4 Other promotional tools

4.4.1 Project Leaflet

The general project leaflet has been updated with a more holistic approach, integrating the SPARTA project activities, and has been delivered in several events.

4.4.2 SPARTA Merchandise

SPARTA merchandise was created to deliver during the C&D activities. It consists of a set of SPARTA T-shirts, bags, ribbons, stickers and carabiners.

Chapter 5 Monitoring and Evaluation

5.1 Monitoring C&D actions

5.1.1 Events

The several C&D actions developed during the first year (e.g. Conferences, workshops, talks, publications) made it possible to inform audiences about SPARTA and to promote their engagement with the project. SPARTA participated in 37 (conferences/workshops/others), organised two conferences and eight Monthly Workshops. Of a total of 50 events, the academia was involved/ represented in 36 and the Industry in 33, thus SPARTA's most preeminent audience at the moment. Most of these events occur at the international level and gather a significant diversity of stakeholders.

Events are listed below:

No	Type of activities	Main leader	Title	Place	Description of the event	Level
1	Organisation of a Workshop	BUT	Brno Security Meetings	Brno, Czech Republic	Workshop and awareness event for students, researchers and general public focused on cryptography and implementation aspects on smart cards.	National
2	Participation to other events	CEA	SPARTA booth at Cyber Festival — 10 years of ANSSI	Paris, France	Presentation of SPARTA to the attendees of the CyberFestival organized by ANSSI for its 10 years	National
3	Participation to other events	CEA	SPARTA booth at DigiHall Days	Palaiseau, France	Presentaton of SPARTA to the attendees of DigHall days	National

No	Type of activities	Main leader	Title	Place	Description of the event	Level
4	Organisation of a Conference	CEA	SPARTA Day	Palaiseau, France	The SPARTA Day proposes high-level presentation and panels discussing about cybersecurity strategy, collaboration, and stakeholders inclusion.	International
5	Participation to other events	CEA	Meeting with Commissioner Mariya Gabriel	Strasbourg, France	Meeting with Commissioner Mariya Gabriel at the European Parliament to present the 4 pilots and discuss cybersecurity challenges Europe faces.	International
6	Participation to other events	CEA	Resilience. Deterrence. Defence – Calls to action for future cybersecurity and privacy policy Concertation meeting of H2020 projects from unit "Cybersecurity & Privacy"	Brussels, Belgium	All four projects now thoroughly active this session will address how each pilot is planning to address the following issues: Cyber-ranges; Threat intelligence; Certification; Cybersecurity skills	International
7	Participation to other events	CEA	Common website for pilots launch	Brussels, Belgium	Welcome from CONCORDIA coordinator and introduction of new project partners, Prof. Dr. Gabi Dreo, Research Institute Cyber Defence (CODE) Panel discussion – True European Cooperation: a Pillar of Digital Sovereignty? Presentation of four pilots - CONCORDIA, SPARTA, ECHO and CyberSec4Europe Launching of the common web site	International

No	Type of activities	Main leader	Title	Place	Description of the event	Level
8	Participation to a Workshop	NCSR	H2020 Ghost clustering workshop	Athens, Greece	This workshop is organized by the GHOST project aiming at establishing tight connections with relative H2020 projects in the field of cybersecurity in IoT and relative domains.	International
9	Participation to a Conference	CEA	13th Meeting of the Community of Users on Secure, Safe, Resilient Societies	Brussels, Belgium	Sub-theme 2.2: Building a cybersecurity ecosystem to secure Europe's society	International
10	Participation to other events	CEA	Presentation of the 4 Cybersecurity Centre Networks at ICT Proposer's Day 2018	Vienna, Austria	The focus: support the audience to join, participate and benefit from the 4 Cybersecurity Competence Networks. Targeting mainly the SME and Start-ups to raise awareness on how they can join.	International
11	Participation to a Conference	CEA	This is SPARTA	Erquy, France	Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information	National
12	Participation to a Workshop	CEA	Advances in Usability of Formal Methods for Code Verification	Prague, Czech Republic	InterAVT 2019 Interactive Workshop on the Industrial Application of Verification and Testing	International
13	Participation to other events		SPARTA Project	Palaiseau, France	CEA List General Assembly	National

No	Type of activities	Main leader	Title	Place	Description of the event	Level
14	Other	CEA	SPARTA Project	Paris, France	Japanese scientific delegation to France	International
15	Other	CEA	SPARTA Project	Paris, France	Meeting with Ministry of Interior of France	National
16	Participation to other events	CEA	SPARTA booth at CEA List Days	Palaiseau, France	Presentaton of SPARTA to the attendees of CEA List days	National
17	Participation to other events	CEA	SPARTA Project	Saclay, France	"Scientifique, toi aussi !" allows high-school students to meet scientists and understand how research is done.	National
18	Participation to other events	CEA	This is SPARTA	Saclay, France	SPRING Saclay	National
19	Other	CEA	SPARTA Project	Brussels, Belgium	Invitation from the US Embassy in Belgium to present SPARTA	International
20	Other	CEA	SPARTA Project	Palaiseau, France	Presentation to Chief Executive of French Defense Innovation Agency	National
21	Other	CEA	SPARTA Project	Palaiseau, France	Presentation to the Working Group of the Systematic cluster	National
22	Participation to other events	CEA	LeHack2019	Paris, France	Presentation of SPARTA to the attendees of the LeHack 2019 event and engagement with the cybersecurity community.	National

No	Type of activities	Main leader	Title	Place	Description of the event	Level
23	Participation to a Conference	JR	Austrian ICT Security Conference	Fürstenfeld, Austria	ICT Security Conference organised by the Austrian Armed Forces, the largest Austrian Cybersecurity conference, that attracted 2.500 interested visitors in two days.	National
24	Participation to a Conference	CETIC	7th europol-interpol cybercrime conference	The Hague, The Netherlands	Attending presentations and discussions on cybersecurity act and cybersecurity ontologies (including UCO and CASE).	International
25	Participation to a Conference	UTARTU	OTM 2019 Conferences, the 27th International Conference on Cooperative Information System	Rhodes, Greece	Attending the presentations, presenting the paper "Security Risk Management in Cooperative Intelligent Transportation Systems: A Systematic Literature Review".	International
26	Participation to a Conference	SAP	Heise devSec	Heidelberg, Germany	Developer conference organized by Heise/dpunkt, during which Eclipse Steady was presented.	International
27	Participation to a Conference	SAP	TechEd	Barcelona, Spain	Industry conference organized by SAP, during which Eclipse Steady was presented.	International
28	Participation to a Conference	SAP	EclipseCon	Ludwigsburg, Germany	Developer conference organized by the Eclipse Foundation, during which Eclipse Steady was presented.	International
29	Participation to a Conference	TEC	XIII Congreso Internacional de Ciberseguridad	Madrid, Spain	https://www.cci-es.org/web/cci/detalle-congreso/-/journal_content/56/10694/850611	International

No	Type of activities	Main leader	Title	Place	Description of the event	Level
			Industrial en Europa			
30	Participation to a Conference	TEC	Congreso Protección de Datos Bilbao | Wolters Kluwer	Bilbao, Spain	https://tienda.wolterskluwer.es/p/congreso-privacidad-bilbao	International
31	Participation to a Conference	TEC	IT.SA The IT Security Expo and Congress	Nurember, Germany	https://www.it-sa.de/en	International
32	Participation to a Conference	TEC	Congreso Basque Industry 4.0 and Basque Cybersecurity Day	Bilbao, Spain	https://agenda.spri.eus/meetingpoint/es	International
33	Organisation of a Conference	LEO	SPARTA Event - Cybertech Europe 2019	La Nuvola Convention Center - Rome	https://www.cyberwatching.eu/projects/1136/sparta/news-events/sparta-event-cybertech-europe-2019	International
34	Organisation of a Workshop	CNIT	CY4GAMES	Rome, Italy	https://www.cy4gate.com/cy4games	International
35	Participation to a Conference	CNIT	NETSOFT 2019	Paris, France	https://netsoft2019.ieee-netsoft.org/	International

No	Type of activities	Main leader	Title	Place	Description of the event	Level
36	Participation to a Conference	LIST	ICT Spring 2019	Luxembourg	https://www.ictspring.com	International
37	Participation to a Conference	LIST	Information Security Day 2019	Luxembourg	https://securitymadein.lu/events/information-security-day/	International
38	Participation to a Conference	LIST	Luxembourg Internet Days 2019	Luxembourg	https://www.luxembourg-internet-days.com	International
39	Participation to a Conference	BUT	14th International Conference on Availability, Reliability and Security	Canterbury, United Kingdom	https://2019.ares-conference.eu/	International
40	Participation to a Conference	BUT	13th International Conference on Network and System Security	Sapporo, Japan	http://nsclab.org/nss2019/	International
41	Participation to a Conference	BUT	ICT Systems Security and Privacy Protection	Lisbon, Portugal	https://www.ifipsec.org/2019/	International
42	Participation to a Conference	TNK	16. Österreichischer IT-	Klagenfurt, Austria	https://www.syssec.at/de/veranstaltungen/sitag2019	International

No	Type of activities	Main leader	Title	Place	Description of the event	Level
			Sicherheitstag 2019			
SPARTA Monthly Workshops*						
43	Organisation of a Workshop	CEA		France	Held during the SPARTA Kick Off meeting	International
44	Organisation of a Workshop	LEO		Italy	Held during the Cybertech Europe Event	International
45	Organisation of a Workshop	CNR		Italy	Held during Cybersecurity day	International
46	Organisation of a Workshop	UBO		Germany	Held during BDCS	International
47	Organisation of a Workshop	L3C		Lithuania	The objective of the workshop was to disseminate the SPARTA goals and results between national stakeholders and promote international collaboration and networking.	International
48	Organisation of a Workshop	Inria	CominLabs workshop – “Security and Privacy”	Rennes France	The CominLabs is an initiative selected as part of the "Laboratoires d'Excellence" program by the French ministry of research and education. The CominLabs workshop – „Security and Privacy” workshop focused on Cybersecurity including a special track on Sparta.	National

No	Type of activities	Main leader	Title	Place	Description of the event	Level
49	Organisation of a Workshop	YWH		Madrid, Spain	The workshop was framed in the 6th edition of Mundo Hacker Day.	International
50	Organisation of a Workshop	TEC	Jornada de Trabajo: Pilotos de Ciberseguridad Europeos y el Impacto para España	13ENISE, León, Spain	A SPARTA workshop was organized in Leon (Spain) within the context of the ENISE 2019 conference, and in cooperation with the CONCORDIA and CyberSec4Europe pilots.	National

Table 9 - List of events

*A more detailed report on the SPARTA Monthly Workshops can be find in the deliverable *D8.1: Initial results of the clustering, platforms, and ecosystems activities*

5.1.2 Scientific Publications

To date, SPARTA partners have submitted 31 articles that have been accepted for presentation/publication. Accepted papers are listed below:

No.	Title (SP/Dataset)	Authors/Owners	Partner	Journal/ Conference	DOI (publisher)
1	Formal Security Verification of Industry 4.0 Applications	Vivek Nigam and Carolyn Talcott	FTS	ETFA	10.1109/ETFA.2019.8869428
2	Fast Keyed-Verification Anonymous Credentials on Standard Smart Cards	Jan Camenisch and Manu Drijvers and Petr Dzurenda and Jan Hajny	BUT	ICT Systems Security and Privacy Protection - IFIP SEC 2019	10.1007/978-3-030-22312-0_20
3	A Secure Publish/Subscribe Protocol for Internet of Things	Lukas Malina, Gautam Srivastava, Petr Dzurenda and Jan Hajny	BUT	The 14th International Conference on Availability, Reliability and Security (ARES 2019) (Track: Iot-SECFOR 2019)	10.1145/3339252.3340503
4	Security Risk Management in Cooperative Intelligent Transportation Systems: A Systematic Literature Review	Abasi-amefon O. Affia, Raimundas Matulevičius, Alexander Nolte	UTARTU	27th International Conference on Cooperative Information Systems	10.1007/978-3-030-33246-4_18

No.	Title (SP/Dataset)	Authors/Owners	Partner	Journal/ Conference	DOI (publisher)
5	Towards Privacy and Secure IoT Services Based on Privacy-Enhancing Technologies	Lukas Malina	BUT	International Workshop on Secure Internet of Things 2019 (SIOT) in conjunction with ESORICS 2019	-
6	CFI: Control Flow Integrity or Control Flow Interruption?	Paolo Prinetto and Gianluca Roascio	CINI	PHISIC 2019 Workshop	10.1109/EWDTS.2019.8884464
7	Experimental analysis of the laser-induced instruction skip fault model	Jean-Max Dutertre, Timothe´ Riom, Olivier Potin, and Jean-Baptiste Rigaud	IMT	2019 FDTC workshop	10.1007/978-3-030-35055-0_14
8	Big Data Analytics for Intrusion Detection: An Overview	Luis Dias, Miguel Correia	IST and INOV		10.4018/978-1-5225-9611-0.ch014
9	OutGene: Detecting Undefined Network Attacks	Luís Dias, Hélder Reia, Rui Neves and Miguel Correia	IST		10.1007/978-3-030-36938-5_12

No.	Title (SP/Dataset)	Authors/Owners	Partner	Journal/ Conference	DOI (publisher)
	with Time Stretching and Genetic Zooms				
10	Visual Analytics for Cyber Security Domain: State-of-the-Art and Challenges	R. Damaševičius, J. Toldinas, A. Venčkauskas, S. Grigaliūnas, N. Morkevičius, V. Jukavičius	KTU		10.1007/978-3-030-30275-7_20
11	The feasibility of Deep learning use for adversarial model extraction in the cybersecurity domain	Pawlicki, Choras and Kozik	ITTI	IDEAL'19	10.1007/978-3-030-33617-2_36
12	On Computer - Aided Techniques for Supporting Safety and Security Co-Engineering	Vivek Nigam, Antonaneta Kondeva, Carmen Carlan and Harald Ruess	FTS	9th IEEE International Workshop on Software Certification (WoSoCer)	http://nigam.info/docs/wosocer02.pdf

No.	Title (SP/Dataset)	Authors/Owners	Partner	Journal/ Conference	DOI (publisher)
13	Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols	Guillaume Celosia, Mathieu Cunche	INRIA	PoPETs2020 (https://www.petsymposium.org/)	10.2478/popets-2020-0003
14	Fingerprinting Bluetooth-Low-Energy Devices Based on the Generic Attribute Profile	Guillaume Celosia, Mathieu Cunche	INRIA	IoT S&P 2019	10.1145/3338507.3358617
15	Saving Private Addresses: An Analysis of Privacy Issues in the Bluetooth-Low-Energy Advertising Mechanism	Guillaume Celosia, Mathieu Cunche	INRIA	Mobiquitous 2019	10.1145/3360774.3360777
16	Towards Formal Methods of IoT Application Layer Protocol	Katharina Hofer-Schmitz and Branka Stojanovic	JR	12th CMI Conference 2019: cybersecurity and privacy	

No.	Title (SP/Dataset)	Authors/Owners	Partner	Journal/ Conference	DOI (publisher)
17	Automated Security Analysis of IoT Software Updates	Nicolas Dejon, Davide Caputo, Luca Verderame, Alessandro Armando and Alessio Merlo	CINI	13th WISTP International Conference on Information Security Theory and Practice	https://www.researchgate.net/publication/337592102_Automated_Security_Analysis_of_IoT_Software_Updates
18	Natural Projection as Partial Model Checking	Costa, G.; Galletta, L.; Degano, P.; Basin, D.; Bodei, C.	CINI	Journal of Automated Reasoning	https://arpi.unipi.it/handle/11568/1013170
19	WAF-A-MoLE: An adversarial tool for assessing ML-based WAFs	Luca Demetrio, Gabriele Costa, Andrea Valenza and Giovanni Lagorio	CINI	SoftwareX and on ACM Symposium on Applied Computing	https://doi.org/10.1016/j.softx.2019.100367
20	A Survey on Multi-Factor Authentication for Online Banking in the Wild		CINI	Computers and Security	
21	Building Next Generation		CINI	Computers and Security	

No.	Title (SP/Dataset)	Authors/Owners	Partner	Journal/ Conference	DOI (publisher)
	Cyber Ranges with CRACK				
22	Secure Firmware Updates for Constrained IoT Devices Using Open Standards: A Reality Check	K. Zandberg, K. Schleiser, F. Acosta, H. Tschofenig, and E. Baccelli	INRIA	IEEE Access, June 2019	10.1109/ACCESS.2019.2919760
23	Cyberphysical Security for the Masses: A Survey of the Internet Protocol Suite for Internet of Things Security	H. Tschofenig, E. Baccelli	INRIA	IEEE Security & Privacy, October 2019	10.1109/MSEC.2019.2923973
24	Requirements for a Lightweight AKE for OSCORE	M. Vucinic, G. Selander, J. Mattsson, D. Garcia	INRIA	IETF Internet Draft, 2019	https://tools.ietf.org/id/draft-selander-lake-reqs-02.html
25	Advances in Usability of Formal Methods for Code Verification with Frama-C	André Maroneze, Valentin Perrelle, Florent Kirchner	CEA	Interactive Workshop on the Industrial Application of Verification and Testing, ETAPS 2019 Workshop (InterAVT 2019)	http://dx.doi.org/10.14279/tuj.eceasst.77.1108

No.	Title (SP/Dataset)	Authors/Owners	Partner	Journal/ Conference	DOI (publisher)
26	Privacy-preserving and yet Robust Collaborative Filtering Recommender as a Service	Qiang Tang	LIST	Inscrypt 2019 — The 15th International Conference on Information Security and Cryptology	https://arxiv.org/abs/1910.03846v1
27	A Privacy-Enhancing Framework for Internet of Things Services	Lukas Malina, Gautam Srivastava, Petr Dzurenda, Jan Hajny and Sara Ricci	BUT	13th International Conference on Network and System Security	10.1007/978-3-030-36938-5_5
28	xMP: Selective Memory Protection for Kernel and User Space	Sergej Proskurin, Marius Momeu, Seyedhamed Ghavamnia, Vasileios P. Kemerlis, and Michalis Polychronakis	TUM	IEEE S&P 2020	https://www3.cs.stonybrook.edu/~mikepo/papers/xmp.sp20.pdf
29	TSNSCHED: Automated Schedule Generation for	Aellison Cassimiro T. dos Santos, Ben Schneider	FTS	FMCAD	10.23919/FMCAD.2019.8894249

No.	Title (SP/Dataset)	Authors/Owners	Partner	Journal/ Conference	DOI (publisher)
	Time Sensitive Networking	and Vivek Nigam			
30	MadDroid: Characterising and Detecting Devious Ad Content for Android Apps	Tianming Liu, Haoyu Wang, Li Li, Xiapu Luo, Feng Dong, Yao Guo, Liu Wang, Tegawendé F. Bissyandé and Jacques Klein	SnT	The WebConf 2020	
31	Methodology and Feedback about Systematic Cybersecurity Experts Auditing in Belgium	Christophe Ponsard, Jeremy Grandclaudon and Nicolas Point	CETIC	ICISSP 2020 conference	

Table 10 - List of Accepted articles

5.1.3 Closing the Gender Gap Campaigns

Women's day campaign

A first action – a women's day campaign dedicated to the women involved in SPARTA - has already been deployed. The Women's Day campaign consisted of two publications presenting Claudia Eckert and Regina Valutytè, members of SPARTA, and a video explaining the State of the art related to the gender gap in cybersecurity. Taking into account that at the time of the publications SPARTA project had just started its communication activities on social media, the number of people that were reached by this campaign is significant. On twitter, SPARTA was able to reach, on average 4000 impressions (number of times people have seen the post) and 57 interactions with the post. On LinkedIn, the publications reach an average of 530 impressions, a total of 28 reactions and 7% of engagement. On Instagram, this campaign was able to reach 138 views, 16 visits to SPARTA profile and an average of 240 impressions. The main objectives of the campaign were to communicate to our audiences the SPARTA position on gender gap issues and to raise awareness on the need to gather efforts to attract women to the cybersecurity field.

" Women4Cyber "

SPARTA is currently involved in the " Women4Cyber " LinkedIn Group where gender balance issues in cybersecurity and the strategies to solve them are discussed, ideas, experiences, and knowledge is shared. "Women4Cyber" is an EU-wide initiative, launched by the European Cyber Security Organisation (ECSO), to promote and support the participation of women in cybersecurity, under the patronage of Mariya Gabriel, European Commissioner for Digital Economy and Society.

SPARTA is also part of the women4cyber mailing list aiming at integrating the Women4Cyber inside meetings and activities, to better tackle the issues associated with gender balance in cybersecurity.

ACM Celebration of Women in Computing: womENcourage 2019

SPARTA attended the ACM womENcourage 2019 event on the 16th September in Italy, Rome.

WomENcourage brings together women in the computing profession and related technical fields to exchange knowledge and experience and provide special support for women who are pursuing their academic degrees and starting their careers in computing. SPARTA engaged with the attendees to understand some of their main concerns and opinions regarding female participation in the cybersecurity field. SPARTA attended some of the workshops, technical talks and panel discussions. SPARTA disseminated some of the event activities through social media, promoting awareness on the topic of female participation in cybersecurity.

Awareness games at leHack 2019

SPARTA attended "leHACK" 2019, one of the oldest French underground hackers' event which brings together professionals, and amateurs around conferences, workshops, lectures and challenges. More than presenting SPARTA project at the event, a booth was prepared with a set of five challenges to engage with the attendees. All challenges were disseminated on SPARTA social media accounts, as well as their solutions. One of the challenges was related to the importance of having diversity within cybersecurity teams:

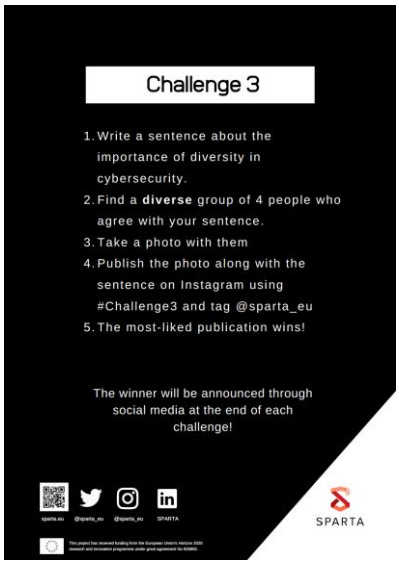


Figure 4 - Challenge addressing diversity in cybersecurity

5.1.4 Engagement of the Outermost Regions of Europe

Regarding action 1 – *Encourage small businesses to adopt cybersecurity measures* (the Caribbean and South America OR) – Martinique island was chosen to be part of the campaign, namely with the Technopole Martinique organisation, that supports innovation initiatives to make Martinique a territory of excellence and offer businesses a favourable environment. The first contact with Martinique was made and a formal presentation is being prepared.

Regarding action 2 – *Stimulate young people to undertake studies or training at the university level within the area of cybersecurity* (Atlantic Ocean OR) **–** Las Palmas de Gran Canaria island was chosen to be part of the campaign, namely the Universidad de Las Palmas de Gran Canaria. A first meeting with the Director of the Informatic Engineering school of the Universidad de Las Palmas de Gran Canaria, Professor Oliverio Santana Jaria was conducted on Wednesday, October 23rd from 10:30 to 12:30. Professor Daniel Hernandez, Professor Francisco Alayon (Computer Network) and Professor Antonio Ocon were present in the meeting. The location was the School's meeting room. The meeting was conducted by Elisabete Carreira, John Rodrigues and Catarina Valente, from INOV.

Regarding action 3 – *Engage with critical infrastructure operators to stimulate them to adopt state-of-the-art. cybersecurity technology* (Indian Ocean OR): The island of La Réunion was chosen, namely the Water Critical Infrastructure Office de L'eau. The first meeting was held on the 14th of November, at Office de L'eau (OE) in La Réunion, conducted in French and introduced by CEA, remotely. The meeting attendees were the Director – Gilbert Sam Yin Yang – the Deputy Director – Faiçal Badat – the Director of Information and Modernization of Services – Yohann Cimbaro – The Head of Service Information Systems and Working Conditions – Olivier Chane Kane – and the Computer scientist and Data Protection Officer - Olivier Sampoil.

For the next steps, there is currently being prepared a Non-Disclosure Agreement to formalize Office de l'eau participation in the Go Cyber with SPARTA campaign; a brief questionnaire to collect their cybersecurity needs; and a formal invitation to have OE on board as an Associate.

A 1st Aid Cybersecurity Kit for Water Critical Infrastructures was deployed and delivered to Office de l'eau.

5.2 Monitoring C&D Instruments

5.2.1 SPARTA Official Website

The SPARTA official website is available since M04 (April 2019) and has been evolved during this reporting period. Here we present the number of unique visitors per month where we can highlight the growth of visitors from June to October due to the awareness campaigns promoting the SPARTA Project among our target audiences, mainly through events and social media official accounts.

Apr 2019	May 2019	Jun 2019	Jul 2019	Aug 2019	Sep 2019	Oct 2019	Nov 2019	Dez 2019	Jan 2019
518	563	960	974	792	1 122	1 265	1,103	-	1351 (17th – 21st)

5.2.2 SPARTA Social Media

A general overview of the results taken from all the C&D activities carried out in the first year of the project on SPARTA social media reveals a positive outcome. SPARTA social media accounts achieved 715 Followers on Twitter, 235 followers on LinkedIn and 127 followers on Instagram. Annex 1 and 2 summarize SPARTA activities on these social media networks.

The C&D activities carried out during the first year of the project on the SPARTA official social media accounts contributed to promoting awareness of SPARTA and cybersecurity among our targeted audiences. Those actions enabled SPARTA to build a community that is now engaged with the project. Mapping audiences is of utmost importance as allows a conscious construction of communication campaigns that take into account the informational needs and characteristics of our community. Below are the main features of our audiences on social media:

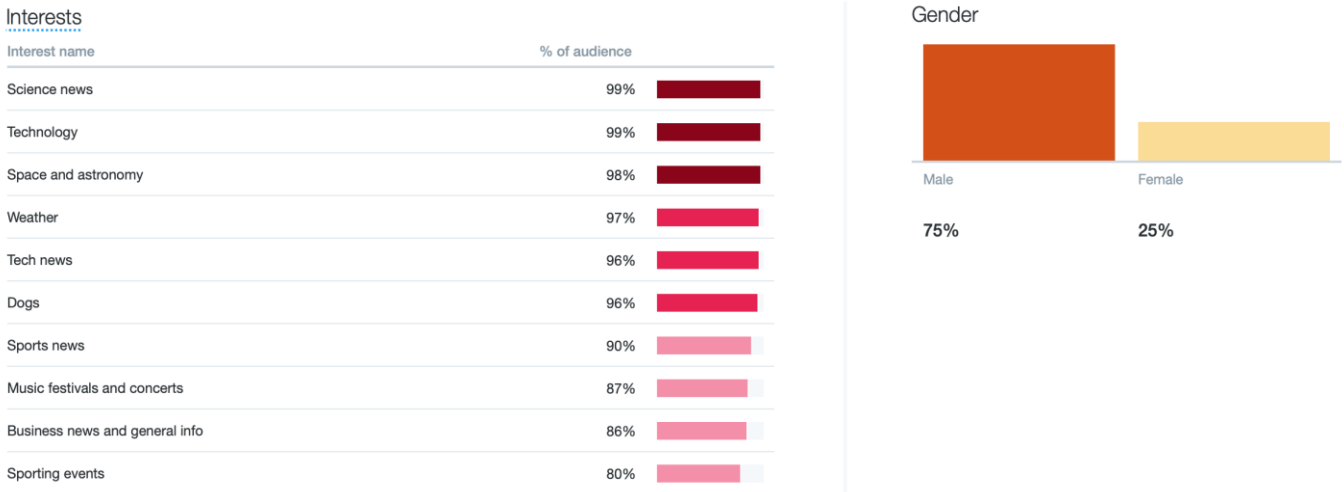


Figure 5 - Twitter Audience

The gender gap among SPARTA audiences is currently 25% female – 75% male on Twitter and 38% female – 62% male on Instagram. The second year of the project aims to reduce this gap.

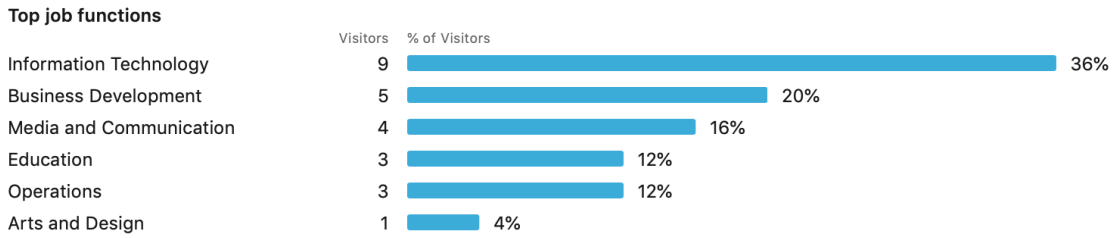


Figure 6 - LinkedIn Audiences

Our audience is mainly interested in science news and technology but people interested in a more diverse kind of subjects also constitute SPARTA audience, as depicted in Figure 4 – Twitter Audience and Figure 5 – LinkedIn Audience.

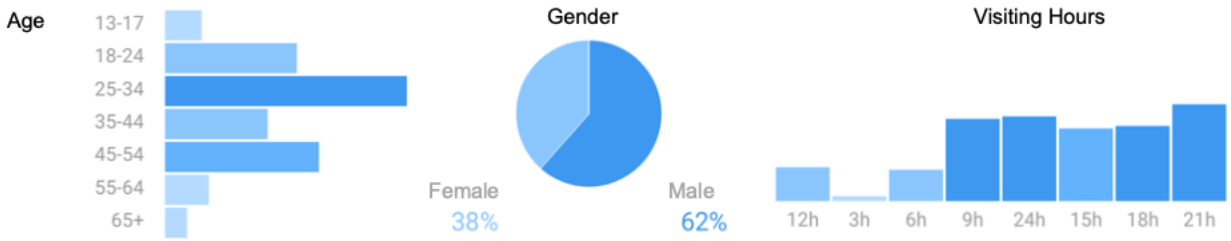


Figure 7 - Instagram Audiences

SPARTA's audiences age ranges mainly between 18 and 54 years old. The data relative to the visiting hours allows wise scheduling of future publications, ideally between 18:00 hours and 21:00 hours.

SPARTA has built a community on social media where audiences expect to be updated with the latest achievements of the SPARTA project as well as informed on the cybersecurity state-of-the-art. The information deployed by our publications must appeal to SPARTA's audiences and attract new followers so that the project can gain more visibility. To reach a more significant spectrum of audience, SPARTA will produce more diverse messages and take into account different informational needs, references and sources. There is a need to improve the frequency and quality of information shared on the three social media platforms (Twitter, Instagram, and LinkedIn). To address such need, a high-level strategy is deployed above in this deliverable.

5.2.3 Media Relations

An initial press release (Figure 6) was produced and published on the SPARTA Official website as well as widely published on partners official websites. Below is a list of major SPARTA presence in the media relative to the first year of the project, with the respective links to publication:

SPARTA PRESS RELEASE

PLACE, DATE: EUROPEAN UNION, 26/02/2019

SPARTA — Re-imagining the way cybersecurity research, innovation, and training are performed in the European Union

Cybersecurity is an urgent and major societal challenge. Highly correlated with the digitalization of our societies, cyberthreats have an increasing impact on our lives. It is therefore essential to ensure digital security and strategic autonomy of the EU by strengthening leading cybersecurity capacities. This challenge will require the coordination of Europe's best competences, towards common research and innovation goals.

SPARTA is a novel Cybersecurity Competence Network, supported by the EU's H2020 program, with the objective to develop and implement top-tier research and innovation collaborative actions. Strongly guided by concrete challenges forming an ambitious Cybersecurity Research & Innovation Roadmap, SPARTA will setup unique collaboration means, leading the way in building transformative capabilities and forming a world-leading Cybersecurity Competence Network across the EU. From basic human needs (health) to economic activities (energy, finance, and transport) to technologies (ICT and industry) to sovereignty (eGovernment, public administration), four research and innovation programs will push the boundaries to deliver advanced solutions to cover emerging challenges.

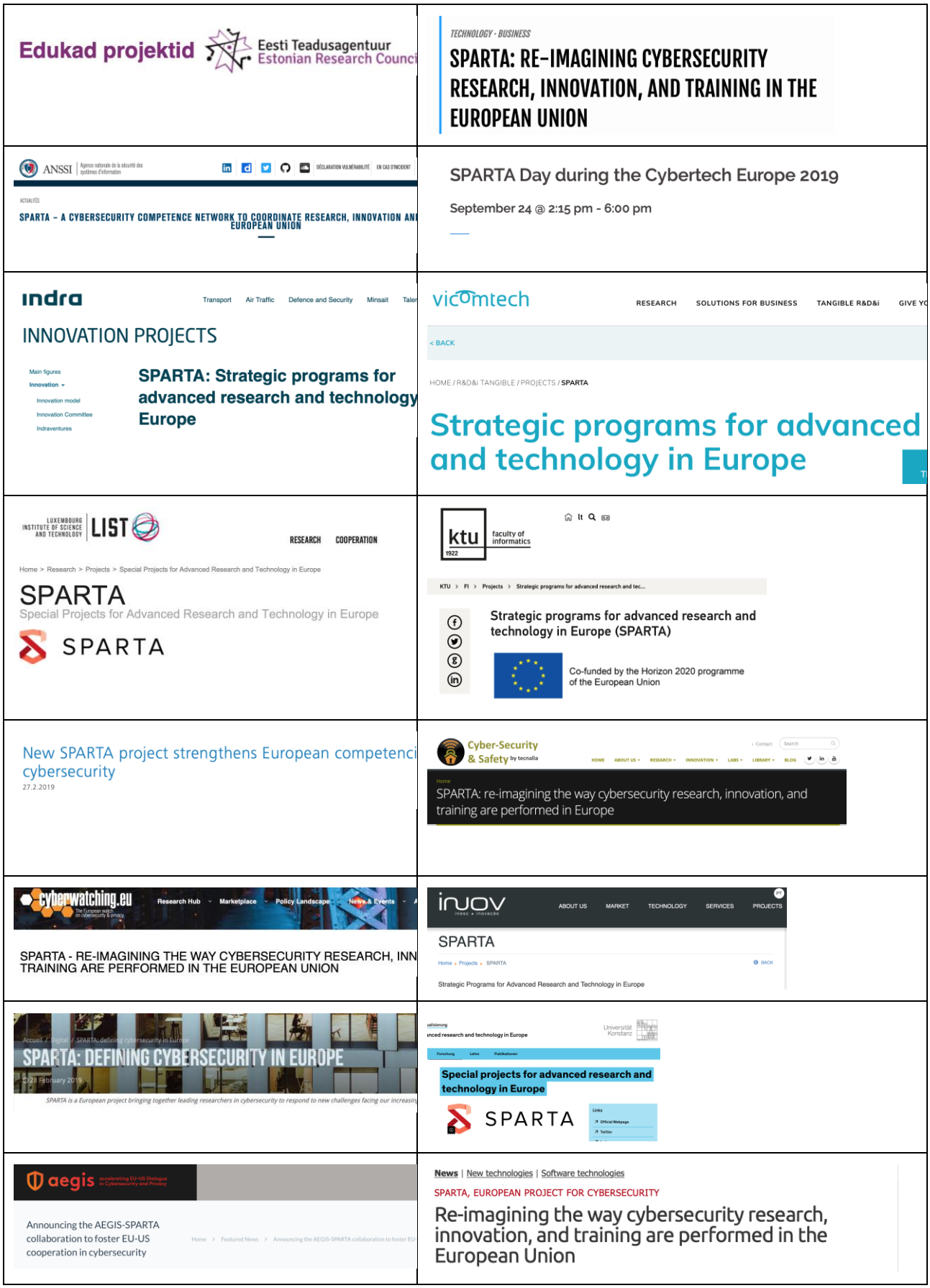
The SPARTA consortium, led by CEA, assembles a balanced set of 44 actors from 14 EU Member States at the intersection of scientific excellence, technological innovation, and societal sciences in cybersecurity. Together, along with SPARTA Associates, they aim at re-imagining the way cybersecurity research, innovation, and training are performed in Europe across domains and expertise, from foundations to applications, in academia and industry.

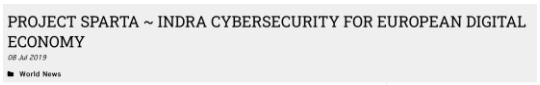
In sharing experiences and excellence, challenges and capabilities, SPARTA makes decisive contributions to European strategic autonomy.

sparta.eu
@sparta_eu
contact@sparta.eu
SPARTA

This proposal has been retained for funding from the European Union's Horizon 2020 research and innovation programme.

Figure 8 - SPARTA Press Release


Edukad projektid
Eesti Teadusagentuur
Estonian Research Council
TECHNOLOGY · BUSINESS
SPARTA: RE-IMAGINING CYBERSECURITY RESEARCH, INNOVATION, AND TRAINING IN THE EUROPEAN UNION
ANSSI
SPARTA – A CYBERSECURITY COMPETENCE NETWORK TO COORDINATE RESEARCH, INNOVATION AN
EUROPEAN UNION
SPARTA Day during the Cybertech Europe 2019
September 24 @ 2:15 pm - 6:00 pm
indra
Transport
Air Traffic
Defence and Security
Minsait
INNOVATION PROJECTS
Main figures
Innovation
Innovation model
Innovation Committee
Indraventures
SPARTA: Strategic programs for advanced research and technology
Europe
vicomtech
RESEARCH
SOLUTIONS FOR BUSINESS
TANGIBLE R&D&i
< BACK
HOME / R&D&i TANGIBLE / PROJECTS / SPARTA
Strategic programs for advanced and technology in Europe
LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY
LIST
RESEARCH
COOPERATION
Home > Research > Projects > Special Projects for Advanced Research and Technology in Europe
SPARTA
Special Projects for Advanced Research and Technology in Europe
SPARTA
ktu
faculty of informatics
1922
KTU > FI > Projects > Strategic programs for advanced research and tec...
Strategic programs for advanced research and technology in Europe (SPARTA)
Co-funded by the Horizon 2020 programme of the European Union
New SPARTA project strengthens European competenci
cybersecurity
27.2.2019
Cyber-Security & Safety by tecnalia
HOME
ABOUT US
RESEARCH
INNOVATION
LABS
LIBRARY
BLOG
Home
SPARTA: re-imagining the way cybersecurity research, innovation, and training are performed in Europe
cyberwatching.eu
The European watch on cybersecurity & privacy
Research Hub
Marketplace
Policy Landscape
News & Events
SPARTA - RE-IMAGINING THE WAY CYBERSECURITY RESEARCH, INN
TRAINING ARE PERFORMED IN THE EUROPEAN UNION
inov
inesc inovação
ABOUT US
MARKET
TECHNOLOGY
SERVICES
PROJECTS
SPARTA
Home › Projects › SPARTA
BACK
Strategic Programs for Advanced Research and Technology in Europe
SPARTA: DEFINING CYBERSECURITY IN EUROPE
28 February 2019
SPARTA is a European project bringing together leading researchers in cybersecurity to respond to new challenges facing our increasin
Universität Konstanz
Special projects for advanced research and technology in Europe
SPARTA
Official Webpage
Twitter
aegis
accelerating EU-US Dialogue in Cybersecurity and Privacy
Announcing the AEGIS-SPARTA collaboration to foster EU-US cooperation in cybersecurity
News | New technologies | Software technologies
SPARTA, EUROPEAN PROJECT FOR CYBERSECURITY
Re-imagining the way cybersecurity research, innovation, and training are performed in the European Union

	
	
http://spazio-news.it/cybertech-spazio-news-proud-announce-a-media-partnership-cybertech-europe-2019	EUVATION (Where SPARTA Podcats have been stored): https://omny.fm/shows/euvation/sparta-h2020-project-cyber-security-in-the-eu-pa-1

SPARTA was highlighted on SIC Magazine as self- explained in the figure bellow:

Figure 9 - SPARTA on SIC Magazine

5.2.4 Project leaflet

The general project leaflet integrates the SPARTA project activities, and has been delivered in several events with a significant outreach.

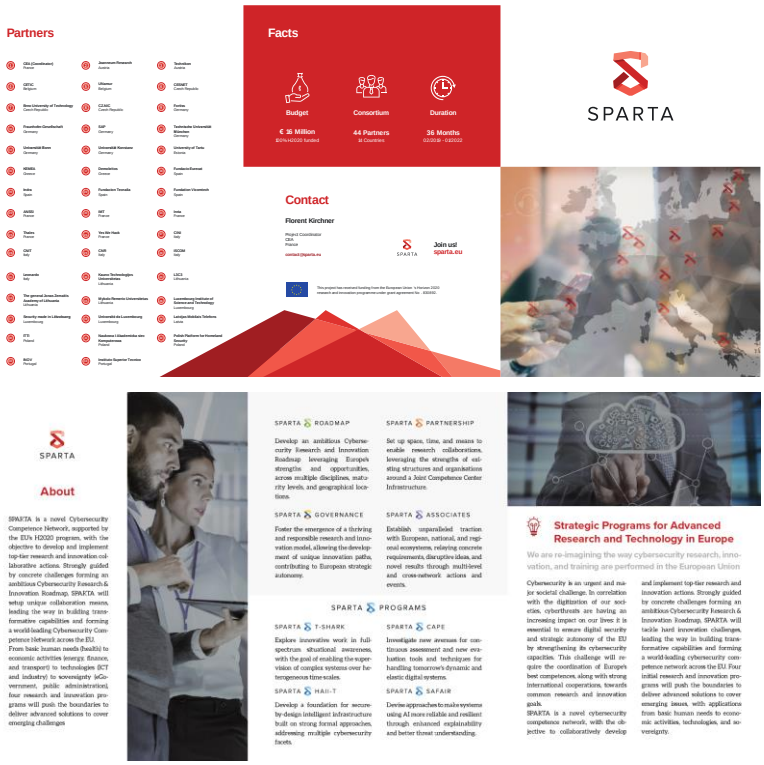


Figure 10 - Updated project leaflet

5.2.5 Podcasts

Podcasts are being published on social media and will soon be published on the website (which will serve as a repository). The 1st and 2nd SPARTA Podcasts were disseminated on social media and are available at:

- SPARTA H2020 project: Cyber Security in the EU (part one)
- https://t.co/hbglUdPxwS?amp=1
  - The first SPARTA podcast was downloaded 155 times
- SPARTA H2020 project: Cyber Security in the EU (part two)
- https://t.co/OL2sAXdTGQ?amp=1
  - The second SPARTA podcast was downloaded 56 times
- SPARTA H2020 project: Cyber Security in the EU (part three) has just been released.

5.2.6 Videos

Three videos (SPARTA presentation video, cybersecurity market video and women in cybersecurity video) have been created within the project launch campaign on social media, including a video for the presentation of the project. Video has shown to be a tool that promotes audiences engagement and curiosity. Videos are the publications on social media with a higher engagement rates. Below are some of the video dissemination results:

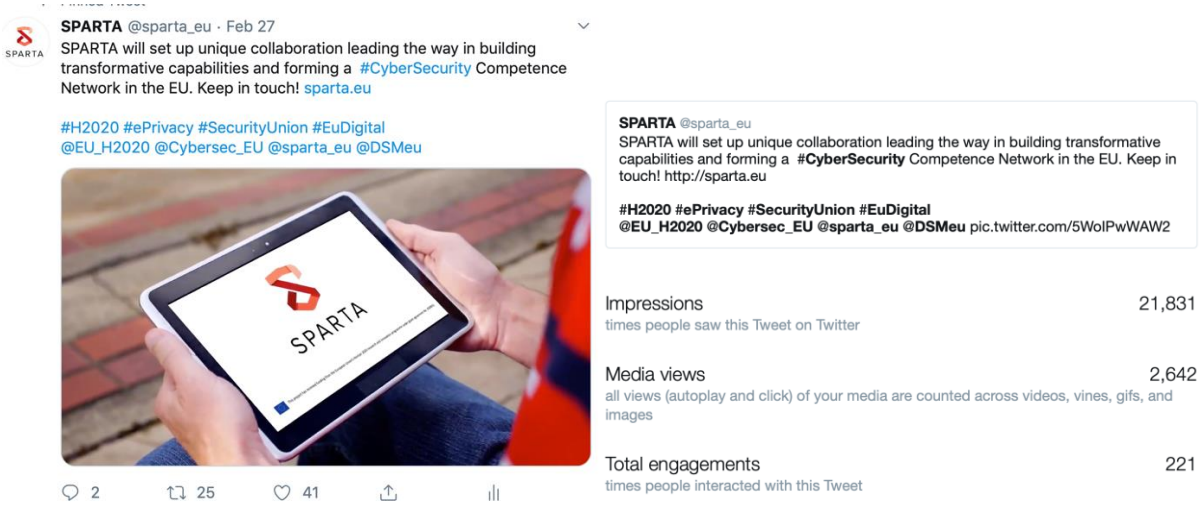


Figure 11 - SPARTA Presentation Video Dissemination results on Twitter

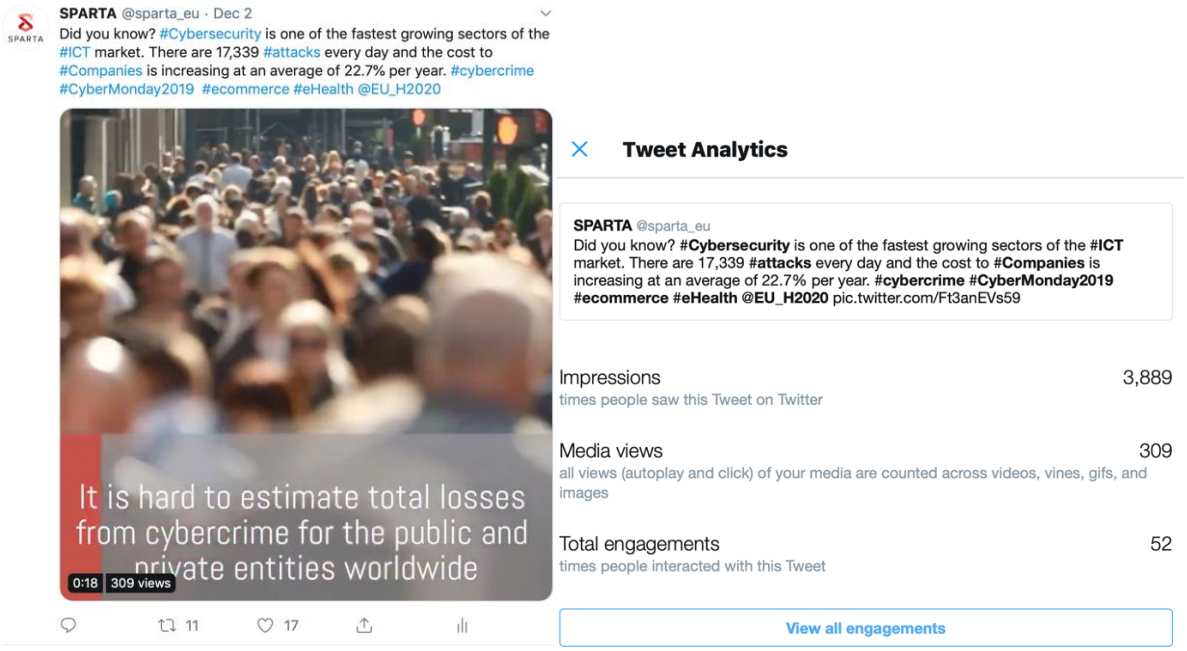


Figure 12 - Cybersecurity market Video Results on Twitter

5.2.7 SPARTA Merchandise

SPARTA products have been delivered on SPARTA day held in Rome at Cybertech 2019 and have received a positive feedback from SPARTA partners.

5.3 First-year general evaluation

A general overview of the results taken from all the C&D activities carried out in the first year of the project reveals that the major communication objectives established in the deliverable 12.1 were achieved.

The diversity of actors that is inherent to the SPARTA project enhances the possibility of outreach to a broader set of audiences across geographies. Through the several communication actions promoted - such as workshops, SPARTA Days, conferences and talks - and through the

communication materials deployed - such as leaflets, podcasts, Roll-ups, SPARTA website, and the official social media platforms - it has been possible to (1) inform the various key audiences about SPARTA project; (2) Enhance awareness about cybersecurity and the importance of this project; (3) Engage the audiences with SPARTA project.

These C&D actions were also instrumental in fostering sustained collaborations with academic, industrial, governmental, and community stakeholders, namely by the launching of the Associates and Friends Programs. The “Go Cyber with SPARTA” campaign also promoted fostering collaborations with, at the moment, two outermost regions of Europe, enhancing the diversity and inclusion pillars of the project.

Regarding social media accounts, they have allowed SPARTA to communicate its main messages, promoting engagement with its audiences and build a sustained community of followers.

Some fractions of the overall strategy must have more considerable attention in the coming year, namely the Internal Communication which, due to its inherent complexity and the large number of partners involved in the project, have been facing some roadblocks. Measures will be taken to leverage a simple and fluid communication between all partners.

Because WP12 is committed to addressing gender and diversity issues in the field of cybersecurity, it is essential to look at our audience in terms of gender. The gender gap existing on our social media audience as well as at the SPARTA events is significant, thus a factor to be taken into account and to carefully address in the upcoming year.

The Awareness axis was structural in the first year and will still be in the coming years, along with the emergence of the participation axis and in a more advanced phase, the emergence of the action axis.

Chapter 6 Summary and Conclusion

The present deliverable provides an update of the Deliverable 12.1 Communication and Dissemination Activities and its evaluation.

In what regards major changes related to the previous deliverable, they have been made aiming to ensure the maximization of the planned activities, enhancing a strong and holistic communication, taking into account all SPARTA stakeholders. Such changes are a result of the plan evaluation and update, reflecting its continuous assessment and improvement.

Main changes can be summarized as the following:

- **Official SPARTA Website:** The website has been under major changes to ensure a friendly user characteristic and to facilitate the storage of public information. SPARTA website is now more dynamic, with dedicated pages to the main pillars of the Project: The Roadmap, the Programs, the Challenges SPARTA is addressing and its results (e.g. scientific publications and podcasts). A news section was also added to keep the visitors updated with SPARTA achievements and events.

- **Internal Communication:**

  - **The use of Stacked**, a tool that allows easier collaboration between partners, sharing tasks and documents. Stackfield provides rooms dedicated to each WP, thus simplifying the exchange of ideas and practical information.
  - **The bi-monthly internal newsletter** created to raise awareness on what is happening within each WP and to enhance the sense of community.

- **Partners involvement in Communication actions on social media:**

  - **Weekly publications managed by partners** allows a more holistic set of publications, feeding the different audiences informational needs and keeping track of a more comprehensive media agenda on the cybersecurity field, from different countries.
  - **Social media content management tool:** The social media content management tool will be selected to better coordinate and manage all publications efficiently. This tool will allow for streamlined teamwork to organize, schedule and publish content effortlessly to all SPARTA social media accounts, whenever a conference, meeting or any public event occurs. With the objective of keeping audiences involved with the contents permanently.

Gender and diversity issues have also been addressed in this deliverable, regarding SPARTA coordinate efforts to promote diversity practices and awareness on the subject.

SPARTA Communication and Dissemination plan provides a strategic basis for the development of successful C&D activities. The following year will have stronger attention to the **participation axis** as to promote the participation of different actors across disciplines, maturity levels and geographies in the SPARTA project.

Annex 1 – Twitter analytics

Feb 2019 • 28 days

TWEET HIGHLIGHTS

Top Tweet earned 9,679 impressions

SPARTA will set up unique collaboration leading the way in building transformative capabilities and forming a **#CyberSecurity** Competence Network in the EU. Keep in touch! sparta.eu

#H2020 #ePrivacy #SecurityUnion #EuDigital @EU_H2020 @Cybersec_EU @sparta_eu @DSMeu pic.twitter.com/5WoIPwWAW2

2 23 40

View all Tweet activity

View Tweet activity

Top Follower followed by 42.4K people

ANSSI
@ANSSI_FR FOLLOWS YOU
Tous connectés, tous impliqués, tous responsables - Agence nationale de la sécurité des systèmes d'information - Contact : communication@ssi.gouv.fr

View profile View followers dashboard

Top mention earned 195 engagements

ANSSI
@ANSSI_FR · Feb 26

L'ANSSI est ravie de participer au nouveau réseau de compétence **@sparta_eu**, soutenu par le programme européen **#H2O2O** pour coordonner la recherche, l'innovation et la formation en matière de cybersécurité au sein de l'UE. **#cybersecurity #ePrivacy**
ssi.gouv.fr/actualite/spar…
pic.twitter.com/AQT7miMpv5

3 38 72

View Tweet

Top media Tweet earned 4,122 impressions

The SPARTA consortium assembles a balanced set of 44 actors from 14 EU Member States at the intersection of scientific excellence, technological innovation, and societal sciences in **#cybersecurity**.

#H2020 #SecurityUnion #EuDigital #ePrivacy @EU_H2020 @Cybersec_EU @DSMeu
pic.twitter.com/j6up9c5d3X

10 27

FEB 2019 SUMMARY

Tweets	Tweet impressions
6	36.2K
Profile visits	**Mentions**
415	22
New followers	
214	

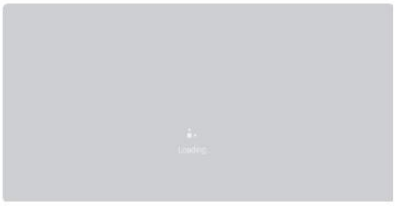
Mar 2019 • 31 days

TWEET HIGHLIGHTS

Top Tweet earned 5,900 impressions

Together we aim at re-imagining the way **#cybersecurity #research**, **#innovation** and training are performed in the 🇪🇺. Across domains and expertise, from foundations to applications, in academia and industry.

#H2020 #ePrivacy #SecurityUnion #EuDigital
@EU_H2020 @Cybersec_EU @DSMeu
pic.twitter.com/zmqKDCJ1XW



1 10 20

View all Tweet activity

View Tweet activity

Top Follower followed by 114K people

Horizon 2020 🇪🇺
@EU_H2020 FOLLOWS YOU
Official DG Research & Innovation account for EU's **#H2020** & future **#HorizonEU** research & innovation prog. Follow **@EUScienceInnov @GabrielMariya @JEPaquetEU**

View profile View followers dashboard

Top mention earned 484 engagements

CyberSec_EU 🇪🇺
@Cybersec_EU · Mar 13

#HappeningNow in **#Strasbourg**: Commissioner **@GabrielMariya** is meeting with **@concordiah2020 @sparta_eu @ECHOcybersec @CyberSec4Europe** to inform the pilots about our **#Cybersecurity** research & policy initiatives & how they can assist **#EU** in strengthening our cybersecurity capacity
pic.twitter.com/oUhxWTG7nX

1 35 70

View Tweet

Top media Tweet earned 5,274 impressions

Globally, corporations and government agencies are increasingly more aware of risks stepping up to protect their **#intellectualproperty** and **#sensitivedata**.

#H2020 #ePrivacy #cybersecurity #SecurityUnion #EuDigital
@EU_H2020 @Cybersec_EU @DSMeu
pic.twitter.com/2Xx2rQpMX0

18 25

View all Tweet activity

MAR 2019 SUMMARY

Tweets	Tweet impressions
17	59.9K
Profile visits	**Mentions**
1,289	73
New followers	
158	

Apr 2019 • 30 days

TWEET HIGHLIGHTS

Top Tweet earned 18.8K impressions

Don't miss workshop on **@sparta_eu** project with an open discussion on Coordinated Vulnerability Disclosure. Session co-organised by **@yeswehack** and **@IndraCompany** at **@mundohackertv** Day.

24 April - 10:30 CET

#H2020 #EuDigital #cybersecurity @Cybersec_EU
pic.twitter.com/mVG2IWDkY3

15 28

View all Tweet activity

View Tweet activity

Top mention earned 140 engagements

Don't miss workshop on **@sparta_eu** project with an open discussion on Coordinated Vulnerability Disclosure. Session co-organised by **@yeswehack** and **@IndraCompany** at **@mundohackertv** Day.

24 April - 10:30 CET

#H2020 #EuDigital #cybersecurity @Cybersec_EU
pic.twitter.com/mVG2IWDkY3

15 28

View all Tweet activity

View Tweet activity

APR 2019 SUMMARY

Tweets 3	Tweet impressions 41.9K
Profile visits 425	Mentions 38
New followers 50	

Top Follower followed by 16.2K people

CEA_Officiel
@CEA_Officiel FOLLOWS YOU
Compte officiel du CEA. **#recherche** et **#innovation** pour l'**#industrie** : **#TransitionEnergétique**, **#médecinedufutur**, **#transformation #numérique**, **#défense #sécurité**.

View profile View followers dashboard

Top media Tweet earned 2,731 impressions

Meet SPARTA Coordinator, **@__ftk**, director of **#cybersecurity #program** at **@CEA_List**.

#H2020 #SecurityUnion @EU_H2020 @Cybersec_EU @DSMeu pic.twitter.com/06kmM6vK8D

7 30

May 2019 • 31 days

TWEET HIGHLIGHTS

Top Tweet earned 14.3K impressions

The first SPARTA project Podcast is now available omny.fm/shows/euvation… Follow the link or search for EUVATION wherever you get your podcasts! Listen and subscribe to stay current with developments in SPARTA **#H2020 #EuDigital #cybersecurity** # **@EU_H2020 @euvation**

9 18

View all Tweet activity

View Tweet activity

Top Follower followed by 9,841 people

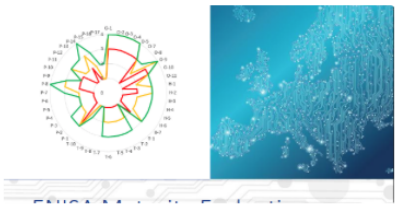
Rollo Davies MSyl
@SecurityRollo FOLLOWS YOU
Managing Editor: The Professional Security Officer mag. Brand Ambassador: Wagestream. Named World #2 Influencer in Security Thought Leadership by IFSEC Global.

View profile View followers dashboard

Top mention earned 61 engagements

Yes We Hack ⁖
@yeswehack · May 2

#Assessment
@enisa_eu Maturity Evaluation Methodology for CSIRTs europa.eu/!PK76yk **#CVD #vulnerabilitymanagement #CERT** cc **@sparta_eu @iotcert**
pic.twitter.com/uq9AdUTvwd



4 7

View Tweet

Top media Tweet earned 1,558 impressions

Want to know more about cryptographic algorithms and secure multi-party computation? **@VUTvBrne** invites you to Brno Security Meetings with **@sparta_eu** and **@CyberSec4Europe** projects. 24 April - 17:00 CET

#H2020 #EuDigital #cybersecurity #Crypto #computing
@Cybersec_EU pic.twitter.com/qiMBbx2qiL

6 15

View all Tweet activity

View Tweet activity

MAY 2019 SUMMARY

Tweets	Tweet impressions
3	41.7K
Profile visits	**Mentions**
186	9
New followers	
22	

Jun 2019 • 30 days

TWEET HIGHLIGHTS

Top Tweet earned 3,324 impressions

The 4 pilots coming to you soon! SPARTA, **@concordiah2020** **@ECHOcybersec** and **@CyberSec4Europe** together to prepare a European Competence Network of Cybersecurity Centres of Excellence.

Stay tuned!

#EU
#h2020
#CyberSecurity
pic.twitter.com/HkwGQ17gq3

16 20

View all Tweet activity

View Tweet activity

Top Follower followed by 26.5K people

halvarflake
@halvarflake FOLLOWS YOU
I do math. And was once asked by R. Morris Sr. : "For whom?" At the moment, for https://t.co/zr0Qzl2a13

View profile View followers dashboard

Top mention earned 181 engagements

Shahid Raza
@shahidraza · Jun 5

A step towards bringing the 4 cybersecurity excellence network pilots together: the launch of a common website during the **@concordiah2020** general assembly in Brussels.
cybercompetencenetwork.eu
@ECHOcybersec **@sparta_eu**
@CyberSec4Europe
@DespinaSpanou **@ecso_eu**
@Cybersec_EU
pic.twitter.com/mPdL5NO959

15 27

View Tweet

Top media Tweet earned 3,101 impressions

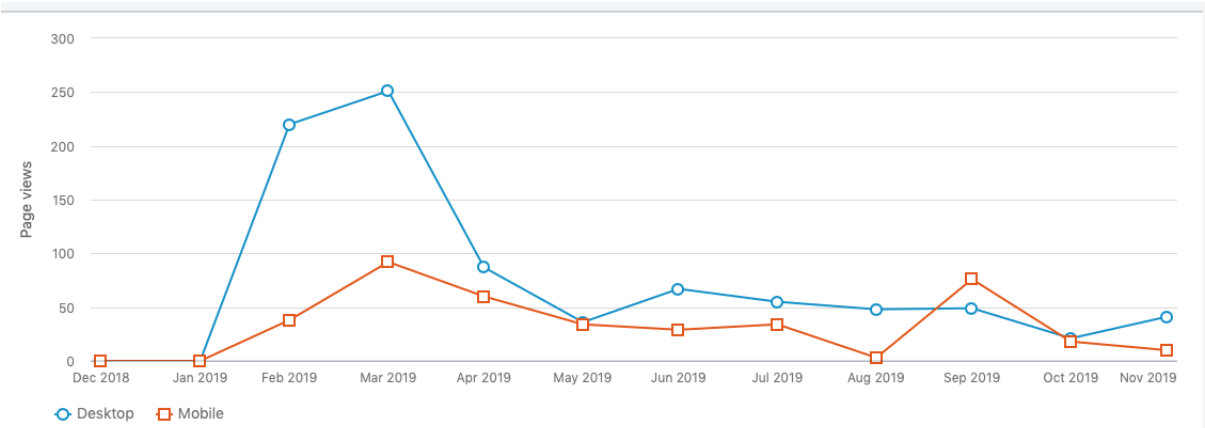
Now together in one platform! **@concordiah2020** **@ECHOcybersec** SPARTA and **@CyberSec4Europe** launch a common website. Visit cybercompetencenetwork.eu to see how we are working to implement a common vision of a more secure **#digital** **#Europe**. **#cybersecurity** **#Competence** **#network** **#H2020** pic.twitter.com/fkN1rs17Nb

20 30

JUN 2019 SUMMARY

Tweets	Tweet impressions
4	30.1K
Profile visits	**Mentions**
171	25
New followers	
50	

Annex 2 – LinkedIn analytics



Visitor demographics | Time range: **Dec 1, 2018 - Nov 30, 2019** | Data for: **Job function**

Top job functions

	Visitors	% of Visitors
Information Technology	254	14.47%
Business Development	232	13.22%
Research	196	11.17%
Education	149	8.49%
Media and Communication	128	7.29%
Engineering	121	6.89%
Program and Project Manag...	102	5.81%
Marketing	88	5.01%
Operations	82	4.67%
Military and Protective Serv...	67	3.82%